REQUEST FOR PROPOSALS

RFP NUMBER: 0A1161
DATE ISSUED: March 15, 2016

The State of Ohio, through the Department of Administrative Services, for the Ohio Office of Information Technology is requesting proposals for:

ENTERPRISE IDENTITY VALIDATION, AUTHENTICATION AND FRAUD SERVICES

INQUIRY PERIOD BEGINS:	**March 15, 2016**
INQUIRY PERIOD ENDS:	**April 29, 2016**
OPENING DATE:	**May 11, 2016**
OPENING TIME:	**1:00 P.M.**
OPENING LOCATION:	**Department of Administrative Services General Services Division Bid Desk 4200 Surface Road Columbus, Ohio 43228-1313**

This RFP consists of five parts and ten attachments, totaling 114 consecutively numbered pages. Supplements also are attached to this RFP with a beginning header page and an ending trailer page. Please verify that you have a complete copy.

In lieu of taking exceptions to RFP requirements, including but not limited to terms and conditions, scope of work statements, service levels requirements, etc., or providing assumptions that may be unacceptable to the State, offerors are strongly encouraged to use the inquiry process in Part Three of the RFP.

PART ONE: EXECUTIVE SUMMARY

Purpose. This is a Request for Competitive Sealed Proposals ("RFP") under Sections 125.071 and 125.18 of the Ohio Revised Code (the "Revised Code") and Section 123:5-1-8 of the Ohio Administrative Code (the "Administrative Code"). The Department of Administrative Services, Office of Information Technology is soliciting competitive sealed proposals ("Proposals") for the development and maintenance of enterprise-wide identity validation, authentication and fraud detection services (the "Work").

If a suitable single offeror solution is made in response to the Work, the State, through the Department of Administrative Services (DAS), may enter into a contract (the "Contract") to have the selected offeror (the "Contractor") perform all or part of the Work.

This RFP provides details on what is required to submit a Proposal for the Work, how the State will evaluate the Proposals, and what will be required of each Contractor in performing the Work.

This RFP also gives the estimated dates for the various events in the submission process, selection process, and performance of the Work. While these dates are subject to change, prospective offerors must be prepared to meet them as they currently stand.

Once awarded, the term of the Contract will be from the award date until the Work is completed to the satisfaction of the State and the Contractor is paid or June 30, 2017, whichever is sooner. The State may renew this Contract for up to two (2) additional one-year term(s), subject to and contingent on the discretionary decision of the Ohio General Assembly to appropriate funds for this Contract in each new biennium. Any such renewal of all or part of the Contract also is subject to the satisfactory performance of the Contractor and the needs of the Department of Administrative Services.

The State may reject any Proposal if the offeror fails to meet a deadline in the submission or evaluation phases of the selection process or objects to the dates for performance of the Work or the terms and conditions in this RFP.

Background. The State, as part of its continual efforts to review, revise and enhance the capabilities of its information technology environment, systems and processes recently conducted an analysis of several large Cabinet Agencies to better understand system capabilities to manage user identities, identify personal information and financial fraud origins and defenses and methods to better protect sensitive data maintained in the State's IT systems portfolio. In summary the analysis determined that:

- Sensitive Data is maintained in almost every Agency across the State and more than half of all State systems maintain some form of Sensitive Data;
- A significant number of State systems maintain Sensitive Data that would have a direct public impact in the event of a data breech or loss;
- While most data maintained by the State is at State data processing centers, there remains a substantial number of systems at Agency locations and State contracted Service Provider locations that require regular review and monitoring for physical, system and other access exposures;
- Many systems that contain Sensitive Data (41%) are not under the sole purview of State Employees
- High value ($ financial) and high volume (e.g., millions of citizens) represent the highest relative risk which require enhanced capabilities to establish, verify, authenticate, log and monitor from a security/privacy perspective
- The State has an opportunity to establish enterprise capabilities and services for State systems that maintain sensitive data as well as a programmatic capability to provide for identity or financial fraud protection; and

This effort is to augment the State's efforts to secure computing locations, networks, servers, storage and data (e.g., physical access, validation and secure encryption) and migrate to more service oriented methods for data exchange that minimizes the "physicalization" of data (data at rest) and other efforts currently underway.

Objectives. The goal of the State is to specify, design and implement a core set of capabilities as an Enterprise Identity Management Framework to allow Individuals (State Workers, Suppliers, Citizens and Businesses) and State Agencies to utilize secure, efficient, easy-to-use, and interoperable identity verification, management,

authorization and fraud detection solutions to access State online services and applications in a manner that promotes confidence, privacy, choice, and innovation.

The Service from an end-to-end perspective (i.e., establishing identities, managing them, integrating with State systems and services, and authenticating access) should foster simpler, more trustworthy and secure interactions between the State and its constituents

The Service must demonstrate an improved user experience (e.g., less passwords to remember and no need to go through laborious credentialing processes for each agency and each system within an agency)

The Service should reduce cost and complexity to State Agencies through economies of scale from an Identity, Integration and Authentication perspective

The Service must result in enhanced security for the State in the form of fraud protection for personal, financial and other sensitive information contained in State systems.

The Service must be an enabler of the State for the increased use of on-line services and increasingly mobile services, thus reducing manual costs

The State is committed to improving the number of minority-owned enterprises that do business with the State of Ohio. A "minority-owned enterprise" is an individual, partnership, corporation or joint venture of any kind that is owned and controlled by U. S. Citizens and residents of Ohio, who are and have held themselves out as members of the following socially and economically disadvantaged groups: Blacks, American Indians, Hispanics and Asians.

The offeror must seek and set aside work for Ohio certified minority business enterprises (MBEs). The MBE must be certified by the Ohio Department of Administrative Services pursuant to ORC 123.151. For more information regarding MBE and MBE certification requirements please refer to the DAS Equal Opportunity Division Web site at: http://das.ohio.gov/Divisions/EqualOpportunity/MBEEDGECertification.aspx

In addition, to search for Ohio MBE-Certified Providers, utilize the following search routine published on the DAS Equal Opportunity Division website:

- Select “MBE Certified Providers” as the EOD Search Area selection;
- On the subsequent screen, at minimum, select the appropriate Procurement Type, e.g., “Information Technology Service” as a search criterion;
- Select “Search”; and
- A list of Ohio MBE Certified Service Providers will be displayed.

Overview of the Project's Scope of Work. The scope of the Work is provided in greater detail within Supplement 1 to this RFP.

Commercial Software Licensing. As part of the Project, the Contractor must license or arrange for the licensing of certain commercial software products (“Commercial Software”) to the State. Commercial Software is software sold in the marketplace in substantial quantities in a substantially unaltered form from one transaction to another and that is maintained through a support program that includes regular updates and new releases. It may also include freeware, such as GNU software, if made generally available in the marketplace, even though such does not precisely meet the above definition. It does not include shells, subroutines, and similar stock bits of software that are not made generally available to the marketplace but that the offeror or others routinely incorporate into otherwise custom work. The offerors proposed software product is considered a key application (“Key Commercial Software”). It must meet the above definition for Commercial Software, and the offeror must offer to license it or arrange for the licensing of it to the State through a license agreement substantially in the form of Attachment Ten to this RFP. Other Commercial Software necessary for the offeror to complete the Project, if awarded the Contract, may be licensed to the State under the terms of Attachment Four or the applicable software marketer’s standard commercial license, if the terms of that license are acceptable to the State, or if the State and the software marketer negotiate acceptable changes to the commercial license.

Offeror’s Proposed Software Environment Requested. Certain aspects of the State’s requirements within Supplement 1 are designated as **optional** and may not be included in the award of the Contract at the discretion of the State. The State may consider other procurement alternatives available (e.g., State price contracts or other means). These include:

- Procurement of all offeror proposed environmental software (e.g., operating system software, system software tools/utilities, database software, etc.) required to operate the offeror's proposed solution for Supplement 1 in applicable environments.
- Procurement of all offeror proposed on-going maintenance environmental software (e.g., operating system software, system software tools/utilities, database software, etc.) required to operate the offeror's proposed solution for Supplement 1 in applicable environments.

Note: The offeror's MBE set-aside costs will be evaluated as a percentage (%) based on the offeror's proposed project management activities and project total costs. The Bill of Materials (BOM) elements, including proposed hardware, environmental software and application solution software costs will not be a component in the evaluation of MBE set-aside percentage.

Calendar of Events. The schedule for the RFP process and the Work is given below. The State may change this schedule at any time. If the State changes the schedule before the Proposal due date, it will do so through an announcement on the State Procurement Website's question and answer area for this RFP. The Website announcement will be followed by an amendment to this RFP, also available through the State's Procurement Website. After the Proposal due date and before the award of the Contract, the State will make schedule changes through the RFP amendment process. Additionally, the State will make changes in the Work schedule after the Contract award through the change order provisions in the General Terms and Conditions Attachment to this RFP. It is each prospective offeror's responsibility to check the Website question and answer area for this RFP for current information regarding this RFP and its Calendar of Events through award of the Contract.

Dates:

<u>Firm Dates</u>	
RFP Issued:	March 15, 2016
Inquiry Period Begins:	March 15, 2016
Inquiry Period Ends:	April 29, 2016 at 8:00 a.m.
Proposal Due Date:	May 11, 2016 at 1:00 p.m.
<u>Estimated Dates</u>	
Award Date:	June 2016
<u>Estimated Work Dates</u>	
Work Begins:	July 2016

There are references in this RFP to the Proposal due date. Unless it is clearly provided to the contrary in this RFP, any such reference means the date and time (Columbus, Ohio local time) that the Proposals are due and not just the date.

PART TWO: STRUCTURE OF THIS RFP

Organization. This RFP is organized into five parts and has eleven (11) attachments. The parts and attachments are listed below. There also may be one or more supplements to this RFP listed below.

Parts:

Part 1 Executive Summary
Part 2 Structure of this RFP
Part 3 General Instructions
Part 4 Evaluation of Proposals
Part 5 Award of the Contract

Attachments:

Attachment One	Evaluation Criteria
Attachment Two	Special Provisions
Attachment Three	Requirements for Proposals
Attachment Four	General Terms and Conditions
Attachment Five	Sample Contract
Attachment Six	Offeror Certification Form
Attachment Seven	Offeror Profile Summary
Attachment Eight	Standard Affirmation and Disclosure Form (EO 2011-2012K)
Attachment Nine	Supplement 1 – Cost Summary Workbook
Attachment Ten	Master Contract for Software Licensing
Attachment Eleven	Master Cloud Services Agreement and Service Attachment

Supplements:

Supplement 1	Enterprise Identity Validation, Authentication and Fraud Services
Supplement 2	Architecture and Computing Standards, Security, Privacy and Data Handling Requirements

PART THREE: GENERAL INSTRUCTIONS

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

Contacts. The following person will represent the State during the RFP process:

Procurement Representative:

Valerie Piccininni
Acquisition Analyst
Department of Administrative Services/OIT
Enterprise IT Contracting
30 East Broad Street, 39th Floor
Columbus, Ohio 43215

During the performance of the Project, a State representative (the "Project Representative") will represent the State and be the primary contact for the Project. The State will designate the Project Representative after the Contract award.

Inquiries. Offerors may make inquiries regarding this RFP anytime during the inquiry period listed in the Calendar of Events. To make an inquiry, offerors must use the following process:

- Access the State's Procurement Website at http://procure.ohio.gov/;
- From the Quick Links menu on the right, select "**Bid Opportunities Search**";
- In the "**Document/Bid Number**" field, enter the RFP number found on the first page of this RFP (the RFP number begins with zero followed by the letter "A");
- Select "**Request for Proposals**" from the Opportunity Type dropdown;
- Click the "Search" button;
- On the Opportunity Search Results page, click on the hyperlinked Bid Number;
- On the Opportunity Details page, click the "Submit Inquiry" button;
- On the document inquiry page, complete the required "Personal Information" section by providing:
  - First and last name of the prospective offeror's representative who is responsible for the inquiry,
  - Name of the prospective offeror,
  - 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 RFP,
  - The heading for the provision under question, and
  - The page number of the RFP where the provision can be found; and
- Enter the Confirmation Number at the bottom of the page
- Click the "Submit" button.

An offeror submitting an inquiry will receive an immediate acknowledgement that the State has received the inquiry as well as an email acknowledging receipt. The offeror will not receive a personalized response to the question nor notification when the State has answered the question.

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

The State usually responds to all inquiries within three business days of receipt, excluding weekends and State holidays. 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.

Amendments to the RFP. If the State revises this RFP before the Proposals are due, it will announce any amendments on the State Procurement Website.

Offerors may view amendments by using the "Bid Opportunities Search" function of the State's Procurement Webpage (described in the Inquiries Section above) and then clicking on the amendment number to display the amendment.

When an amendment to this RFP is necessary, the State may extend the Proposal due date through an announcement on the State Procurement Website. The State may issue amendment announcements any time before 5:00 p.m. on the day before Proposals are due, and it is each prospective offeror's responsibility to check for announcements and other current information regarding this RFP.

After the Proposal due date, the State will distribute amendments only to those offerors whose Proposals are under active consideration. When the State amends the RFP after the due date for Proposals, the State will permit offerors to withdraw their Proposals within five business days after the amendment is issued. This withdrawal option will allow any offeror to remove its Proposal from active consideration should the offeror feel that the amendment changes the nature of the transaction so much that the offeror's Proposal is no longer in its interest. Alternatively, the State may allow offerors that have Proposals under active consideration to modify their Proposals in response to the amendment.

If the State allows offerors to modify their Proposals in response to an amendment, the State may limit the nature and scope of the modifications. Unless otherwise provided in the State's notice, offerors must make any modifications or withdrawals in writing and submit them to the State within five business days after the amendment is issued at the address and in the same manner required for the submission of the original Proposals. If this RFP provides for a negotiation phase, this submission procedure will not apply to changes negotiated during that phase. The State may reject any modification that is broader in scope than the State has authorized in the announcement of the amendment and treat it as a withdrawal of the offeror's Proposal.

Proposal Submittal. Each offeror must submit a technical section and a cost section as part of its total Proposal before the opening time on the Proposal due date. The offeror must submit the technical section as a separate package from the cost section of its Proposal, and each section must be submitted in its own separate, opaque package. The package with the technical section of the Proposal must be sealed and contain one (1) originally signed technical section and eight (8) copies of the technical section, and the package with the cost section also must be sealed and contain three (3) complete copies of the cost section of the Proposal. Further, the offeror must mark the outside of each package with either "**Enterprise Identity Validation, Authentication and Fraud Services RFP – Technical Proposal**" or "**Enterprise Identity Validation, Authentication and Fraud Services RFP – Cost Summary**," as appropriate.

All offerors are subject to the architecture and computing standards, security, privacy and data handling requirements of Supplement 2, regardless of the offeror's proposed solution.

Included in each sealed package, the offeror also must provide an electronic "searchable" copy of everything contained within the package on CD-ROM in Microsoft Office (native format), Microsoft Word (native format), Microsoft Project (native format), Microsoft Excel (native format) and Adobe Acrobat format, as appropriate. If there is a discrepancy between the hard copy and the electronic copy of the Proposal, the hard copy will control, and the State will base its evaluation of the offeror's Proposal on the hard copy.

Proposals are due no later than 1:00 p.m. on the Proposal due date. Proposals submitted by email, fax, or other electronic means are <u>not</u> acceptable, and the State may reject them. Offerors must submit their Proposals to:

Department of Administrative Services
Attn: Bid Desk
4200 Surface Road
Columbus, Ohio 43228

Bid Desk Main Phone Number: 614-466-5090

The State may reject any Proposals or unsolicited modifications it receives after the deadline. An offeror that mails its Proposal must allow for adequate mailing time to ensure its timely receipt. Offerors also must allow for

potential delays due to increased security. The Bid Desk accepts packages between the hours of 7:30 A.M. to 5:00 P.M. Monday through Friday, excluding State Holidays. No deliveries will be accepted before or after these hours without prior arrangements. Offerors must allow sufficient time since the State may reject late Proposals regardless of the cause for the delay.

Each offeror must carefully review the requirements of this RFP and the contents of its Proposal. Once opened, Proposals cannot be altered or withdrawn, except as allowed by this RFP.

By submitting a Proposal, the offeror acknowledges it has read this RFP, understands it, and agrees to be bound by its requirements. The State is not responsible for the accuracy of any information regarding this RFP that was gathered through a source other than the inquiry process described in the RFP.

Revised Code Section 9.24 prohibits the State from awarding a contract to any entity against whom the Auditor of State has issued a finding for recovery (a "Finding"), if the Finding is unresolved at the time of the award. This also applies to renewals of contracts. By submitting a Proposal, the offeror warrants it is not subject to an unresolved Finding under Section 9.24 at the time of its submission. Additionally, the offeror warrants it will notify the Department of Administrative Services in writing immediately upon becoming subject to such an unresolved Finding after submitting its Proposal and before the award of a Contract under this RFP. Should the State select the offeror's Proposal for award of a Contract, this warranty of immediate written notice will apply during the term of the Contract, including any renewals or extensions. Further, the State may treat any unresolved Finding against the Contractor that prevents a renewal of the Contract as a breach, in accordance with the provisions of Attachment Four, General Terms and Conditions.

The State may reject any Proposal if the offeror takes exception to the terms and conditions of this RFP, includes unacceptable assumptions or conditions in its Proposal, fails to comply with the procedure for participating in the RFP process, or fails to meet any requirement of this RFP. The State also may reject any Proposal it believes is not in its interest to accept and may decide not to award a contract to any or all of the offerors responding to this RFP.

Offerors may not prepare or modify their Proposals on State premises.

All Proposals and other material offerors submit will become the property of the State and may be returned only at the State's option. Offerors should not include any confidential information in a Proposal or other material submitted as part of the evaluation process. All Proposals will be open to the public after the State has awarded the Contract.

The State will retain all Proposals, or a copy of them, as part of the Contract file for at least three years. After the three-year retention period, the State may return, destroy, or otherwise dispose of the Proposals and any copies of them.

Waiver of Defects. The State may waive any defects in any Proposal or in the submission process followed by an offeror, but the State will only do so if it believes that it is in the State's interest and will not cause any material unfairness to other offerors.

Multiple or Alternate Proposals. The State will not accept multiple Proposals from a single offeror or any alternative solutions or options to the requirements of this RFP. Additionally, any offeror that disregards a requirement in this RFP simply by proposing an alternative to it may have its Proposal rejected by the State. Further, any offeror that submits multiple Proposals for each of these options may have all of its Proposals rejected.

Changes to Proposals. The State will allow modifications or withdrawals of Proposals only if the State receives them before the Proposal due date. No modifications or withdrawals will be permitted after the due date, except as authorized by this RFP.

Proposal Instructions. Each Proposal must be organized in an indexed binder ordered in the same manner as the response items are ordered in the applicable attachments to this RFP. The requirements for a Proposal's contents and formatting are contained in the attachments to this RFP. The State wants clear and concise Proposals, but offerors must answer questions completely and meet all the RFP's requirements.

The State is not liable for any costs an offeror incurs in responding to this RFP or from participating in the evaluation process, regardless of whether the State awards the Contract through this process, decides not to go forward with the Work, cancels this RFP for any reason, or contracts for the Work through some other process or through another RFP.

PART FOUR: EVALUATION OF PROPOSALS

Disclosure of Proposal Contents. The State will seek to open the Proposals in a manner that avoids disclosing their contents. Additionally, the State will seek to keep the contents of all Proposals confidential until the Contract is awarded. But the State will prepare a registry of Proposals that contains the name of each offeror. The public may inspect that registry after the State opens the Proposals.

Rejection of Proposals. The State may reject any Proposal that is not in the required format, does not address all the requirements of this RFP, objects to the terms or conditions of this RFP, or that the State determines is excessive in price or otherwise not in the State's interest to accept. In addition, the State may cancel this RFP, reject all the Proposals, and seek to do the Work through a new RFP or other means.

Evaluation of Proposals Generally. The evaluation process may consist of up to six distinct phases:

1. Initial review;
2. Technical evaluation;
3. Evaluation of costs;
4. Requests for more information;
5. Determination of responsibility; and
6. Contract Negotiations.

The State may decide whether phases four and six are necessary, and the State may rearrange the order in which it proceeds with the phases. The State also may add or remove sub-phases to any phase at any time, if the State believes doing so will improve the evaluation process.

Clarifications and Corrections. During the evaluation process, in the State's sole discretion, it may request clarifications from any offeror under active consideration and may give any offeror the opportunity to correct defects in its Proposal, if the State believes doing so would not result in an unfair advantage for the offeror, and it is in the State's interest. The State may reject any clarification that is non-responsive or broader in scope than what the State requested. If the State does so, or if the offeror fails to respond to the request for clarification, the State then may request a corrected clarification, consider the offeror's Proposal without the clarification, or disqualify the offeror's Proposal.

Corrections and clarifications must be completed off State premises.

Initial Review. The State will review all Proposals for their format and completeness. The State normally rejects incomplete or incorrectly formatted Proposals, though it may waive any defects or allow an offeror to submit a correction, if the State believes doing so would not result in an unfair advantage for the offeror and it is in the State's interest. Further, if the Auditor of State does not certify a Proposal due to lateness, the State will not open it. After the initial review, the State will forward all timely, complete, and properly formatted Proposals to an evaluation team, which the Procurement Representative will lead.

Technical Evaluation. The State will evaluate each Proposal that it has determined is timely, complete, and properly formatted. The evaluation will be scored according to the requirements identified in this RFP, including the requirements in Attachment One. Other attachments to this RFP may further refine these requirements, and the State has a right to break these requirements into components and weight any components of a requirement according to their perceived importance.

The State also may have the Proposals or portions of them reviewed and evaluated by independent third parties or various State personnel with experience that relates to the Work or to a criterion in the evaluation process. Additionally, the State may seek reviews from end users of the Work or the advice or evaluations of various State personnel that have subject matter expertise or an interest in the Work. The State may adopt or reject any

recommendations it receives from such reviews and evaluations or give them such weight as the State believes is appropriate.

During the technical evaluation, the State will calculate a point total for each Proposal that it evaluates. At the sole discretion of the State, it may reject any Proposal receiving a significant number of zeros for sections in the technical portions of the evaluation. The State may select those offerors submitting the highest rated Proposals for the next phase. The number of Proposals that advance to the next phase will be within the State's discretion, but regardless of the number of Proposals selected, they always will be the highest rated Proposals from this phase.

At any time during this phase, in the State's sole discretion, it may ask an offeror to correct, revise, or clarify any portions of its Proposal.

The State will document all major decisions and make these a part of the Contract file, along with the evaluation results for each Proposal considered.

Requirements. Attachment One provides requirements the State will use to evaluate the Proposals, including any mandatory requirements. If the offeror's Proposal meets all the mandatory requirements, the offeror's Proposal may be included in the next phase of the evaluation, which will consider other requirements described in a table in Attachment One.

In the case of any requirements for a team of people the offeror is proposing, the offeror must submit a team to do the Work that collectively meets all the team requirements. But the experience of multiple candidates may not be combined to meet a single requirement. Further, previous experience of the candidate submitted for a Work Manager position may not be used to meet any other team member requirements. Each candidate proposed for the Work team must meet at least one of the requirements.

This RFP asks for responses and submissions from offerors, most of which represent components of the requirements in Attachment One. While each requirement represents only a part of the total basis for a decision to award the Contract to an offeror, a failure by an offeror to make a required submission or meet a mandatory requirement normally will result in a rejection of that offeror's Proposal. The value assigned above to each requirement is only a value used to determine which Proposal is the most advantageous to the State in relation to the other Proposals that the State received. It is not a basis for determining the importance of meeting that requirement.

If the State does not receive any Proposal that meets all the mandatory requirements, the State may cancel this RFP. Alternatively, if the State believes it is in its interest, the State may continue to consider the highest-ranking Proposals despite their failure to meet all the mandatory requirements. In doing this, the State may consider one or more of the highest-ranking Proposals. But the State may not consider any lower-ranking Proposals unless all Proposals ranked above it are also considered, except as provided below.

In any case where no Proposal meets all the mandatory requirements, it may be that an upper ranking Proposal contains a failure to meet a mandatory requirement that the State believes is critical to the success of the RFP's objectives. When this is so, the State may reject that Proposal and consider lower ranking Proposals. Before doing so, the State may notify the offeror of the situation and allow the offeror an opportunity to cure its failure to meet that mandatory requirement.

If the offeror cures its failure to meet a mandatory requirement that the State has deemed critical to the success of the RFP's objectives, the State may continue to consider the offeror's Proposal. But if the offeror is unwilling or unable to cure the failure, its Proposal may be rejected. The State then may continue to consider the other remaining Proposals, including, if the State so chooses, Proposals that ranked lower than the rejected Proposal.

Cost Evaluation. Once the technical merits of the Proposals are considered, the State may consider the costs of one or more of the highest-ranking Proposals. But it is within the State's discretion to wait until after any interviews, presentations, and demonstrations to evaluate costs. Also, before evaluating the technical merits of the Proposals, the State may do an initial review of costs to determine if any Proposals should be rejected because of excessive cost. And the State may reconsider the excessiveness of any Proposal's cost at any time in the evaluation process.

The State may select one or more of the Proposals for further consideration in the next phase of the evaluation process based on the price performance formula contained in Attachment One. The Proposal(s) selected for consideration in the next phase always will be the highest-ranking Proposal(s) based on this analysis. That is, the State may not move a lower-ranking Proposal to the next phase unless all Proposals that rank above it also are moved to the next phase, excluding any Proposals that the State disqualifies because of excessive cost or other irregularities.

If the State finds that it should give one or more of the highest-ranking Proposals further consideration, the State may move the selected Proposals to the next phase. The State alternatively may choose to bypass any or all subsequent phases and make an award based solely on its scoring of the preceding phases, subject only to its review of the highest-ranking offeror's responsibility, as described below.

Requests for More Information. The State may require some offerors to interview, make a presentation about their Proposals, or demonstrate their products or services. If the presentations, demonstrations, or interviews are held as part of the technical evaluation phase, all offerors that have Proposals under evaluation may participate. Alternatively, if the presentations, demonstrations, or interviews are held after the technical evaluation, the State normally will limit them to one or more of the highest ranking offerors. The State normally will limit such presentations, demonstrations, and interviews to areas in which it seeks further information from the highest ranking offeror or offerors. Typically, these discussions provide an offeror with an opportunity to do one or more of the following:

- Clarify its Proposal and ensure a mutual understanding of the Proposal's content;
- Showcase its approach to the Work; and
- Demonstrate the professionalism, qualifications, skills, and work knowledge of its proposed candidates.

The State will schedule the presentations, demonstrations, and interviews at its convenience and discretion. The State will determine the scope and format of any such presentations, demonstrations, and interviews and may record them. Additionally, if the State moves more than one offeror to this phase, the scope and format of these presentations, demonstrations, and interviews may vary from one offeror to the next, depending on the particular issues or concerns the State may have with each offeror's Proposal.

The State normally will not rank interviews, demonstrations, and presentations. Rather, if the State conducts the interviews, demonstrations, or presentations as part of the technical evaluation, the State may use the information it gathers during this process in evaluating the technical merits of the Proposals. If the State holds the demonstrations, presentations, or interviews only for one or more of the top-ranking offerors after the evaluation phase, the State may decide to revise its existing Proposal evaluations based on the results of this process.

Determination of Responsibility. The State may review the background of one or more of the highest-ranking offerors and its or their key team members and subcontractors to ensure their responsibility. For purposes of this RFP, a key team member is a person that an offeror identifies by name in its Proposal as a member of its proposed team. The State will not award the Contract to an offeror that it determines is not responsible or that has proposed candidates or subcontractors to do the Work that are not responsible. The State's determination of an offeror's responsibility may include the following factors: experience of the offeror and its key team members and subcontractors, its and their past conduct on previous contracts, past performance on previous contracts, ability to execute this Contract properly, and management skill. The State may make this determination of responsibility based on the offeror's Proposal, reference evaluations, a review of the offeror's financial ability, and any other information the State requests or determines is relevant.

Some of the factors used in determining an offeror's responsibility, such as reference checks, may also be used in the technical evaluation of Proposals in phase two of the evaluation process. In evaluating those factors in phase two, the weight the State assigns to them, if any, for purposes of the technical evaluation will not preclude the State from rejecting a Proposal based on a determination that an offeror is not responsible. For example, if the offeror's financial ability is adequate, the value, if any, assigned to the offeror's relative financial ability in relation to other offerors in the technical evaluation phase may or may not be significant, depending on the nature of the Work. If the State believes the offeror's financial ability is inadequate, the State may reject the offeror's Proposal despite its other merits.

The State may make a responsibility determination at any time during the evaluation process, but it typically will do so only once it has evaluated the technical merits and costs of the Proposals. The State always will review the

responsibility of an offeror selected for an award before making the award, if it has not already done so earlier in the evaluation process. If the State determines that the offeror selected for award is not responsible, the State then may go down the line of remaining offerors, according to rank, and determine responsibility with the next highest-ranking offeror.

Reference Checks. As part of the State's determination of an offeror's responsibility, the State may conduct reference checks to verify and validate the offeror's and its proposed candidates' and subcontractors' past performance. Reference checks that indicate poor or failed performance by the offeror or a proposed candidate or subcontractor may be cause for rejection of the offeror's Proposal. Additionally, the State may reject an offeror's Proposal as non-responsive if the offeror fails to provide requested reference contact information.

The State may consider the quality of an offeror's and its candidates' and subcontractors' references as part of the technical evaluation phase, as well as in the State's determination of the offeror's responsibility. The State also may consider the information it receives from the references in weighing any requirement contained in the technical evaluation phase, if that information is relevant to the requirement. In checking an offeror's or any of its proposed candidates' or subcontractors' references, the State will seek information that relates to the offeror's previous contract performance. This may include performance with other governmental entities, as well as any other information the State deems important for the successful operation and management of the Work and a positive working relationship between the State and the offeror. In doing this, the State may check references other than those provided in the offeror's Proposal. The State also may use information from other sources, such as third-party reporting agencies.

Financial Ability. Part of State's determination of an offeror's responsibility may include the offeror's financial ability to perform the Contract. This RFP may expressly require the submission of audited financial statements from all offerors in their Proposals, but if this RFP does not make this an express requirement, the State still may insist that an offeror submit audited financial statements for up to the past three years, if the State is concerned that an offeror may not have the financial ability to carry out the Contract. Also, the State may consider financial information other than the information that this RFP requires as part of the offeror's Proposal, such as credit reports from third-party reporting agencies.

Contract Negotiations. The final phase of the evaluation process may be contract negotiations. It is entirely within the discretion of the State whether to permit negotiations. An offeror must not submit a Proposal assuming that there will be an opportunity to negotiate any aspect of the Proposal, and any Proposal that is contingent on the State negotiating with the offeror may be rejected. The State is free to limit negotiations to particular aspects of any Proposal or the RFP, to limit the offerors with whom the State negotiates, and to dispense with negotiations entirely. If negotiations are held, they will be scheduled at the convenience of the State, and the selected offeror or offerors must negotiate in good faith.

The State may limit negotiations to specific aspects of the RFP or the offeror's Proposal. Should the evaluation result in a top-ranked Proposal, the State may limit negotiations to only that offeror and not hold negotiations with any lower-ranking offeror. If negotiations are unsuccessful with the top-ranked offeror, the State then may go down the line of remaining offerors, according to rank, and negotiate with the next highest-ranking offeror. Lower-ranking offerors do not have a right to participate in negotiations conducted in such a manner.

If the State decides to negotiate simultaneously with more than one offeror, or decides that negotiations with the top-ranked offeror are not satisfactory and therefore negotiates with one or more of the lower-ranking offerors, the State then will determine if an adjustment in the ranking of the offerors with which it held negotiations is appropriate based on the negotiations. The Contract award, if any, then will be based on the final ranking of offerors, as adjusted.

Auction techniques that reveal one offeror's price to another or disclose any other material information derived from competing Proposals are prohibited. Any oral modification of a Proposal will be reduced to writing by the offeror as described below.

Following negotiations, the State may set a date and time for the offeror(s) with which the State conducted negotiations to submit a best and final Proposal. If negotiations were limited and all changes were reduced to signed writings during negotiations, the State need not require a best and final Proposal.

If best and final Proposals are required, they may be submitted only once, unless the State determines that it is in the State's interest to conduct additional negotiations. In such cases, the State may require another submission of best and final Proposals. Otherwise, discussion of or changes in the best and final Proposals will not be allowed. If an offeror does not submit a best and final Proposal, the State will treat that offeror's previous Proposal as its best and final Proposal.

The State usually will not rank negotiations and normally will hold them only to correct deficiencies in or enhance the value of the highest-ranked offeror's Proposal.

From the opening of the Proposals to the award of the Contract, everyone evaluating Proposals on behalf of the State will seek to limit access to information contained in the Proposals solely to those people with a need to know the information. The State also will seek to keep this information away from other offerors, and the State may not tell one offeror about the contents of another offeror's Proposal in order to gain a negotiating advantage.

Before the award of the Contract or cancellation of the RFP, any offeror that seeks to gain access to the contents of another offeror's Proposal may be disqualified from further consideration.

Negotiated changes will be reduced to writing and become a part of the Contract file, which will be available for public inspection after award of the Contract or cancellation of the RFP, provided the State does not plan to reissue the RFP. If the State plans to reissue the RFP, the Contract file will not be available until the subsequent RFP process is completed. Unless the State agrees otherwise in writing, the offeror must draft and sign the written changes and submit them to the State within five business days. If the State accepts the changes, the State will give the offeror written notice of the State’s acceptance, and the negotiated changes to the successful offer will become a part of the Contract.

Failure to Negotiate. If an offeror fails to provide the necessary information for negotiations in a timely manner, or fails to negotiate in good faith, the State may terminate negotiations with that offeror, remove the offeror’s Proposal from further consideration, and seek such other remedies as may be available in law or in equity.

PART FIVE: AWARD OF THE CONTRACT

Contract Award. The State plans to award the Contract based on the schedule in the RFP, if the State decides the Work is in its best interest and has not changed the award date.

Included with this RFP, as Attachment Five, is a sample of the Contract for the RFP. The State will issue two originals of the Contract to the Contractor proposed for award. The offeror must sign and return the two originals to the Procurement Representative. The State also may issue two originals of any Master Contract(s) for Software Licensing (Master Contract(s)) or Master Cloud Services Agreement (Cloud), if applicable to the Contractor. If the licensor under any such Master Contract or Cloud is not the offeror, the offeror will be responsible for coordinating execution of the document by the licensor and returning it to the State with the two originally signed copies of the Contract. The Contract and any Master Contract or Cloud will bind the State only when the State's duly authorized representative signs all copies and returns one to the Contractor with an award letter, the State issues a purchase order, and all other prerequisites identified in the Contract have occurred.

The Contractor must begin work within 15 business days after the State issues a purchase order, or on a mutually agreed start date, under the Contract. If the State awards a Contract pursuant to this RFP, and the Contractor is unable or unwilling to perform the Work, the State may cancel the Contract, effective immediately on notice to the Contractor. The State then may return to the evaluation process under this RFP and resume the process without giving further consideration to the originally selected Proposal. Additionally, the State may seek such other remedies as may be available to the State in law or in equity for the selected Contractor's failure to perform under the Contract.

Contract. If this RFP results in a Contract award, the Contract will consist of:

1. The one page Contract (Attachment Five) in its final form; and
2. The 0A1161 Enterprise Identity Validation, Authentication and Fraud Services Contract dated _____, 2016 which includes Attachment Four, Attachments, Supplements and the Cost Proposal Workbook dated _____, 2016.

The Contract is the result of and includes agreed upon changes to the RFP its attachments and supplements including any written amendments to the RFP, any materials incorporated by reference in the RFP, the Contractor's Proposal, and written, authorized amendments and clarifications to the Contractor's Proposal. It also includes any purchase orders and change orders issued under the Contract.

Change Orders and amendments issued after the Contract is executed may expressly change the provisions of the Contract. If they do so expressly, then the most recent of them will take precedence over anything else that is part of the Contract.

Any Master Contract for Software Licensing or Cloud will be a separate agreement and not part of the Contract, but the State may require the incorporation into the Master Contract or Cloud of any representations regarding the performance, features, and functions of the Key Commercial Software or Hosting made in the RFP.

ATTACHMENT ONE: EVALUATION CRITERIA

Mandatory Requirements. The first table lists this RFP's mandatory requirements for this RFP. If the offeror's Proposal meets all the mandatory requirements, the offeror's Proposal may be included in the next part of the technical evaluation phase as described in the next table.

Mandatory Requirements	Accept	Reject
1. The offeror, as the prime Contractor, must be an HSPD-12 (ICAM) qualified Contractor or Service Provider as of the date of proposal submission.		
2. The offeror, must as part of their offer to the State include a FICAM TFS Approved Identity Service at National Institute of Standards and Technology (NIST) Levels 1, 2 or 3 as of the date of proposal submission.		
3. The offeror, as the prime Contractor, must have performed and completed a systems integration project using the proposed architecture in a production environment for at least one Public Governmental, Federal, State, Local, Institution of Higher Education, Fortune 500 or Global Fortune 500 customer within the last four years.		

Scored Criteria. In the technical evaluation phase, the State will rate the technical merits of the Proposals based on the following requirements and the weight assigned to each requirement:

Enterprise Identity Validation, Authentication and Fraud Services					
Scored Criteria	**Weight**	**Does Not Meet**	**Partially Meets**	**Meets**	**Exceeds**
Offeror Requirement: The offeror, as the Prime Contractor, must have performed and completed a systems integration project using the proposed architecture in a production environment for at least one Public Governmental, Federal, State, Local, Institution of Higher Education, Fortune 500 or Global Fortune 500 customer within the last four years.	**50**	**Rejected**	**2**	**5**	**7**
Enterprise Architecture and Integration Standards and Conventions: Supplement 1, Section 3 in its entirety.	**50**	**0**	**2**	**5**	**7**
Multi-Factor Definitive Identity Proofing: Supplement 1, Section 4 in its entirety.	**75**	**0**	**2**	**5**	**7**
State Systems Integration Services: Supplement 1, Section 5 in its entirety.	**50**	**0**	**2**	**5**	**7**
Solution, Implementation Plan and Completeness of Solution for Enterprise e-Licensing Platform (Pilot 1): Supplement 1, Section 6.1 in its entirety.	**50**	**0**	**2**	**5**	**7**
Solution, Implementation Plan and Completeness of Solution for Ohio Business Gateway Project (Pilot 2): Supplement 1, Section 6.2 in its entirety.	**50**	**0**	**2**	**5**	**7**
Solution, Implementation Plan and Completeness of Solution for Department of Taxation Identity Attribute Proofing Service (Pilot 3): Supplement 1, Section 6.3 in its entirety.	**50**	**0**	**2**	**5**	**7**
Implementation of Two Factor Authentication (2FA): Supplement 1, Section 7 in its entirety.	**50**	**0**	**2**	**5**	**7**
Implementation of Enterprise Logging, Audit and Fraud Detection: Supplement 1, Section 8 in its entirety.	**75**	**0**	**2**	**5**	**7**
Project Delivery, Management, Methodology and Approach: Supplement 1, Sections 9.1 – 9.17	**50**	**0**	**2**	**5**	**7**

Enterprise Identity Validation, Authentication and Fraud Services					
Scored Criteria	**Weight**	**Does Not Meet**	**Partially Meets**	**Meets**	**Exceeds**
Project Completion, Knowledge Transfer, Documentation, Post-Implementation and Production Support/Transition: Supplement 1, Sections 9.18 and 9.19.	**25**	**0**	**2**	**5**	**7**
Project Staffing Requirements and Use of State Staff on OIT and Pilot Projects: Including the completeness of the overall solution, project plan in delivery of the proposed solution and use of State Resources (OIT and Pilot Agencies) in the successful delivery of an Enterprise Solution (in general) and the Pilot Projects (specifically).	**50**	**0**	**2**	**5**	**7**
Offeror Proposed Key Personnel and Team: Supplement 1, Section 12 in its entirety.	**75**	**0**	**2**	**5**	**7**
Adherence to State Delivery Service Level Standards: Supplement 1, Sections 13 and 14.	**25**	**0**	**2**	**5**	
Adherence to State Architecture and Computing Standards, Security and Privacy, IT Computing and Data Handling Requirements: Supplement 2.	**25**	**0**		**5**	

Evaluation Scoring 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	20%
MBE Set-aside	10%

The State is committed to making more State contracts, services, benefits and opportunities available to minority business enterprises (MBE). To foster this commitment, the State included an MBE Set-aside component in the Evaluation Scoring Formula (shown above) of this RFP.

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 Supplement 1 Technical Proposal will receive 700 points. The remaining offerors will receive a percentage of the maximum points available based upon the following formulas:

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

The offeror with the lowest proposed Not-To-Exceed Fixed Price will receive 200 points. The remaining offerors will receive a percentage of the maximum cost points available based upon the following formula:

> **Cost Summary Points** = (Lowest Not-To-Exceed Fixed Price/Offeror's Not-To-Exceed Fixed Price) x 200

The offeror with the highest proposed MBE Set-aside Cost percentage will receive 100 points respectively. The remaining offerors will receive a percentage of the maximum MBE Set-aside points available based upon the following formula:

> **MBE Set-aside Points** = (Offeror's MBE Set-aside Cost Percentage/Highest MBE Set-aside Cost Percentage) x 100

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

Total Points = Technical Proposal Points + Cost Summary Points + MBE Set-aside Points

Note: The offeror's MBE set-aside costs will be evaluated as a percentage (%) based on the offeror's proposed project management activities and project total costs. Any Hardware, Software or Cloud Service Bill of Materials (BOM) elements, including proposed hardware, environmental software and application solution software costs will not be a component in the evaluation of MBE set-aside percentage.

ATTACHMENT TWO: SPECIAL PROVISIONS

Submittal of Deliverables. The Contractor must perform its tasks in a timely and professional manner that produces Deliverables that fully meet the Contract's requirements. And the Contractor must provide the Deliverables no later than the due dates the Contract requires. At the time of delivery of a written Deliverable, the Contractor must submit an original and one copy of each Deliverable, plus an electronic copy. The Contractor must provide the electronic copy in a file format acceptable to the State.

By submitting a Deliverable, the Contractor represents that, it has performed the associated tasks in a manner that meets the Contract's requirements.

The Contractor must provide all Deliverables to the State Project Representative, who will review (or delegate review of) the materials or documents within a reasonable time after receipt, as specified in the State approved, base-lined Project Plan.

If the State determines that a Deliverable is not in compliance, the State Project Representative will note the reason for non-compliance and send notification to the Contractor Project Manager. At no expense to the State, the Contractor then must bring the Deliverable into conformance and re-submit it to the Project Representative within ten business days.

If the State agrees the Deliverable is compliant, the State Project Representative will sign a Deliverable Submittal Form and return a copy to the Contractor. In addition, if the State Project Representative or designee determines that the State should make a payment associated with the Deliverable, the State Project Representative will indicate that the payment should be made on the Deliverable Submittal Form.

The State form authorizing payment and the payment itself do not indicate that the State has accepted the Deliverables associated with the payment. The State's acceptance of the Deliverables that are part of developing the Project is conditioned on a successful performance test upon completion of the Project or Services (if applicable).

General Systems Implementation Standards. The Contractor has and will continue to use its best efforts through quality assurance procedures to ensure there are no viruses or malware or undocumented features in its infrastructure and services and that they do not contain any embedded device or code (e.g., time bomb) that is intended to obstruct or prevent any use of or access to them by the State.

Inconsistencies between Contract and Deliverables. If any terms and conditions that may be incorporated in a User, Operations, Training Document or Guide or Contractor created Deliverable, work product, assumption, responsibility or activity are inconsistent or conflict with the Contract, the Contract shall prevail.

The Contractor's Fee Structure. The Contract award will be for a Not-To-Exceed Fixed Price as agreed in the offerors Cost Summary Microsoft Excel® Workbook, Attachment Nine, (in native MS Excel format) payable in accordance with the following:

- **Project Management Services.** The Contractor may submit an invoice upon receipt of a signed Deliverable Submittal Form indicating State acceptance that the monthly Project Management Services delivered met Contract requirements and payment should be made.

  The monthly Project Management Services will be paid within 30 days of receipt of a valid invoice, noting that the services have been ordered, delivered, and accepted in accordance with the offeror's proposed Project Plan.

- **Project Deliverables.** The Contractor may submit an invoice for Deliverables or milestones upon receipt of a signed Deliverable Submittal Form indicating State acceptance that the Deliverable or milestone completed met Contract requirements and payment should be made.

  Project Deliverables will be paid within 30 days of receipt of a valid invoice, noting that the Deliverable has been accepted in accordance with the offeror's proposed Project Plan.

- **Application (Solution) and Environmental Software.** The State will pay fees related to the "solution" application and environmental software and any other Commercial Software that it acquires as part of this Contract only on the State's execution of a schedule or other ordering document, delivery of the software F.O.B. to the Project site, acceptance of the software in accordance with the applicable schedule or other ordering document, and receipt of a proper invoice for the software.

  Software licenses will be paid within 30 days of receipt of a valid invoice, noting that the software license(s) have been ordered, delivered, installed and accepted in the identified environment in accordance with the offeror's proposed Project Plan.

  The State will pay ongoing annual maintenance fees for any application and environmental software and any other Commercial Software acquired as part of this Contract only on the State's execution of a schedule or other ordering document on an annual basis within 30 days of receipt of a valid invoice. At the State's request, the first Support Period may be pro-rated so that the Anniversary Date coincides with the end of the State's Fiscal Year.

- **Hardware and Related Components.** The State will pay fees related to the "solution" hardware and related components that it acquires as part of this Contract if required, only on the State's execution of a ordering document, delivery of the hardware and related components F.O.B. to the Project site, acceptance of the hardware and related components in accordance with the applicable ordering document, and receipt of a proper invoice for the hardware and related components.

  Hardware and related components will be paid within 30 days of receipt of a valid invoice, noting that the hardware and related components have been ordered, delivered, installed and accepted in the identified environment in accordance with the offeror's proposed Project Plan.

  The State will pay ongoing annual maintenance fees for any hardware and related components acquired as part of this Contract only on the State's execution of an ordering document on an annual basis within 30 days of receipt of a valid invoice. At the State's request, the first Support Period may be pro-rated so that the Anniversary Date coincides with the end of the State's Fiscal Year.

MBE Set-aside and Reporting. In the State's commitment to make more State contracts, services, benefits and opportunities available to minority business enterprises (MBE), the State included in the Evaluation Scoring Formula of this RFP, a provision for the offeror to seek and set aside work for MBE subcontractors. The work set-aside must equate to a minimum of 15% of the offeror's cost proposal under this RFP. In seeking bids, the offeror must:

- Utilize a competitive process to which only Ohio certified MBEs may respond;
- Have established criteria by which prospective MBEs will be evaluated including business ability and specific experience related to the work requirements;
- Require the MBE subcontractor to maintain their certification throughout the term of the Contract, including any renewals; and
- Propose the awarded MBE as a subcontractor under this RFP 0A1161.

After award of the RFP, the Contractor must submit a quarterly report to the DAS Contract Manager or designee documenting the work performed by and payments made to the MBE subcontractor. These reports must reflect the level of MBE commitment agreed to in the Contract. The reports must be filed at a time and in a form prescribed by the DAS Contract Manager or designee.

Notes:

1. For this RFP Ohio certified MBE's that are the prime **must** subcontract with an Ohio-certified MBE to meet the above requirement.
2. The offeror's MBE set-aside costs will be evaluated as a percentage (%) based on the offeror's proposed project management activities, deliverables and project services total costs. The Bill of Materials (BOM) elements, including proposed hardware, environmental software and application solution software costs will not be a component in the evaluation of MBE set-aside percentage.

Reimbursable Expenses. None.

Bill to Address. The State will provide the bill to address(s) after contract award. The bill to address may vary depending upon the work or services delivered.

Location of Data. The Contractor must perform all work on the Project and keep all State data within the United States, and the State may reject any Proposal that proposes to do any work or make State data available outside the United States. The State also may reject any Proposal for which the Contractor has not submitted the affirmation and disclosure form EXECUTIVE ORDER 2011-12K representing that it will ensure that all work on the Project will be done within the United States and that all State data will remain in the United States. Additionally, the Contractor must provide written notification for approval if at any time the location of work or data changes.

Interval Deliverable Agreement (IDA). The State may use the Interval Deliverable Agreement (IDA) model for work identified during the life of the Contract that cannot be defined to the appropriate level of detail during the RFP process. The Contractor must work with designated State staff to develop the deliverables and identify all work for each IDA. Deliverables or sub-deliverables will be defined prior to the start of each designated interval, and monitored throughout the designated interval and the life of the Contract. The IDAs will be identified and agreed to at least 30 days in advance of the beginning of the interval. For each IDA, the State and the Contractor will agree, in writing, to specific deliverables, work assignments, sub-deliverables, services to be provided using time and materials, the length of the interval, due dates, and Contractor staffing requirements based on positions and not-to-exceed hourly rates quoted in the Rate Card on the Cost Summary. The IDA is not effective until the State and Contractor have signed the agreement and a purchase order is issued to the Contractor. The agreed upon IDA will be incorporated into the Contract.

The IDA (i.e., specifications, deliverables, work assignments, and due dates) may be amended based upon changing circumstances during a particular interval. An amendment to an IDA must be in writing and signed by both the State and the Contractor prior to performing the work specified in the amendment.

Specific application of standards of performance and acceptance may be defined in an IDA. The information below sets a guide and general rule of thumb for these standards.

If the IDA so indicates, there will be a period for performance testing in a production environment specific to the deliverables identified in the IDA. Prior to the performance period, the State, with the assistance of the Contractor, will perform user acceptance testing. Specifics of the performance period such as the timeframe, resources, support required, entrance and exit performance criteria, and standards of performance will be determined by the State, negotiated with the Contractor and incorporated in the IDA. The performance criteria in the IDA may be supplemented with relevant user manuals, technical materials and related writings, to the extent that the specifications in those writings supplement and refine rather than contradict the performance criteria in the IDA. Acceptance of the Deliverable depends on a successful completion of the performance period defined in this section and the IDA. This section applies to the Deliverables defined in the IDA, and any part of it, as well as replacements or substitutes for the Deliverable after completion of a successful performance period.

If the Deliverable does not meet the standard of performance during the performance period, the State will document the issues in a timely manner and in a useful and relevant form. Until the Contractor has demonstrably corrected all outstanding problems, the performance period will not restart and the Deliverable (or part thereof) will not be accepted. The performance period will continue on a day-by-day basis until the standard of performance and exit criteria are met. The Contractor will not be compensated until the Deliverable is accepted and any additional cost associated with the iterations required to obtain acceptance are the responsibility of the Contractor.

If the work fails to meet the standard of performance and exit criteria during the performance period, the Contractor will be in default and will not have a cure period. In addition to all other remedies the State may have under this Contract, the State will have the right to request correction or replacement of the relevant portion of the IDA.

The work may have components that can be tested for acceptance individually. If so, there may be acceptance criteria listed in the IDA for each Deliverable that will be independently tested and accepted. But, unless the IDA expressly provides otherwise, the failure of any independently tested component to meet its acceptance criteria will give the State the right to reject the entire Deliverable. Alternatively, if the State determines that it is in the

State's interest to reject only the part of the Deliverable that was independently and unsuccessfully tested, it may do so. If the State chooses this option, the State will be entitled to a refund or credit toward the Contractor's Fee.

All IDAs must contain the following information, at a minimum:

- The designated interval length for each IDA.
- Goals and Objectives for the interval.
- Deliverables to be completed or partially completed during the interval. This will include, but not be limited to:
  - Deliverable Name;
  - Description of Deliverable including tasks or milestones to be completed; o Detailed acceptance criteria and standards of performance;
  - State dependencies identified by the Contractor for successful completion of the Deliverable; o Deliverable Due Date;
  - Risks associated with delays and incomplete Deliverables; and
  - Fixed pricing for each Deliverable based on staffing requirements (services to be performed, identification of Contractor staff resource by name and position, number of hours allocated to the task for each assigned position, individual hourly rate for each Contractor resource assigned to a task, etc.).

The State may identify tasks and services that will be billed on a time and material basis. The State does not anticipate a need for time and material services for this work, however in the event that time and materials work is appropriate, at the sole discretion of the State, the following information, at a minimum, must be provided in the IDA:

- Name, title, identification of the employer (prime or subcontractor) and number of staff;
- Staff work hours with any known exceptions noted;
- Description of the work to be performed by the Contractor;
- Specific Contractor resources assigned;
- Individual rate for each Contractor resource assigned;
- Projected number of Contractor hours allocated (per resource);
- Dates covered in the work;
- Dependencies;
- Management or staffing issues;
- Standards of performance; and
- Work Breakdown Schedule (WBS) for all work in the IDA.

In addition, the following information may also be required:

- Staffing Issues
- Required work related travel and training.

It is the Contractor's responsibility to provide qualified professionals to meet the goals, tasks, and objectives of each IDA.

The State's intent is for all IDAs to be developed and negotiated in partnership between the State and the Contractor, with each having a vested interest in its success

ATTACHMENT THREE: REQUIREMENTS FOR PROPOSALS

Proposal Format. These instructions describe the required format for a responsive Proposal. The offeror may include any additional information it believes is relevant. The offeror's proposal submission must be submitted using the Microsoft Word version of the RFP to provide an **in-line response** to the RFP. An identifiable tab sheet must precede each section of the Proposal, and each Proposal must follow the format outlined below. All pages, except pre-printed technical inserts, must be sequentially numbered. Any material deviation from the format outlined below may result in a rejection of the non-conforming Proposal.

Offeror responses should use a consistent contrasting color (**blue** is suggested to contrast with the black text of this document) to provide their response to each requirement so that the offeror response is readily distinguishable to the State. Below is an example of the required format for responding to the RFP requirements. To aid offerors in the creation of the most favorable depiction of their responses, alternative formats are acceptable that use typefaces, ***styles*** or shaded backgrounds, so long as the use of these formats are consistent throughout the offerors response and readily distinguishable from the baseline RFP. Alterations to the State provided baseline RFP language is strictly prohibited. The State will electronically compare offeror responses to the baseline RFP and deviations or alterations to the State's RFP requirements may result in a rejection of the offeror's Proposal.

To ensure that each Proposal addresses the required sections of the RFP, offerors must address each RFP requirement by section and sub-section heading and provide the offeror's proposed solution or response to the requirement by section and subsection **in-line** using the provided Microsoft Word version of this RFP.

Additionally, offerors must include the entire content of Attachment Four as a single section in their proposal. **Offerors must include a statement at the beginning of the section** indicating that the offeror has read, understands and agrees to the General Terms and conditions contained in Attachment Four.

***Illustrative Example*: Customers Served in the Widget Space:**

Instructions: *The offeror is to describe the customers (i.e., companies, agencies, entities, etc.) served in the Widget domain and the nature of the services provided, as well as the duration of the service.*

> ***Offeror Response:*** *The Acme Corporation has been in business for over 20 years, Acme is a leading supplier of Widget and Widget based services with clients in a variety of sectors including public (23 states) and private (125 of the Fortune 400).*

Each Proposal must include a response to every request for information in this attachment and Supplement 1 whether the request requires a simple "yes" or "no" or requires a detailed explanation. When a detailed response is required, simply repeating the RFP's requirement and agreeing to comply may be an unacceptable response and may cause the Proposal to be rejected.

Offerors are required to page limit their responses to Supplement 1 and Supplement 2 to be no longer than three times the State provided page count for Supplement 1 and 2. As offeror responses are to respond in an in-line format, and by way of example, as Supplement 1 is approximately 80 pages, the offeror's in-line response, inclusive of State requirements shall not exceed 240 pages in total. Offerors should choose a similarly sized typeface (generally 10 point for text and 8 point for tables) as are included in the State's requirements and not utilize smaller than 8 point fonts to work under this page limit restriction.

State evaluators read every RFP from front-to-back inclusive of all Attachments, Supplements, Forms and other elements. Offerors are advised to limit offeror marketing statements and positioning to the area(s) of the RFP applicable to those statement(s) and not include duplicative or otherwise repetitive statements throughout its response. This page limit shall not apply to: State mandatory forms, representations and affirmations, response form(s) and other structured forms required under this RFP.

Each Proposal must contain the following ***tabbed sections in the in-line response***:

Technical Proposal

1. Cover Letter
2. Supplier Information Form (OBM-5657)
3. Subcontractor Letters
4. Offeror Certification Form
5. MBE Certification(s)
6. Offeror Profile (as it relates to the proposed work)
7. Proposed Solution – Supplement 1 Response (Sections 2 through 14 in their entirety)
8. Acceptance of Supplement 2 – State Architecture and Computing Standards, Security and Privacy, IT Computing Policy and Data Handling Requirements.
9. Proof of Insurance
10. Payment Address
11. Legal Notice Address
12. W-9 Form
13. Independent Contractor Acknowledgement
14. Standard Affirmation and Disclosure Form (EO 2011-12K)
15. Acceptance of Attachment 4: General Terms and Conditions
16. Attachment 10: Master Contract for Software Licensing **(if applicable)**
17. Attachment 11: Master Cloud Services Agreement **(if applicable)**

Cost Proposal

Cost Summary - Microsoft Excel Workbook – Attachment Nine (must be separately sealed**, in native Excel format – not PDF**)

Cover Letter. The cover letter must be in the form of a standard business letter and must be signed by an individual authorized to legally bind the offeror. The cover letter must include a brief executive summary of the solution the offeror plans to provide. The letter must also have the following:

a. A statement regarding the offeror's legal structure (e.g., an Ohio corporation), Federal tax identification number, and principal place of business;
b. A list of the people who prepared the Proposal, including their titles; and
c. A statement certifying the Contractor is a business entity and will not submit the Independent Contractor/Worker Acknowledgement to the ordering agency.

Supplier Information Form. The offeror must submit a signed and completed Supplier Information Form (OBM-5657). The form is available at: http://ohiosharedservices.ohio.gov/Suppliers.aspx

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

1. The subcontractor's legal status, federal tax identification number, D-U-N-S number, and principal place of business address;
2. The name, phone number, fax number, email address, and mailing address of a person who is authorized to legally bind the subcontractor to contractual obligations;
3. A description of the work the subcontractor will do;
4. A commitment to do the work if the offeror is selected; and
5. A statement that the subcontractor has read and understood the RFP and will comply with the requirements of the RFP.

Offeror Certifications. The offeror must complete Attachment 6, Offeror Certification Form.

MBE Certification. Any offeror proposing an MBE subcontractor certified by the Department of Administrative Services pursuant to ORC 123.151 must provide a copy of their Ohio MBE Certification.

Offeror Profile. Each Supplement Response must include a description of the offeror capability, capacity, and experience in support of the requirements of each Supplements response. The description should include the date the offeror was established, its leadership, number of employees, number of employees the offeror will engage in tasks directly related to the Project, and any other background information or relevant experience that will help the State gauge the ability of the offeror to fulfill the obligations of the Contract.

The offeror must use the Offeror Profile Summary Form(s) (Attachment Seven) and fill them out completely to provide the required information. All offerors must demonstrate experience to meet each of the applicable mandatory requirement(s) evaluation criteria by including the offeror mandatory requirement form provided in this RFP. Each offeror must meet the applicable mandatory requirement(s) in the RFP. If an offeror does not meet the applicable mandatory requirement(s), the State may reject the offeror's Proposal as non-responsive.

The various sections of the Offeror Profile Summary Forms are described below:

a) **Mandatory Experience and Qualifications.** The offeror must complete this section to demonstrate that it has the experience needed to meet the RFP's mandatory requirements. For each reference, the offeror must provide the following information:

- Contact Information. The offeror must provide a client contact name, title, phone number, email address, company name, and mailing address. The offeror also must include the same information for an alternate client contact, in case the State cannot reach the primary contact. Failure to provide this information or providing information that is inaccurate or out of date may result in the State not including the reference in the evaluation process or rejecting the offeror's Proposal. The contact information given must be for a person within the client's organization and not a co-worker or a contact within the offeror's organization, subsidiaries, partnerships, etc.
- Project Name. The offeror must provide the name of the project where it obtained the mandatory experience.
- Dates of Experience. The offeror must complete this area with a beginning month and year and an ending month and year to show the length of time the offeror performed the work, not just the length of time the offeror was engaged by the reference.
- Description of the Related Service Provided. The State will not assume that, since the experience requirement is provided at the top of the page, all descriptions on that page relate to that requirement. The offeror must reiterate the experience being described, including the capacity in which the work was performed and the role of the offeror on the Project. It is the offeror's responsibility to customize the description to clearly substantiate the qualification.
- Description of how the related service shows the offeror's experience, capability, and capacity to develop the Deliverables and to achieve the milestones within the scope of work of this RFP.

The offeror must list each project experience separately and completely every time it is referenced, regardless of whether it is on the same or different pages of the form.

Proposed Solution – Supplement 1 Response. The offeror must describe in detail how its proposed solution meets the Work and requirements described in this RFP. The offeror may not simply state that the proposed services will meet or exceed the specified requirements. Instead, the offeror must provide a written narrative that shows that the offeror understands the requirements of this RFP and how the offeror's proposed services meets those requirements.

- All Supplements are being provided as a Microsoft Word through the State's procurement website as a convenience for responding to the RFP. The supplement's content must not be modified. If the content is modified, reformatted or omitted, the offeror's response may be disqualified. As part of their response, Offerors are to provide native Microsoft Word, Excel and Project based documents that comprise the requirements of a Supplement, inclusive of their response.
- Offerors must provide proposal responses to Sections 2 through 14 in their entirety of Supplement 1.

Acceptance of Supplement 2 – State Architecture and Computing Standards, Security and Privacy, IT Computing Policy and Data Handling Requirements. Offerors must include the entire content of Supplement 2 as a single section in their proposal. The offerors must include a statement at the beginning of the section indicating that the offeror has read, understands and agrees to the Requirements contained in Supplement 2.

Proof of Insurance. The offeror must provide the certificate of insurance required by Attachment Four. The policy may be written on an occurrence or claims made basis.

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

Legal Notice Address. The offeror must give the name, title, and address to which the State should send legal notices under the Contract.

W-9 Form. The offeror must complete a W-9 form in its entirety. The offeror must submit at least one originally signed W-9. All other copies of a Proposal may contain copies of the W-9. The offeror must indicate on the outside of the binder which Proposal contains the originally signed W-9. A current version of the Internal Revenue's W-9 form is available at: http://www.irs.gov/pub/irs-pdf/fw9.pdf

Independent Contractor Acknowledgement Form. Unless the offeror is a "business entity" as that term is defined in ORC. 145.037 ("an entity with five or more employees that is a corporation, association, firm, limited liability company, partnership, sole proprietorship, or other entity engaged in business"), the offeror must complete and submit an originally signed Independent Contractor Acknowledgement form in its entirety. All other copies of a Proposal may contain copies of the Independent Contractor Acknowledgement form. The offeror must indicate on the outside of the binder which Proposal contains the originally signed Independent Contractor Acknowledgement form. A current version of the Independent Contractor Acknowledgement form is available at: https://www.opers.org/forms-archive/PEDACKN.pdf

Standard Affirmation and Disclosure Form (EO 2011-12K). The offeror must complete and sign the Affirmation and Disclosure Form (Attachment Eight) as part of its Proposal. Executive Order 2011-12K is available at: http://www.governor.ohio.gov/Portals/0/pdf/executiveOrders/EO%202011-12K.pdf

Acceptance of Attachment Four – General Terms and Conditions. Offerors must include the entire content of Attachment Four as a single section in their proposal. The offerors must include a statement at the beginning of the section indicating that the offeror has read, understands and agrees to the General Terms and conditions contained in Attachment Four.

Proposed Changes to Attachment Ten (if applicable). The State requires the offeror to complete Attachment Ten, Master Contract for Software Licensing for each Commercial Software License proposed. If the offeror seeks changes to the Master Contract for Software Licensing, the offeror must identify those changes, with the precise alternative language the offeror seeks, and include the markup of the Master Contract for Software Licensing as an attachment to its Proposal. Generalized objections to the Master Contract for Software Licensing's terms and conditions are not acceptable. The State may reject any Proposal with extensive changes to the Master Contract for Software Licensing or with changes that the State finds objectionable. Alternatively, the State may seek to negotiate over proposed changes to attempt to make them acceptable to the State. The State, in its sole and exclusive judgment, will determine whether any changes are acceptable and whether any negotiations make the proposed changes acceptable to the State.

Proposed Changes to Attachment Eleven (if applicable). The State requires the offeror to complete Attachment Eleven, the Master Cloud Services Agreement (MCSA). If the offeror seeks changes to the MCSA, the offeror must identify those changes, with the precise alternative language the offeror seeks, and include the markup of the MCSA as an attachment to its Proposal. Generalized objections to the MCSA's terms and conditions are not acceptable. The State may reject any Proposal with extensive changes to the MCSA or with changes that the State finds objectionable. Alternatively, the State may seek to negotiate over proposed changes to attempt to make them acceptable to the State. The State, in its sole and exclusive judgment, will determine whether any changes are acceptable and whether any negotiations make the proposed changes acceptable to the State.

Cost Summary (must be separately sealed package). This RFP includes Cost Summary Workbooks in Microsoft Excel® as Attachments Nine. Offerors may not reformat the State's Cost Summary Workbooks. Each offeror must complete the applicable Cost Summary Workbooks in the exact format provided, since the State may

reject any Proposal with a reformatted Cost Summary Workbook or that is not separately sealed. (See: Part Three: General Instructions, Proposal Submittal.)

In addition, offerors must indicate the MBE cost and percentage for each element of the offeror's proposed cost utilizing the Cost Summary Workbook. The total MBE cost will be the sum of all MBE elements in the Cost Summary Workbook. The percentage will be the total MBE cost divided by the total offeror proposed cost.

Note: MBE percentage will be calculated based on the offeror's proposed project management services and solution project implementation services.

The Cost Summary Workbook must not include exceptions, additional terms and conditions, or assumptions.

The offeror's total cost for all the Project must be represented as the Not-To-Exceed Fixed Price.

The State will not be liable for or pay any Project costs that the offeror does not identify in its Proposal.

ATTACHMENT FOUR: GENERAL TERMS AND CONDITIONS

PART ONE: PERFORMANCE AND PAYMENT

Statement of Work. The selected offeror's Proposal and the State's Request for Proposal (collectively, the "RFP Documents") are a part of this Contract and describe the work (the "Project") the Contractor must do and any materials the Contractor must deliver (the "Deliverables") under this Contract. The Contractor must do the Project in a professional, timely, and efficient manner and must provide the Deliverables in a proper fashion. The Contractor also must furnish its own support staff necessary for the satisfactory performance of the Project.

The Contractor must consult with the appropriate State representatives and others necessary to ensure a thorough understanding of the Project and satisfactory performance. The State may give instructions to or make requests of the Contractor relating to the Project, and the Contractor must comply with those instructions and fulfill those requests in a timely and professional manner. Those instructions and requests will be for the sole purpose of ensuring satisfactory completion of the Project and will not amend or alter the scope of the Project.

Term. Unless this Contract is terminated or expires without renewal, it will remain in effect until the Project is completed to the satisfaction of the State, including all optional renewal periods for maintenance or continuing commitments, and the Contractor is paid. However, the current General Assembly cannot commit a future General Assembly to an expenditure. Therefore, this Contract will automatically expire at the end of each biennium, the first of which is June 30, 2017. The State may renew this Contract in the next biennium by issuing written notice to the Contractor of the decision to do so. This expiration and renewal procedure also will apply to the end of any subsequent biennium during which the Project continues, including any optional renewal periods. Termination or expiration of this Contract will not limit the Contractor's continuing obligations with respect to Deliverables that the State paid for before or after termination or limit the State's rights in such.

The State's funds are contingent upon the availability of lawful appropriations by the Ohio General Assembly. If the General Assembly fails to continue funding for the payments and other obligations due as part of this Contract, the State's obligations under this Contract will terminate as of the date that the funding expires without further obligation of the State.

The Project has a completion date that is identified in the RFP Documents. The RFP Documents also may have several dates for the delivery of Deliverables or reaching certain milestones in the Project. The Contractor must make those deliveries, meet those milestones, and complete the Project within the times the RFP Documents require. If the Contractor does not meet those dates, the Contractor will be in default, and the State may terminate this Contract under the termination provision contained below.

The State also may have certain obligations to meet. Those obligations, if any, are also listed in the RFP Documents. If the State agrees that the Contractor's failure to meet the delivery, milestone, or completion dates in the RFP Documents is due to the State's failure to meet its own obligations in a timely fashion, then the Contractor will not be in default, and the delivery, milestone, and completion dates affected by the State's failure to perform will be extended by the same amount of time as the State's delay. The Contractor may not rely on this provision unless the Contractor has in good faith exerted reasonable management skill to avoid an extension and has given the State meaningful written notice of the State's failure to meet its obligations within five business days of the Contractor's realization that the State's delay may impact the Project. The Contractor must deliver any such notice to both the Project Representative and Procurement Representative and title the notice as a "Notice of State Delay." The notice must identify any delay in detail, as well as the impact the delay has or will have on the Project. Unless the State decides, in its sole and exclusive judgment, that an equitable adjustment in the Contractor's Fee is warranted in the case of an extended delay, an extension of the Contractor's time to perform will be the Contractor's exclusive remedy for the State's delay. Should the State determine that an equitable adjustment in the Contractor's Fee is warranted, the equitable adjustment will be handled as a Change Order under the Changes Section of this Contract, and the extension of time and equitable adjustment will be the exclusive remedies of the Contractor for the State's delay.

The State seeks a complete project, and the Contractor must provide any incidental items omitted in the RFP Documents as part of the Contractor's not-to-exceed fixed price. The Contractor also must fully identify, describe, and document all systems that are delivered as a part of the Project. Unless expressly excluded elsewhere in the RFP, all hardware, software, supplies, and other required components (such as documentation, conversion,

training, and maintenance) necessary for the Project to be complete and useful to the State are included in the Project and the not-to-exceed fixed price.

Compensation. In consideration of the Contractor's promises and satisfactory performance, the State will pay the Contractor the amount(s) identified in the RFP Documents (the "Fee"), plus any other expenses identified as reimbursable in the RFP Documents. In no event, however, will payments under this Contract exceed the “total not-to-exceed” amount in the RFP Documents without the prior written approval of the State and, when required, the Ohio Controlling Board and any other source of funding. The Contractor's right to the Fee is contingent on the complete and satisfactory performance of the Project or, in the case of milestone payments or periodic payments of an hourly, daily, weekly, monthly, or annual rate, all relevant parts of the Project tied to the applicable milestone or period. Payment of the Fee also is contingent on the Contractor delivering a proper invoice and any other documents the RFP Documents require. An invoice must comply with the State's then current policies regarding invoices and their submission. The State will notify the Contractor in writing within 15 business days after it receives a defective invoice of any defect and provide the information necessary to correct the defect.

The Contractor must send all invoices under this Contract to the “bill to” address in the RFP Documents or in the applicable purchase order.

The State will pay the Contractor interest on any late payment, as provided in Section 126.30 of the Ohio Revised Code (the "Revised Code"). If the State disputes a payment for anything covered by an invoice, within 15 business days after receipt of that invoice, the State will notify the Contractor, in writing, stating the grounds for the dispute. The State then may deduct the disputed amount from its payment as a nonexclusive remedy. If the Contractor has committed a material breach, in the sole opinion of the State, the State also may withhold payment otherwise due to the Contractor. Both parties will attempt to resolve any claims of material breach or payment disputes through discussions among the Contractor’s Implementation Manager (e.g., Contractor’s Project Manager), the Contractor’s Project executive, the State’s Project Representative, and the State Contract Management Administrator. The State will consult with the Contractor as early as reasonably possible about the nature of the claim or dispute and the amount of payment affected. When the Contractor has resolved the matter to the State's satisfaction, the State will pay the disputed amount within 30 business days after the matter is resolved. The State has no obligation to make any disputed payments until the matter is resolved, and the Contractor must continue its performance under this Contract pending resolution of the dispute or claim.

If the State has already paid the Contractor on an invoice but later disputes the amount covered by the invoice, and if the Contractor fails to correct the problem within 30 calendar days after written notice, the Contractor must reimburse the State for that amount at the end of the 30 calendar days as a nonexclusive remedy for the State. On written request from the Contractor, the State will provide reasonable assistance in determining the nature of the problem by giving the Contractor reasonable access to the State’s facilities and any information the State has regarding the problem.

Payment of an invoice by the State will not prejudice the State’s right to object to or question that or any other invoice or matter in relation thereto. The Contractor’s invoice will be subject to reduction for amounts included in any invoice or payment made which are determined by the State not to constitute allowable costs, on the basis of audits conducted in accordance with the terms of this Contract. At the State’s sole discretion all payments shall be subject to reduction for amounts equal to prior overpayments to the Contractor.

If the RFP Documents provide for any retainage, the State will withhold from each invoice paid the percentage specified in the RFP Documents as retainage. The State will pay the retainage only after the State has accepted the Project, and then only in accordance with the payment schedule specified in the RFP Documents. The State will withhold all amounts under this section arising from claims or disputes in addition to any retainage specified in the RFP Documents.

The State may pay any part of the not-to-exceed fixed price identified in the RFP documents as being for a license in Commercial Material from a third party in accordance with the applicable license agreement, if the license agreement addresses payment. For all Key Commercial Software with a license agreement substantially in the form of Attachment Twelve, payment of any license or support fees will be governed exclusively by that license agreement.

Reimbursable Expenses. The State will pay all reimbursable expenses identified in the RFP Documents, if any, in accordance with the terms in the RFP Documents and, where applicable, Section 126.31 of the Revised Code.

The Contractor must assume all expenses that it incurs in the performance of this Contract that are not identified as reimbursable in the RFP Documents.

In making any reimbursable expenditure, the Contractor always must comply with the more restrictive of its own, then current internal policies for making such expenditures or the State's then current policies. All reimbursable travel will require the advance written approval of the State's Project Representative. The Contractor must bill all reimbursable expenses monthly, and the State will reimburse the Contractor for them within 30 business days of receiving the Contractor's invoice.

Right of Offset. The State may set off the amount of any Ohio tax liability, liquidated damages or other damages or claims for damages, or other obligation of the Contractor or its subsidiaries to the State, including any amounts the Contractor owes to the State under this or other contracts, against any payments due from the State to the Contractor under this or any other contracts with the State.

Certification of Funds. None of the rights, duties, or obligations in this Contract will be binding on the State, and the Contractor will not begin its performance until all the following conditions have been met:

(a) All statutory provisions under the Revised Code, including Section 126.07, have been met;
(b) All necessary funds are made available by the appropriate State entities;
(c) If required, the Controlling Board of Ohio approves this Contract; and
(d) If the State is relying on federal or third-party funds for this Contract, the State gives the Contractor written notice that such funds are available.

Employment Taxes. All people furnished by the Contractor (the “Contractor Personnel”) are employees or subcontractors of the Contractor, and none are or will be deemed employees or contractors of the State. No Contractor Personnel will be entitled to participate in, claim benefits under, or become an “eligible employee” for purposes of any employee benefit plan of the State by reason of any work done under this Contract. The Contractor will pay all federal, state, local, and other applicable payroll taxes and make the required contributions, withholdings, and deductions imposed or assessed under any provision of any law and measured by wages, salaries, or other remuneration paid by or which may be due from the Contractor to the Contractor Personnel. The Contractor will indemnify, defend (with the consent and approval of the Ohio Attorney General), and hold the State harmless from and against all claims, losses, liability, demands, fines, and expense (including court costs, defense costs, and redeemable attorney fees) arising out of or relating to such taxes, withholdings, deductions, and contributions with respect to the Contractor Personnel. The Contractor’s indemnity and defense obligations also apply to any claim or assertion of tax liability made by or on behalf of any Contractor Personnel or governmental agency on the basis that any Contractor Personnel are employees or contractors of the State, that the State is the “joint employer” or “co-employer” of any Contractor Personnel, or that any Contractor Personnel are entitled to any employee benefit offered only to eligible regular fulltime or regular part-time employees of the State.

Sales, Use, Excise, and Property Taxes. The State is exempt from any sales, use, excise, and property tax. To the extent sales, use, excise, or any similar tax is imposed on the Contractor in connection with the Project, such will be the sole and exclusive responsibility of the Contractor. Further, the Contractor will pay such taxes, together with any interest and penalties not disputed with the appropriate taxing authority, whether they are imposed at the time the services are rendered or a later time.

PART TWO: WORK AND CONTRACT ADMINISTRATION

Related Contracts. The Contractor warrants that the Contractor has not and will not enter into any contracts without written approval of the State to perform substantially identical services for the State, such that the Project duplicates the work done or to be done under the other contracts.

Other Contractors. The State may hold other contracts for additional or related work, including among others independent verification and validation (IV&V) work for this Project. The Contractor must fully cooperate with all other contractors and State employees and coordinate its work with such other contractors and State employees as may be required for the smooth and efficient operation of all related or additional work. The Contractor may not act in any way that may unreasonably interfere with the work of any other contractors or the State’s employees. Further, the Contractor must fully cooperate with any IV&V contractor assigned to this Project. Such cooperation includes expeditiously providing the IV&V contractor with full and complete access to all project work

product, records, materials, personnel, meetings, and correspondence as the IV&V contractor may request. If the State assigns an IV&V contractor to the Project, the State will obligate the IV&V contractor to a confidentiality provision similar to the Confidentiality Section contained in this Contract. Additionally, the Contractor must include the obligations of this provision in all its contracts with its subcontractors that work on this project.

Subcontracting. The Contractor may not enter into subcontracts related to the Project after award without written approval from the State. Nevertheless, the Contractor will not need the State's written approval to subcontract for the purchase of commercial goods that are required for satisfactory completion of the Project. All subcontracts will be at the sole expense of the Contractor unless expressly stated otherwise in the RFP Documents.

The State's approval of the use of subcontractors does not mean that the State will pay for them. The Contractor will be solely responsible for payment of its subcontractor and any claims of subcontractors for any failure of the Contractor or any of its other subcontractors to meet the performance schedule or performance specifications for the Project in a timely and professional manner. The Contractor must hold the State harmless for and must indemnify the State against any such claims.

The Contractor assumes responsibility for all Deliverables whether it, a subcontractor, or third-party manufacturer produces them in whole or in part. Further, the Contractor will be the sole point of contact with regard to contractual matters, including payment of all charges resulting from the Contract. Further, the Contractor will be fully responsible for any default by a subcontractor, just as if the Contractor itself had defaulted.

If the Contractor uses any subcontractors, each subcontractor must have a written agreement with the Contractor. That written agreement must incorporate this Contract by reference. The agreement also must pass through to the subcontractor all provisions of this Contract that would be fully effective only if they bind both the subcontractor and the Contractor. Among such provisions are the limitations on the Contractor's remedies, the insurance requirements, record keeping obligations, and audit rights. Some sections of this Contract may limit the need to pass through their requirements to subcontracts to avoid placing cumbersome obligations on minor subcontractors. This exception is applicable only to sections that expressly provide an exclusion for small-dollar subcontracts. Should the Contractor fail to pass through any provisions of this Contract to one of its subcontractors and the failure damages the State in any way, the Contractor must indemnify the State for the damage.

Record Keeping. The Contractor must keep all financial records in accordance with generally accepted accounting principles or equivalent consistently applied. The Contractor also must file documentation to support each action under this Contract in a manner allowing the documentation to be readily located. Additionally, the Contractor must keep all Project-related records and documents at its principal place of business or at its office where the work was performed.

Audits. During the term of this Contract and for three years after the payment of the Contractor’s Fee, on reasonable notice, and during customary business hours, the State may audit the Contractor’s records and other materials that relate to the Project. This audit right also applies to the State’s duly authorized representatives and any person or organization providing financial support for the Project. State audit rights will apply to those Contractor materials that are required to verify the accuracy of a Contractor invoice to the State inclusive of: Contractor personnel timesheets; Contractor purchased or provided equipment for benefit of the State that will remain in the State’s possession; State deliverable acceptance documentation; any required State written approvals as required herein; final Work products and deliverables; any partial or incomplete Work products or deliverables that should the Contractor submit for partial compensation from the State as a result of termination of this contract.

Right to Terminate as a Result of Audit Findings. In the event the State determines that the results of any examination of the Contractor is unsatisfactory per the requirements of the Contract and not remedied within a 90 day period following written notice from the State, the State may terminate this Agreement, in part or in full.

If the Contractor fails to satisfy the requirements of the State with regard to security of information, or if an examination reveals information that would result in a continuing contractual relationship that causes the State to be in violation of any law, the State may terminate this Contract immediately without notice.

If the Contractor fails to satisfy the requirements of the State with regard to matters not related to items contained in the preceding two (2) paragraphs, the State will provide Contractor with notice and an opportunity to cure the

failure within forty-five (45) days. If the failure is not cured by Contractor within such forty-five (45) day period, the State may terminate this Contract without further notice.

Insurance. The Contractor must provide the following insurance coverage at its own expense throughout the term of this Contract:

(a) Workers' compensation insurance, as required by Ohio law, and, if some of the Project will be done outside Ohio, the laws of the appropriate state(s) where work on the project will be done. The Contractor also must maintain employer's liability insurance with at least a $1,000,000.00 limit.

(b) Commercial General Liability insurance coverage for bodily injury, personal injury, wrongful death, and property damage. The defense cost must be outside of the policy limits. Such policy must designate the State of Ohio as an additional insured, as its interest may appear. The policy also must be endorsed to include a waiver of subrogation. At a minimum, the limits of the insurance must be:

$ 2,000,000 General Aggregate
$ 2,000,000 Products/Completed Operations Aggregate
$ 1,000,000 Per Occurrence Limit
$ 1,000,000 Personal and Advertising Injury Limit
$ 100,000 Fire Legal Liability
$ 10,000 Medical Payments

The Contractor shall, for each policy required by this Contract, provide the State with 30-days prior written notice of cancellation, material change, or non-renewal, except a 10-days notice of non-payment of premium. And the Contractor's Commercial General Liability must be primary over any other insurance coverage.

(c) Commercial Automobile Liability insurance with a combined single limit of $500,000.

(d) Professional Liability insurance covering all staff with a minimum limit of $1,000,000 per incident and $3,000,000 aggregate. If the Contractor's policy is written on a "claims made" basis, the Contractor must provide the State with proof of continuous coverage at the time the policy is renewed. If for any reason the policy expires, or coverage is terminated, the Contractor must purchase and maintain "tail" coverage through the applicable statute of limitations.

The certificate(s) must be in a form that is reasonably satisfactory to the State as to the contents of the policies and the quality of the insurance carriers. All carriers must have at least an "A-" rating by A.M. Best.

Replacement Personnel. If the RFP Documents contain the names of specific people (e.g., Key Project Personnel) who will work on the Project, then the quality and professional credentials of those people were material factors in the State's decision to enter into this Contract. Therefore, the Contractor must use all commercially reasonable efforts to ensure the continued availability of those people. Also, the Contractor may not remove those people from the Project without the prior written consent of the State, except as provided below.

The Contractor may remove a person listed in the RFP Documents from the Project, if doing so is necessary for legal or disciplinary reasons. However, the Contractor must make a reasonable effort to give the State 30 calendar days' prior, written notice of the removal.

If the Contractor removes a person listed in the RFP Documents from the Project for any reason other than those specified above, the State may assess liquidated damages in the amount of $1,500.00 for every day between the date on which the individual was removed and the date that this Contract is terminated or the individual's qualified replacement, selected in accordance with the process identified in this section, starts performing on the Project. The State also may provide the Contractor with written notice of its default under this section, which the Contractor must cure within 30 days. Should the Contractor fail to cure its default within the 30 day cure period, this Contract will terminate immediately for cause, and the State will be entitled to damages in accordance with the Suspension and Termination Section of this Contract due to the termination. Should the State assess

liquidated damages or otherwise be entitled to damages under this provision, it may offset these damages from any Fees due under this Contract.

The Contractor must have qualified replacement people available to replace any people listed in the RFP Documents by name or identified as a key individual on the Project. When the removal of a listed person is permitted under this Section, or if a person becomes unavailable, the Contractor must submit the resumes for two replacement people to the State for each person removed or who otherwise becomes unavailable. The Contractor must submit the two resumes, along with such other information as the State may reasonably request, within five business days after the decision to remove a person is made or the unavailability of a listed person becomes known to the Contractor.

The State will select one of the two proposed replacements or will reject both of them within ten business days after the Contractor has submitted the proposed replacements to the State. The State may reject the proposed replacements for any legal reason. Should the State reject both replacement candidates due to their failure to meet the minimum qualifications identified in the RFP Documents, or should the Contractor fail to provide the notice required under this Section or fail to provide two qualified replacement candidates for each removed or unavailable person, the Contractor will be in default and the cure period for default specified elsewhere in this Contract will not apply. In any such case, the State will have the following options:

(a) The State may assess liquidated damages in the amount of $1,500.00 for every day between the date on which the Contractor failed to provide the applicable notice, failed to provide the two replacement candidates, or the date the State rejected all candidates for cause and the date on which the Contractor affects a cure or the Contract expires without renewal or is terminated.
(b) The State may terminate this Contract immediately for cause and without any cure period.

Should the State exercise its option under item (a) above, it nevertheless will be entitled anytime thereafter to exercise its option under item (b) above. Additionally, should the State terminate this Contract under this provision, it will be entitled to damages in accordance with the Suspension and Termination Section of this Contract due to the termination. Should the State assess liquidated damages or otherwise be entitled to damages under this provision, it may offset these damages from any Fees due under this Contract.

The State may determine that the proposed replacement candidates meet the minimum qualifications of this Contract and still substantially reduce the value the State perceived it would receive through the effort of the original individual(s) the Contractor proposed and on whose credentials the State decided to enter into this Contract. Therefore, the State will have the right to reject any candidate that the State determines may provide it with diminished value.

Should the State reject both proposed candidates for any legal reason other than their failure to meet the minimum qualifications identified in the RFP Documents, the State may terminate this Contract for its convenience.

The State has an interest in providing a healthy and safe environment for its employees and guests at its facilities. The State also has an interest in ensuring that its operations are carried out in an efficient, professional, legal, and secure manner. Therefore, the State will have the right to require the Contractor to remove any individual involved in the Project, if the State determines that any such individual has or may interfere with the State's interests identified above. In such a case, the request for removal will be treated as a case in which an individual providing services under this Contract has become unavailable, and the Contractor must follow the procedures identified above for replacing unavailable people. This provision also applies to people that the Contractor's subcontractors engage, if they are listed by name or as a key person in the RFP Documents.

Replacement Personnel Background Checks. All Contractor and subcontractor personnel assigned to the Identity Validation, Authentication and Fraud Services Project who may have access to sensitive or confidential information or to sensitive State systems must have a current fingerprint search and background check performed by the Federal Bureau of Investigation or other Federal investigative authority. The fingerprint search and background checks must be completed before any such Contractor or subcontractor personnel gain access to State facilities, sensitive and/or confidential information or systems. All costs associated with this requirement will be at the Contractor’s expense. At its discretion, the State may reject any Contractor or subcontractor personnel based on the information provided in the completed background check.

Suspension and Termination. The State may terminate this Contract in full or in part for cause if the Contractor defaults in meeting its obligations under this Contract and fails to cure its default within the time allowed by this Contract, or if a petition in bankruptcy (or similar proceeding) has been filed by or against the Contractor. The State also may terminate this Contract if the Contractor violates any law or regulation in doing the Project, or if it appears to the State that the Contractor's performance is substantially endangered through no fault of the State. In any such case, the termination will be for cause, and the State's rights and remedies will be those identified below for termination for cause.

On written notice, the Contractor will have 30 calendar days to cure any breach of its obligations under this Contract, provided the breach is curable. If the Contractor fails to cure the breach within 30 calendar days after written notice, or if the breach is not one that is curable, the State will have the right to terminate this Contract immediately on notice to the Contractor. The State also may terminate this Contract in the case of breaches that are cured within 30 calendar days but are persistent. "Persistent" in this context means that the State has notified the Contractor in writing of the Contractor's failure to meet any of its obligations three times. After the third notice, the State may terminate this Contract on written notice to the Contractor without a cure period if the Contractor again fails to meet any obligation. The three notices do not have to relate to the same obligation or type of failure. Some provisions of this Contract may provide for a shorter cure period than 30 calendar days or for no cure period at all, and those provisions will prevail over this one. If a particular section does not state what the cure period will be, this provision will govern.

The State also may terminate this Contract in full or in part for its convenience and without cause or if the Ohio General Assembly fails to appropriate funds for any part of the Project. If a third party is providing funding for the Project, the State also may terminate this Contract should that third party fail to release any Project funds. The RFP Documents normally identify any third party source of funds for the Project, but an absence of such in the RFP Documents will not diminish the State’s rights under this section.

The notice of termination, whether for cause or without cause, will be effective as soon as the Contractor receives it. Upon receipt of the notice of termination, the Contractor must immediately cease all work on the project and take all steps necessary to minimize any costs the Contractor will incur related to this Contract. The Contractor also must immediately prepare a report and deliver it to the State. The report must be all-inclusive and must detail the work completed at the date of termination, the percentage of the Project's completion, any costs incurred in doing the Project to that date, and any Deliverables completed or partially completed but not delivered to the State at the time of termination. The Contractor also must deliver all the completed and partially completed Deliverables to the State with its report. However, if the State determines that delivery in that manner would not be in its interest, then the State will designate a suitable alternative form of delivery, which the Contractor must honor.

If the State terminates this Contract for cause, the State will be entitled to cover for the Work by using another Contractor on such commercially reasonable terms as the State and the covering contractor may agree. The Contractor will be liable to the State for all costs related to covering for the Work to the extent that such costs, when combined with payments already made to the Contractor for the Work before termination, exceed the costs that the State would have incurred under this Contract. The Contractor also will be liable for any other direct damages resulting from its breach of this Contract or other action leading to termination for cause. If the Contractor fails to deliver Deliverables or provide satisfactory services, the State has the right to withhold any and all payments due to the Contractor without penalty or work stoppage by the Contractor until such failure to perform is cured.

If the termination is for the convenience of the State, the Contractor will be entitled to the Contract price as prorated by the State Contract price for deliverables, products or services accepted by the State and not previously paid for provided in that in no event will total payments exceed the amount payable to the Contractor is the Contract had been fully performed. For items not specifically priced, the State will use fair market value to determine the price owed. The Contractor will use generally accepted accounting principles or equivalent and sound business practices in determining all costs claimed, agreed to, or determined under this clause.

The State will have the option of suspending this Contract in full or in part rather than terminating the Project, if the State believes that doing so would better serve its interests. In the event of a suspension for the convenience of the State, the Contractor will be entitled to receive payment for the work performed before the suspension. In the case of suspension of the Project for cause rather than termination for cause, the Contractor will not be entitled to any compensation for any work performed. If the State reinstates the Project after suspension for cause, rather than terminating this Contract after the suspension, the Contractor may be entitled to compensation

for work performed before the suspension, less any damage to the State resulting from the Contractor's breach of this Contract or other fault. Any amount due for work before or after the suspension for cause will be offset by any damage to the State from the default or other event giving rise to the suspension.

In the case of a suspension for the State's convenience, the State will calculate the amount of compensation due to the Contractor for work performed before the suspension in the same manner as provided in this section for termination for the State's convenience. The Contractor will not be entitled to compensation for any other costs associated with a suspension for the State's convenience, and the State will make no payment under this provision to the Contractor until the Contractor submits a proper invoice. If the State decides to allow the work to continue rather than terminating this Contract after the suspension, the State will not be required to make any payment to the Contractor other than those payments specified in this Contract and in accordance with the payment schedule specified in this Contract for properly completed work.

Any notice of suspension, whether with or without cause, will be effective immediately on the Contractor's receipt of the notice. The Contractor will prepare a report concerning the Project just as is required by this Section in the case of termination. After suspension of the Project, the Contractor may not perform any work without the consent of the State and may resume work only on written notice from the State to do so. In any case of suspension, the State retains its right to terminate this Contract rather than to continue the suspension or resume the Project.

The State may not suspend the Project for its convenience more than twice during the term of this Contract, and any suspension for the State's convenience may not continue for more than 30 calendar days. If the Contractor does not receive notice to resume or terminate the Project within the 30-day suspension, then this Contract will terminate automatically for the State's convenience at the end of the 30 calendar day period.

Any default by the Contractor or one of its subcontractors will be treated as a default by the Contractor and all of its subcontractors. The Contractor will be solely responsible for satisfying any claims of its subcontractors for any suspension or termination and must indemnify the State for any liability to them. Notwithstanding the foregoing, each subcontractor must hold the State harmless for any damage caused to them from a suspension or termination. They must look solely to the Contractor for any compensation to which they may be entitled.

Representatives. The State's representative under this Contract will be the person identified in the RFP Documents or in a subsequent notice to the Contractor as the "Project Representative." The Project Representative will review all reports the Contractor makes in the performance of the Project, will conduct all liaison with the Contractor, and will accept or reject the Deliverables and the completed Project. The Project Representative may delegate his responsibilities for individual aspects of the Project to one or more managers, who may act as the Project Representative for those individual portions of the Project.

The Contractor's Implementation Manager under this Contract will be the person identified on the RFP Documents as the "Implementation Manager." The Implementation Manager will be the Contractor's liaison with the State under this Contract. The Implementation Manager also will conduct all Project meetings and prepare and submit to the Project Representative all reports, plans, and other materials that the RFP Documents require from the Contractor.

Either party, upon written notice to the other party, may designate another representative. However, the Contractor may not replace the Implementation Manager without the approval of the State if that person is identified in the RFP Documents by name or as a key individual on the Project.

Project Responsibilities. The State will be responsible for providing only those things, if any, expressly identified in the RFP Documents. If the State has agreed to provide facilities or equipment, the Contractor, by signing this Contract, warrants that the Contractor has either inspected the facilities and equipment or has voluntarily waived an inspection and will work with the equipment and facilities on an "as is" basis.

The Contractor must assume the lead in the areas of management, design, and development of the Project. The Contractor must coordinate the successful execution of the Project and direct all Project activities on a day-to-day basis, with the advice and consent of the Project Representative. The Contractor will be responsible for all communications regarding the progress of the Project and will discuss with the Project Representative any issues, recommendations, and decisions related to the Project.

If any part of the Project requires installation on the State's property, the State will provide the Contractor with reasonable access to the installation site for the installation and any site preparation that is needed. After the installation is complete, the Contractor must complete an installation letter and secure the signature of the Project Representative certifying that installation is complete and the Project, or applicable portion of it, is operational. The letter must describe the nature, date, and location of the installation, as well as the date the Project Representative certified the installation as complete and operational.

Unless otherwise provided in the RFP Documents, the Contractor is solely responsible for obtaining all official permits, approvals, licenses, certifications, and similar authorizations required by any local, state, or federal agency for the Project and maintaining them throughout the duration of this Contract.

Changes. The State may make reasonable changes within the general scope of the Project. The State will do so by issuing a written order under this Contract describing the nature of the change ("Change Order"). Additionally, if the State provides directions or makes requests of the Contractor without a change order, and the Contractor reasonably believes the directions or requests are outside the specifications for the Project, the Contractor may request a Change Order from the State. The parties will handle such changes as follows: The Contractor will provide pricing to the State. The State will execute a Change Order once it and the Contractor have agreed on the description of and specifications for the change, as well as any equitable adjustments that need to be made in the Contractor's Fee or the performance schedule for the work. Then within five business days after receiving the Change Order, the Contractor must sign it to signify agreement with it.

If a change causes an increase in the cost of, or the time required for, the performance of the Project, the Contractor must notify the State in writing and request an equitable adjustment in its Fee, the delivery schedule, or both before the Contractor signs the Change Order. If the Contractor claims an adjustment under this section in connection with a change to the Project not described in a written Change Order, the Contractor must notify the State in writing of the claim within five business days after the Contractor is notified of the change and before work on the change begins. Otherwise, the Contractor will have waived the claim. In no event will the State be responsible for any increase in the Fee or revision in any delivery schedule unless the State expressly ordered the relevant change in writing and the Contractor has complied with the requirements of this section. Provided the State has complied with the procedure for Change Orders in this section, nothing in this clause will excuse the Contractor from proceeding with performance of the Project, as changed.

Where an equitable adjustment to the Contractor's Fee is appropriate, the State and the Contractor may agree upon such an adjustment. If the State and the Contractor are unable to agree, either party may submit the dispute to the senior management of the Contractor and the senior management of the State's Department of Administrative Services for resolution. If within 30 calendar days following referral to senior management, the claim or dispute has not been resolved, the Contractor must submit its actual costs for materials needed for the change (or estimated amount if the precise amount of materials cannot be determined) and an estimate of the hours of labor required to do the work under the Change Order. The Contractor must break down the hours of labor by employee position, and provide the actual hourly pay rate for each employee involved in the change. The total amount of the equitable adjustment for the Change Order then will be made based on the actual cost of materials (or estimated materials) and actual rate for each person doing the labor (based on the estimated hours of work required to do the change). Labor rates will be increased by 25% to cover benefits and taxes. The equitable adjustment for the Change Order then will be set based on this amount, plus 15% to cover overhead and profit. This amount will be the not-to-exceed amount of the Change Order. If the change involves removing a requirement from the Project or replacing one part of the Project with the change, the State will get a credit for the work no longer required under the original scope of the Project. The credit will be calculated in the same manner as the Contractor's Fee for the change, and the not-to-exceed amount will be reduced by this credit.

The Contractor is responsible for coordinating changes with its subcontractors and adjusting their compensation and performance schedule. The State will not pay any subcontractor for the Change Order. If a subcontractor will perform any work under a Change Order, that work must be included in the Contractor's not-to-exceed amount and calculated in the same manner as the Contractor's equitable adjustment for the portion of the work the Contractor will perform. The Contractor will not receive an overhead percentage for any work a subcontractor will do under a Change Order.

If the RFP Documents provide for the retainage of a portion of the Contractor's Fee, all equitable adjustments for Change Orders also will be subject to the same retainage, which the State will pay only on completion and acceptance of the Project, as provided in the RFP Documents.

Excusable Delay. Neither party will be liable for any delay in its performance that arises from causes beyond its control and without its negligence or fault. The delayed party must notify the other promptly of any material delay in performance and must specify in writing the proposed revised performance date as soon as practicable after notice of delay. In the event of any such excusable delay, the date of performance or of delivery will be extended for a period equal to the time lost by reason of the excusable delay. The delayed party also must describe the cause of the delay and what steps it is taking to remove the cause. The delayed party may not rely on a claim of excusable delay to avoid liability for a delay if the delayed party has not taken commercially reasonable steps to mitigate or avoid the delay. Things that are controllable by the Contractor's subcontractors will be considered controllable by the Contractor, except for third-party manufacturers supplying commercial items and over whom the Contractor has no legal control.

Independent Contractor Acknowledgement. It is fully understood and agreed that Contractor is an independent contractor and is not an agent, servant, or employee of the State of Ohio or the Ohio Department of Administrative Services. Contractor declares that it is engaged as an independent business and has complied with all applicable federal, state, and local laws regarding business permits and licenses of any kind, including but not limited to any insurance coverage, workers' compensation, or unemployment compensation that is required in the normal course of business and will assume all responsibility for any federal, state, municipal or other tax liabilities. Additionally, Contractor understands that as an independent contractor, it is not a public employee and is not entitled to contributions from DAS to any public employee retirement system.

Contractor acknowledges and agrees any individual providing personal services under this agreement is not a public employee for purposes of Chapter 145 of the Ohio Revised Code. Unless Contractor is a "business entity" as that term is defined in ORC. 145.037 ("an entity with five or more employees that is a corporation, association, firm, limited liability company, partnership, sole proprietorship, or other entity engaged in business") Contractor shall have any individual performing services under this agreement complete and submit to the ordering agency the Independent Contractor/Worker Acknowledgement found at the following link: https://www.opers.org/forms-archive/PEDACKN.pdf

Contractor's failure to complete and submit the Independent/Worker Acknowledgement prior to commencement of the work, service or deliverable, provided under this agreement, shall serve as Contractor's certification that contractor is a "Business entity" as the term is defined in ORC Section 145.037.

Background Checks. All Contractor and subcontractor personnel assigned to the Identity Validation, Authentication and Fraud Services Project who have access to sensitive or confidential information or to sensitive State systems must have a current fingerprint search and background check performed by the Federal Bureau of Investigation or other Federal investigative authority. The fingerprint search and background checks must be completed before any such Contractor or subcontractor personnel gain access to State facilities, sensitive and/or confidential information or systems. All costs associated with this will be at the Contractor's expense. At its discretion, the State may reject any Contractor or subcontractor personnel based on the information provided in the completed background check.

Ohio MBE Certification. The MBE must maintain their certification throughout the term of the Contract, including any renewals. Failure to maintain such certification will be considered a breach of the Contract.

Publicity. The Contractor may not advertise or publicize that it is doing business with the State or use this Contract or the Contractor's relationship with the State as a marketing or sales tool, unless the State agrees otherwise in writing.

PART THREE: OWNERSHIP AND HANDLING OF INTELLECTUAL PROPERTY AND CONFIDENTIAL INFORMATION

Confidentiality. The State may disclose to the Contractor written material or oral or other information that the State treats as confidential ("Confidential Information"). Title to the Confidential Information and all related materials and documentation the State delivers to the Contractor will remain with the State. The Contractor must treat such Confidential Information as secret, if it is so marked, otherwise identified as such, or when, by its very nature, it deals with matters that, if generally known, would be damaging to the best interest of the public, other contractors, potential contractors with the State, or individuals or organizations about whom the State keeps

information. By way of example, information must be treated as confidential if it includes any proprietary documentation, materials, flow charts, codes, software, computer instructions, techniques, models, information, diagrams, know-how, trade secrets, data, business records, or marketing information. By way of further example, the Contractor also must treat as confidential materials such as police and investigative records, files containing personal information about individuals or employees of the State, such as personnel records, tax records, and so on, court and administrative records related to pending actions, any material to which an attorney-client, physician-patient, or similar privilege may apply, and any documents or records excluded by Ohio law from public records disclosure requirements.

The Contractor may not disclose any Confidential Information to third parties and must use it solely to do the Project. The Contractor must restrict circulation of Confidential Information within its organization and then only to people in the Contractor's organization that have a need to know the Confidential Information to do the Project. The Contractor will be liable for the disclosure of such information, whether the disclosure is intentional, negligent, or accidental, unless otherwise provided below.

The Contractor will not incorporate any portion of any Confidential Information into any work or product, other than a Deliverable, and will have no proprietary interest in any of the Confidential Information. Furthermore, the Contractor must cause all of its Personnel who have access to any Confidential Information to execute a confidentiality agreement incorporating the obligations in this section.

The Contractor's obligation to maintain the confidentiality of the Confidential Information will not apply where such: (1) was already in the Contractor's possession before disclosure by the State, and such was received by the Contractor without obligation of confidence; (2) is independently developed by the Contractor; (3) except as provided in the next paragraph, is or becomes publicly available without breach of this Contract; (4) is rightfully received by the Contractor from a third party without an obligation of confidence; (5) is disclosed by the Contractor with the written consent of the State; or (6) is released in accordance with a valid order of a court or governmental agency, provided that the Contractor (a) notifies the State of such order immediately upon receipt of the order and (b) makes a reasonable effort to obtain a protective order from the issuing court or agency limiting disclosure and use of the Confidential Information solely for the purposes intended to be served by the original order of production. The Contractor must return all originals of any Confidential Information and destroy any copies it has made on termination or expiration of this Contract.

Information that may be available publicly through other sources about people that is personal in nature, such as medical records, addresses, phone numbers, social security numbers, and similar things are nevertheless sensitive in nature and may not be disclosed or used in any manner except as expressly authorized in this Contract. Therefore, item (3) in the preceding paragraph does not apply, and the Contractor must treat such information as Confidential Information whether it is available elsewhere or not.

The Contractor may disclose Confidential Information to its subcontractors on a need-to-know basis, but the Contractor first must obligate them to the requirements of this section.

Confidentiality Agreements. When the Contractor performs services under this Contract that require the Contractor’s and its subcontractors’ personnel to access facilities, data, or systems that the State in its sole discretion deems sensitive, the State may require the Contractor’s and its subcontractors’ personnel with such access to sign an individual confidential agreement and policy acknowledgements, and have a background check performed before accessing those facilities, data, or systems. Each State agency, board, and commission may require a different confidentiality agreement or acknowledgement, and the Contractor’s and its subcontractors’ personnel may be required to sign a different confidentiality agreement or acknowledgement for each agency. The Contractor must immediately replace any of its or its subcontractors’ personnel who refuse to sign a required confidentiality agreement or acknowledgment or have a background check performed.

Ownership of Deliverables. The State owns all Deliverables that the Contractor produces under this Contract, including any software modifications, and documentation, with all rights, title, and interest in all intellectual property that come into existence through the Contractor’s custom work being assigned to the State. Additionally, the Contractor waives any author rights and similar retained interests in custom-developed material. The Contractor must provide the State with all assistance reasonably needed to vest such rights of ownership in the State. The Contractor will retain ownership of all tools, methods, techniques, standards, and other development procedures, as well as generic and preexisting shells, subroutines, and similar material incorporated into any

custom Deliverable ("Pre-existing Materials"), if the Contractor provides the non-exclusive license described in the next paragraph.

The Contractor may grant the State a worldwide, non-exclusive, royalty-free, perpetual license to use, modify, and distribute all Pre-existing Materials that are incorporated into any custom-developed Deliverable rather than grant the State ownership of the Pre-existing Materials. The State may distribute such Pre-existing materials to third parties only to the extent required by governmental funding mandates. The Contractor may not include in any custom Deliverable any intellectual property unless such has been created under this Contract or qualifies as Pre-existing Material. If the Contractor wants to incorporate any Pre-existing Materials into a custom Deliverable, the Contractor must first disclose that desire to the State in writing and seek the State's approval for doing so in advance. The State will not be obligated to provide that approval, unless the Contractor disclosed its intention to do so in the RFP Documents. On the Contractor's request, the State will incorporate into any copies of a custom Deliverable any proprietary notice that the Contractor included with the original copy, if that notice is reasonably necessary to protect the Contractor's interest in any Pre-existing Materials contained in the custom Deliverable.

Subject to the limitations and obligations of the State with respect to Pre-existing Materials, the State may make all custom Deliverables available to the general public without any proprietary notices of any kind.

For Deliverables that include custom materials such as software, scripts, or similar computer instructions developed for the State, the State is entitled to the source material. Scripts and similar functionality may not be locked or otherwise protected from access by the State, unless the State has any passwords or other tools necessary to access the material. Source material must include annotations or comments according to industry standards. Further, the State is entitled to any working papers the Contractor has developed during the performance of the Project that would reasonably assist the State in using the Deliverables that include source materials or that would help the State protect its interests in the Deliverable or update, modify, or otherwise maintain the Deliverable. This also includes all design and architectural materials, such as schemas.

The Contractor may use Confidential Information only as necessary for Contractor's performance under or pursuant to rights granted in this Agreement and for no other purpose. The Contractor's limited right to use Confidential Information expires upon expiration or termination of this Agreement for any reason. The Contractor's obligations of confidentiality and non-disclosure survive termination or expiration for any reason of this Agreement.

License in Commercial Material. As used in this section, "Commercial Material" means anything that the Contractor or a third party has developed at private expense, is commercially available in the marketplace, subject to intellectual property rights, and readily copied through duplication on magnetic media, paper, or other media. Examples include written reports, books, pictures, videos, movies, computer programs, and computer source code and documentation. It does not include Key Commercial Software that will be governed by Attachment Ten, Master Contract, but does include other Commercial Software.

Any Commercial Material that the Contractor intends to deliver as a Deliverable must have the scope of the license granted in such material disclosed in the RFP Documents or as an attachment referenced in the RFP Documents, if that scope of license is different from the scope of license contained in this section for Commercial Materials.

Except for Commercial Material that is software ("Commercial Software"), if the Commercial Material is copyrighted and published material, then the State will have the rights permitted under the federal copyright laws for each copy of the Commercial Material delivered to it by the Contractor.

Except for Commercial Software, if the Commercial Material is patented, then the State will have the rights permitted under the federal patent laws for each copy of the Commercial Material delivered to it by the Contractor.

Except for Commercial Software, if the Commercial Material consists of trade secrets, then the State will treat the material as confidential. In this regard, the State will assume all obligations with respect to the Commercial Material that the Contractor assumes under the Confidentiality section of this Contract with respect to the State's Confidential Information. Otherwise, the State will have the same rights and duties permitted under the federal copyright laws for each copy of the Commercial Material delivered to it by the Contractor, whether or not the material is copyrighted when delivered to the State.

For Commercial Software, the State will have the rights in items (1) through (6) of this section with respect to the software. The State will not use any Commercial Software except as provided in the six items below or as expressly stated otherwise in this Contract. The Commercial Software may be:

1. Used or copied for use in or with the computer or computers for which it was acquired, including use at any State installation to which such computer or computers may be transferred;
2. Used or copied for use in or with a backup computer for disaster recovery and disaster recovery testing purposes or if any computer for which it was acquired is inoperative;
3. Reproduced for safekeeping (archives) or backup purposes;
4. Modified, adapted, or combined with other computer software, but the modified, combined, or adapted portions of the derivative software incorporating any of the Commercial Software will be subject to same restrictions set forth in this Contract;
5. Disclosed to and reproduced for use on behalf of the State by support service contractors or their subcontractors, subject to the same restrictions set forth in this Contract; and
6. Used or copied for use in or transferred to a replacement computer.

Commercial Software delivered under this Contract is licensed to the State without disclosure restrictions unless it is clearly marked as confidential or secret. The State will treat any Commercial Software that is marked as confidential or secret as Confidential Information to the extent that such is actually the case.

Key Commercial Software will be covered by a separate Master Contract for Software Licensing, in the form of Attachment Ten. When such a Master Contract is executed, it will be a separate agreement and not part of this Contract, though the Contractor remains responsible for ensuring that the completed Project, including any Key Commercial Software, meets the requirements of this Contract and performs according to the RFP Documents' requirements.

Cloud Software solutions will be covered by a separate Master Cloud Services Agreement and Service Attachment for Software Licensing, in the form of Attachment Eleven. When such a Master Cloud Service Agreement and Service Attachment are executed, it will be a separate agreement and not part of this Contract, though the Contractor remains responsible for ensuring that the completed Project, including any Cloud Software, meets the requirements of this Contract and performs according to the RFP Documents' requirements.

PART FOUR: REPRESENTATIONS, WARRANTIES, AND LIABILITIES

General Warranties. The Contractor warrants that the recommendations, guidance, and performance of the Contractor under this Contract will: (1) be in accordance with sound professional standards and the requirements of this Contract and without any material defects; and (2) unless otherwise provided in the RFP Documents, be the work solely of the Contractor. The Contractor also warrants that: (1) no Deliverable will infringe on the intellectual property rights of any third party; and (2) the Contractor's work and the Deliverables resulting from that work will be merchantable and fit for the particular purposes described in the RFP Documents.

Additionally, with respect to the Contractor's activities under this Contract, the Contractor warrants that: (1) the Contractor has the right to enter into this Contract; (2) the Contractor has not entered into any other contracts or employment relationships that restrict the Contractor's ability to perform the contemplated services; (3) the Contractor will observe and abide by all applicable laws and regulations, including those of the State regarding conduct on any premises under the State's control and security for the State's data, systems, and networks; (4) the Contractor has good and marketable title to any goods delivered under this Contract and in which title passes to the State; (5) the Contractor has the right and ability to grant the license granted in any Deliverable in which title does not pass to the State; and (6) the Contractor is not subject to any unresolved findings of the Auditor of State under Revised Code Section 9.24 and will not become subject to an unresolved finding that prevents the extension or renewal of this Contract.

The warranties regarding material defects, merchantability, and fitness are one-year warranties. All other warranties will be continuing warranties. If any portion of the Project fails to comply with these warranties, and the Contractor is so notified in writing, the Contractor must correct such failure with all due speed or must refund the amount of the compensation paid for such portion of the Project. The Contractor also must indemnify the State for any direct damages and claims by third parties based on a breach of these warranties. This obligation of indemnification will not apply where the State has modified or misused the Deliverable and the claim is based on the modification or misuse. The State will give the Contractor notice of any such claim as soon as reasonably

practicable. If a successful claim of infringement is made, or if the Contractor reasonably believes that an infringement claim that is pending may actually succeed, the Contractor must do one of the following things: (1) modify the Deliverable so that it is no longer infringing; (2) replace the Deliverable with an equivalent or better item; (3) acquire the right for the State to use the infringing Deliverable as it was intended for the State to use under this Contract; or (4) remove the Deliverable and refund the amount the State paid for the Deliverable and the amount of any other Deliverable or item that requires the availability of the infringing Deliverable for it to be useful to the State.

Software Warranty. If this Contract involves software as a Deliverable, then, on acceptance and for 12 months after the date of acceptance of any Deliverable that includes software, the Contractor warrants as to all software developed under this Contract that: (a) the software will operate on the computer(s) for which the software is intended in the manner described in the relevant software documentation, the Contractor's Proposal, and the RFP Documents; (b) the software will be free of any material defects; (c) the Contractor will deliver and maintain relevant and complete software documentation, commentary, and source code; and (d) the source code language used to code the software is readily available in the commercial market, widely used and accepted for the type of programming involved, and support programming in the language is reasonably available in the open market; and (e) the software and all maintenance will be provided in a professional, timely, and efficient manner.

For Commercial Software licensed from a third party that is incorporated into a Deliverable, and for which the State has not approved a separate license agreement governing that Commercial Software's warranties as part of the RFP process, the Contractor represents and warrants that it has done one of the following things: (a) obtained the right from the third-party licensor to commit to the warranties and maintenance obligations in this Section; (b) obtained a binding commitment from the licensor to make those warranties and maintenance obligations directly to the State; or (c) fully disclosed in the RFP Documents any discrepancies between the requirements of this section and the commitment the third-party licensor has made.

In addition, for Commercial Software that is incorporated into a Deliverable, the Contractor will: (a) maintain or cause the third-party licensor to maintain the Commercial Software so that it operates in the manner described in the RFP Documents (or any attachment referenced in the RFP Documents) and relevant Commercial Software documentation; (b) supply technical bulletins and updated user guides; (c) supply the State with updates, improvements, enhancements, and modifications to the Commercial Software and documentation and, if available, the commentary and the source code; (d) correct or replace the Commercial Software and/or remedy any material programming error that is attributable to the Contractor or the third-party licensee; (e) maintain or cause the third-party licensor to maintain the Commercial Software and documentation to reflect changes in the subject matter the Commercial Software deals with; (f) maintain or obtain a commitment from the third-party licensor to maintain the Commercial Software so that it will properly operate in conjunction with changes in the operating environment in which it is designed to operate.

For purposes of the warranties and the delivery requirements in this Contract, software documentation means well written, readily understood, clear, and concise instructions for the software's users as well as a system administrator. The software documentation will provide the users of the software with meaningful instructions on how to take full advantage of all of the capabilities designed for end users. It also means installation and system administration documentation for a system administrator to allow proper control, configuration, and management of the software. Source code means the uncompiled operating instructions for the software. However, the Contractor will not be obligated to provide source code for Commercial Software unless it is readily available from the licensor. The source code must be provided in the language in which it was written and will include commentary that will allow a competent programmer proficient in the source language to readily interpret the source code and understand the purpose of all routines and subroutines contained within the source code.

Equipment Warranty. If any electrical equipment, mechanical device, computer hardware, telecommunications hardware, or other type of physical machinery ("Equipment") will be a part of any Deliverable, the following warranties apply. The Contractor warrants that the Equipment fully complies with all government environmental and safety standards applicable to the Equipment. The Contractor also warrants for one year from the acceptance date of the Equipment that the Equipment will perform substantially in accordance with specifications described in the RFP Documents, the user manuals, technical materials, and related writings published by the manufacturer for the Equipment. The foregoing warranties will not apply to Equipment that is modified or damaged after title passes to the State.

The Contractor must notify the State in writing immediately upon the discovery of any breach of the warranties given above.

The Contractor must do the following if any Equipment does not meet the above warranties:

(a) Cause the Equipment to perform as required, or, if that is not commercially practicable, then;
(b) Grant the State a refund equal to the amount the State paid for the Equipment or, if such has not been individually priced, the manufacturer's suggested retail price for the Equipment.

Except where the Contractor's breach of a warranty makes it not possible for the State to do so, the State will return the affected Equipment to the Contractor in the case of a refund under the previous paragraph.

GENERAL EXCLUSION OF WARRANTIES. THE CONTRACTOR MAKES NO WARRANTIES, EXPRESS OR IMPLIED, OTHER THAN THOSE EXPRESS WARRANTIES CONTAINED IN THIS CONTRACT.

Indemnity for Property Damage and Bodily Injury. The Contractor must indemnify the State for all liability and expense resulting from bodily injury to any person (including injury resulting in death) and damage to tangible or real property arising out of the performance of this Contract, provided that such bodily injury or property damage is due to the negligence or other tortious conduct of the Contractor, its employees, agents, or subcontractors. The Contractor will not be responsible for any damages or liability to the extent caused by the negligence or willful misconduct of the State, its employees, other contractors, or agents.

Limitation of Liability. Neither party will be liable for any indirect, incidental, or consequential loss or damage of the other party, including but not limited to lost profits, even if the parties have been advised, knew, or should have known of the possibility of such damages. Additionally, neither party will be liable to the other for direct or other damages in excess of two times the Not-To-Exceed Fixed Price of this Contract. The limitations in this paragraph do not apply to any obligation of the Contractor to indemnify the State against claims made against it or for damages to the State caused by the Contractor’s negligence or other tortious conduct.

PART FIVE: ACCEPTANCE AND MAINTENANCE

Standards of Performance and Acceptance. There will be a period for performance testing of the completed Project. During the performance period, the State, with the assistance of the Contractor, will perform acceptance testing. The performance period will last up to 90 calendar days, during which time the Project must meet the standard of performance required by the RFP Documents for 30 consecutive calendar days. The performance criteria in the RFP Documents will be supplemented with the relevant user manuals, technical materials, and related writings, to the extent that the specifications in those writings supplement and refine rather than contradict the performance criteria in the RFP Documents. Acceptance of the Project depends on a successful completion of the performance period defined in this section and the RFP Documents. This section applies to the Project, and any part of it, as well as replacements or substitutes for the Project after completion of a successful performance period.

If the Project does not meet the standard of performance during the initial performance period, the State will give the Contractor details about the problems in a timely manner and in a useful and relevant form. Until the Contractor demonstrably corrects all outstanding problems, the second performance period will not start, and the State will not accept the Project (or part thereof). The second performance test will continue on a day-by-day basis until the standard of performance is met for a total of 30 consecutive calendar days or until the 90-day performance period has ended without meeting the standard of performance.

If the Project fails to meet the standard of performance after 90 calendar days from the start of the second performance period, the Contractor will be in default and will not have a cure period. In addition to all other remedies the State may have under this Contract, the State may request a correction or replacement of the relevant portion of the Project.

The Project may have components that can be tested for acceptance individually. If that is so, there may be acceptance criteria listed on the RFP Documents for each part of the Project that will be independently tested and accepted. However, unless the RFP Documents expressly provide otherwise, the failure of any independently tested component to meet its acceptance criteria will give the State the right to reject the entire Project. Alternatively, if the State determines that it is in the State's interest to reject only the part of the Project that was

independently and unsuccessfully tested, it may do so. If the State chooses this option, the State will be entitled to a refund or credit toward the Contractor's Fee equal to the cost of acquiring a replacement for the rejected component.

The acceptable level of performance for the Project will be 98.5%, unless otherwise specified in the RFP Documents. The performance level for the Project is computed by dividing the sum of the uptime by the number of working hours during the test time. “Uptime” means the total hours, rounded to the nearest quarter hour, during which all components of the Project are operational and all functions of the Project are available to its users. The number of “working hours” means the total number of working hours for the period during which the Project was scheduled to be available to its users. Uptime and downtime will be measured in hours and quarter hours.

The Project “downtime” is that period when any part of the Project is inoperable due to failure of the Project or a particular Deliverable to operate according to the specifications in the RFP Documents, the user documentation, or the published technical specifications. During a period of downtime, the State may use operable components of the Project when that will not interfere with repair of inoperable components of the Project. Downtime will start from the time the State notifies the Project Manager of the inoperable condition of the Project until the Project is returned in proper operating condition.

The Project will not be accepted until the performance period is complete.

Should it be necessary, the State may delay the start of the performance period, but the delay will not exceed 30 consecutive calendar days after the scheduled date for implementation of the Project. Such a delay will not be considered a suspension of work under the Suspension and Termination section of this Contract.

Passage of Title. Title to any Deliverable will pass to the State only on acceptance of the Deliverable. All risk of loss, regardless of the cause, will remain with the Contractor until title to the Deliverable passes to the State.

Software Maintenance. If this Contract involves software as a Deliverable, then, during the warranty period, as well as any optional maintenance periods that the State exercises, the Contractor must correct any material programming errors that are attributable to the Contractor within a reasonable period of time. However, the State must notify the Contractor, either orally or in writing, of a problem with the software and provide sufficient information for the Contractor to identify the problem.

The Contractor's response to a programming error will depend upon the severity of the problem. For programming errors that slow the processing of data by a small degree, render minor and non-mandatory functions of the System inoperable or unstable, or require users or administrators to employ workarounds to fully use the software, Contractor will respond to the request for resolution within four business hours. Furthermore, the Contractor must begin working on a proper solution for the problem within one business day, dedicating the resources required to fix the problem. For any defects with more significant consequences, including those that render key functions of the system inoperable or significantly slow processing of data, the Contractor will respond within two business hours of notice. The Contractor also must begin working on a proper solution for the problem immediately after responding and, if requested, provide on-site assistance and dedicate all available resources to resolving the problem.

For software classified as Commercial Software in the Ownership of Deliverables section and for which the State has not signed a separate license agreement, the Contractor must acquire for the State the right to maintenance for one year. That maintenance must be the third-party licensor's standard maintenance program, but at a minimum, that maintenance program must include all, updates, patches, and fixes to the software. It also must include a commitment to keep the software current with the operating environment in which it is designed to function (and, if applicable, the subject matter covered by the software) and to correct material defects in the software in a timely fashion. Additionally, the Contractor must obtain a commitment from the licensor to make maintenance available for the product for at least five years after the first year of maintenance. The Contractor also must obtain a commitment from the licensor to limit increases in the annual Fee for maintenance to no more than 7% annually. If the licensor is unable to provide maintenance during that five-year period, then the licensor must be committed to doing one of the following two things: (a) give the State a *pro rata* refund of the license fee based on a five-year useful life; or (b) release the source code for the software (except third party software) to the State for use by the State solely for the purpose of maintaining the copy(ies) of the software for which the State has a proper license. For purposes of receiving the source code, the State agrees to treat it as confidential and to be obligated to the requirements under the Confidentiality section of this Contract with respect to the source code.

That is, with respect to the source code that the State gets under this section, the State will do all the things that the Confidentiality section requires the Contractor to do in handling the State's Confidential Information.

Equipment Maintenance. If this Contract involves Equipment as a Deliverable, then, upon Equipment delivery and for 12 months after acceptance, the Contractor must provide Equipment maintenance to keep the Equipment in or restore the Equipment to good working order. If the State exercises its right to any optional maintenance periods, the Contractor's obligations hereunder will extend to those periods as well. This maintenance must include preventative and remedial maintenance, installation of safety changes, and installation of engineering changes based upon the specific needs of the individual item of Equipment. This maintenance must include the repair, replacement, or exchange deemed necessary to keep the Equipment in good working condition. For purposes of this Contract, Equipment restored to good working condition means Equipment that performs in accordance with the manufacturer's published specifications and the RFP Documents.

The Contractor must exert its best efforts to perform all fault isolation and problem determination attributed to the Equipment covered under this Contract.

The following services are outside the scope of this Contract:

a. Maintenance to bring the Equipment into compliance with any law, rule, or regulation if such law, rule, or regulation was not in effect on the acceptance date.
b. Repair and replacement work or increase in maintenance time as a result of damage or loss resulting from casualty or the State's misuse of the Equipment, damage resulting from improper packing or failure to follow prescribed shipping instructions (if such is done by the State), failure of electrical power, air conditioning or humidity control, use of supplies not approved by the original manufacturer of the Equipment as described or included in the Contractor's Proposal, or causes other than ordinary use of the Equipment.
c. Furnishing supplies or accessories, making specification changes, or adding or removing approved accessories, attachments, or other devices.
d. Maintenance or any increase in maintenance time resulting from any maintenance or inappropriate connection to other equipment (not done by the Contractor) that results in damage to the Equipment.
e. Activities required to restore the Equipment to good operating condition if the problem has resulted from someone other than Contractor's authorized service personnel repairing, modifying, or performing any maintenance service on the Equipment.

Equipment Maintenance Standards. This section applies if Equipment will be a Deliverable under this Contract.

The Contractor must complete all remedial Equipment maintenance within eight business hours after notification by the State that maintenance is required. In the case of preventative maintenance, the Contractor must perform such in accordance with the manufacturer's published schedule and specifications. If maintenance is not completed or substitute equipment provided within eight hours after notification by the State, the Contractor will be in default.

All maintenance also must meet any standards contained in the RFP Documents. Failure of the Contractor to meet or maintain these requirements will provide the State with the same rights and remedies specified elsewhere in the RFP Documents for default, except that the Contractor will only have eight hours to remedy the default.

The Contractor must provide adequate staff to provide the maintenance required by this Contract.

Equipment Maintenance Continuity. This section applies if Equipment will be a Deliverable under this Contract.

If the Contractor is unable to provide maintenance services to meet the State's ongoing performance requirements for Equipment delivered under this Contract, and if, in the State's sole opinion, the Contractor is unlikely to resume providing warranty services that meet the State's ongoing performance requirement, the Contractor will be in default. The State then will be entitled to the remedies in the default section of this Contract. However, the State will also be entitled to the following items from the Contractor: (a) all information necessary for the State to perform the maintenance, including logic diagrams, maintenance manuals and system and unit schematics, as modified by the Contractor; and (b) a listing of suppliers capable of supplying necessary spare parts.

Any information in items (a) and (b) above that is rightfully identified by the Contractor as confidential information will be maintained in confidence by the State, except where disclosure to a third party is necessary for the State to continue the maintenance. However, any third party to whom disclosure is made must agree to hold such proprietary information in confidence and to make no further disclosure of it. Further, any such confidential information will be used solely to perform the Contractor's maintenance obligations hereunder and will be returned to the Contractor upon completion of such use.

Principal Period of Maintenance (General). This section applies if software or Equipment will be a Deliverable under this Contract.

The Contractor must make maintenance available twelve working hours per weekday, between 7:00 a.m. and 7:00 p.m. (Columbus, Ohio local time). Travel time and expenses related to remedial and preventive maintenance will not be considered billable but will be included in the Contractor's firm, fixed Fee for the Project during the warranty period and a part of the annual maintenance Fee during later annual maintenance periods.

Maintenance Access (General). This section applies if software or Equipment will be a Deliverable under this Contract.

The Contractor must keep the Project in good operating condition during the warranty period and any annual maintenance period during which the State contracts for continued maintenance. The State will provide the Contractor with reasonable access to the Project to perform maintenance. All maintenance that requires the Project to be inoperable must be performed outside the State's customary working hours, except when the Project is already inoperable. Preventive or scheduled maintenance will be performed at mutually agreeable times, within the parameters of the manufacturer's published schedule.

Key Maintenance Personnel (General). This section applies if software or Equipment will be a Deliverable under this Contract.

The Contractor must identify all key people responsible for providing maintenance on the Project, furnish the State with a means of identifying these people, furnish the State with their credentials, and notify the State at least 30 calendar days in advance of any reductions in staffing levels of key people at the office serving the State.

PART SIX: CONSTRUCTION

Entire Document. This Contract is the entire agreement between the parties with respect to its subject matter and supersedes any previous agreements, whether oral or written.

Binding Effect. This Contract will be binding upon and inure to the benefit of the respective successors and assigns of the State and the Contractor.

Amendments – Waiver. No change to any provision of this Contract will be effective unless it is in writing and signed by both parties. The failure of either party at any time to demand strict performance by the other party of any of the terms of this Contract will not be a waiver of those terms. Waivers must be in writing to be effective, and either party may at any later time demand strict performance.

Severability. If any provision of this Contract is held by a court of competent jurisdiction to be contrary to law, the remaining provisions of this Contract will remain in full force and effect to the extent that such does not create an absurdity.

Construction. This Contract will be construed in accordance with the plain meaning of its language and neither for nor against the drafting party.

Headings. The headings used herein are for the sole sake of convenience and may not be used to interpret any section.

Notices. For any notice under this Contract to be effective, it must be made in writing and sent to the address of the appropriate contact provided elsewhere in the Contract, unless such party has notified the other party, in

accordance with the provisions of this section, of a new mailing address. This notice requirement will not apply to any notices that this Contract expressly authorized to be made orally.

Continuing Obligations. The terms of this Contract will survive the termination or expiration of the time for completion of Project and the time for meeting any final payment of compensation, except where such creates an absurdity.

Time. Unless otherwise expressly provided, any reference in this document to a number of days for an action or event to occur means calendar days, and any reference to a time of the day, such as 5:00 p.m., is a reference to the local time in Columbus, Ohio.

Time is of the Essence. Contractor hereby acknowledges that time is of the essence for performance of this Contract unless, otherwise agreed to in writing by the parties.

PART SEVEN: LAW AND COURTS

Compliance with Law. The Contractor must comply with all applicable federal, state, and local laws while performing under this Contract.

Drug-Free Workplace. The Contractor must comply with all applicable state and federal laws regarding keeping a drug-free workplace. The Contractor must make a good faith effort to ensure that all the Contractor's Personnel, while working on state property, will not have or be under the influence of illegal drugs or alcohol or abuse prescription drugs in any way.

Conflicts of Interest and Ethics Compliance Certification. None of the Contractor's Personnel may voluntarily acquire any personal interest that conflicts with their responsibilities under this Contract. Additionally, the Contractor may not knowingly permit any public official or public employee who has any responsibilities related to this Contract or the Project to acquire an interest in anything or any entity under the Contractor's control, if such an interest would conflict with that official's or employee's duties. The Contractor must disclose to the State knowledge of any such person who acquires an incompatible or conflicting personal interest related to this Contract. The Contractor also must take steps to ensure that such a person does not participate in any action affecting the work under this Contract. However, this will not apply when the State has determined, in light of the personal interest disclosed, that person's participation in any such action would not be contrary to the public interest.

Ohio Ethics Law and Limits on Political Contributions. The Contractor certifies that it is currently in compliance and will continue to adhere to the requirements of the Ohio ethics laws. The Contractor also certifies that all applicable parties listed in Ohio Revised Code Section 3517.13 are in full compliance with Ohio Revised Code Section 3517.13.

Unresolved Finding for Recovery. If the Contractor was subject to an unresolved finding of the Auditor of State under Revised Code Section 9.24 on the date the parties sign this Contract, the Contract is void. Further, if the Contractor is subject to an unresolved finding of the Auditor of State under Revised Code Section 9.24 on any date on which the parties renew or extend this Contract, the renewal or extension will be void.

Equal Employment Opportunity. The Contractor will comply with all state and federal laws regarding equal employment opportunity and fair labor and employment practices, including Ohio Revised Code Section 125.111 and all related Executive Orders.

Before a contract can be awarded or renewed, an Affirmative Action Program Verification Form must be submitted to the Department of Administrative Services Equal Opportunity Division to comply with the affirmative action requirements. Affirmative Action Verification Forms and approved Affirmative Action Plans can be found by going to the Ohio Business Gateway at: http://business.ohio.gov/efiling/

Use of MBE and EDGE Suppliers. The State encourages Contractor to purchase goods and services from Minority Business Enterprises (MBE) and Encouraging Diversity, Growth, and Equity (EDGE) suppliers.

Security & Safety Rules. When using or possessing State data or accessing State networks and systems, the Contractor must comply with all applicable State rules, policies, and regulations regarding data security and

integrity. And when on any property owned or controlled by the State, the Contractor must comply with all security and safety rules, regulations, and policies applicable to people on those premises.

Governing the Expenditure of Public Funds on Offshore Services (EO 2011-12K). The Service Provider affirms it has read and understands Executive Order 2011-12K and will abide by those requirements in the performance of this Agreement. Notwithstanding any other terms of this Agreement, the State reserves the right to recover any funds paid for Services the Service Provider performs outside of the United States for which it did not receive a waiver. The State does not waive any other rights or remedies provided the State in this Agreement.

The Service Provider agrees to complete the attached Executive Order 2011-12K Affirmation and Disclosure Form, which is incorporated and becomes a part of this Agreement.

Injunctive Relief. Nothing in this Contract is intended to limit the State's right to injunctive relief, if such is necessary to protect its interests or to keep it whole.

Assignment. The Contractor may not assign this Contract or any of its rights or obligations under this Contract without the prior, written consent of the State. The State is not obligated to provide its consent to any proposed assignment.

Governing Law. This Contract will be governed by the laws of Ohio, and venue for any disputes will lie exclusively with the appropriate court in Franklin County, Ohio.

Registration with the Secretary of State. By providing a Charter Number and signature within the Certification Offer Letter, the Contractor attests that the Contractor is:

An Ohio corporation that is properly registered with the Ohio Secretary of State; or

A foreign corporation, not incorporated under the laws of the state of Ohio, but is registered with the Ohio Secretary of State pursuant to Ohio Revised Code Sections 1703.01 to 1703.31, as applicable.

Any foreign corporation required to be licensed under O.R.C. § 1703.01-1703.31, which transacts business in the state of Ohio, without being so licensed, or when its license has expired or been canceled, shall forfeit not less than $250.00 nor more than ten thousand dollars. No officer of a foreign corporation http://codes.ohio.gov/orc/1703.01 shall transact business in the state of Ohio, if such corporation is required by O.R.C. § 1703.01-1803.31 to procure and maintain a license, but has not done so. Whoever violates this is guilty of a misdemeanor of the forth degree. Questions regarding registration should be directed to (614) 466-3910, or visit http://www.sos.state.oh.us .

ATTACHMENT FIVE
SAMPLE CONTRACT

A CONTRACT BETWEEN
THE OFFICE OF INFORMATION TECHNOLOGY
ON BEHALF OF THE

_____

AND

_____

(CONTRACTOR)

THIS CONTRACT, which results from RFP 0A1161, entitled Enterprise Identity Validation, Authentication and Fraud Services , is between the State of Ohio, through the Department of Administrative Services, on behalf of the Ohio Department of Administrative Services, Office of Information Technology and _____ (the "Contractor").

The Contract is the result of agreed upon changes to the RFP its attachments and supplements including any written amendments to the RFP, any materials incorporated by reference in the RFP, the Contractor's Proposal, and written, authorized amendments and clarifications to the Contractor's Proposal. It also includes any purchase orders and change orders issued under the Contract.

This Contract consists of:

1. The one page Contract (Attachment Five) in its final form; and
2. The 0A1161 Enterprise Identity Validation, Authentication and Fraud Services Contract dated _____, 2016 which includes Attachment Four, Attachments, Supplements and the Cost Proposal Workbook dated _____, 2016.

Change Orders and amendments issued after the Contract is executed may expressly change the provisions of the Contract. If they do so expressly, then the most recent of them will take precedence over anything else that is part of the Contract.

This Contract has an effective date of the later of _____, 2016, or the occurrence of all conditions precedent specified in the General Terms and Conditions.

TO SHOW THEIR AGREEMENT, the parties have executed this Contract as of the dates below.

SAMPLE

CONTRACTOR	STATE OF OHIO DEPARTMENT OF ADMINISTRATIVE SERVICES
SAMPLE – DO NOT FILL OUT	_____
By:	By: DAS Director
Title: _____	Title: Director
Date: _____	Date: _____

ATTACHMENT SIX

OFFEROR CERTIFICATION FORM

Note: Offeror must provide a response to each of the numbered items in the Offeror Certification Form.

1. The offeror is not currently subject to an "unresolved" finding for recovery under Revised Code Section 9.24, and the offeror will notify the Procurement Representative any time it becomes subject to such a finding before the award of a Contract arising out of this RFP.

2. The offeror certifies that it will not and will not allow others to perform work for the State of Ohio outside the geographic limitations contained in Attachment Two or take data that belongs to the State of Ohio outside the geographic limitations contained in Attachment Two without express written authorization from the State.

3. The offeror certifies that its responses to the following statements are true and accurate. The offeror's answers apply to the last seven years. Please indicate yes or no in each column.

Yes/No	Description
	The offeror has had a contract terminated for default or cause.
	The offeror has been assessed any penalties in excess of $10,000.00, including liquidated damages, under any of its existing or past contracts with any organization (including any governmental entity).
	The offeror was the subject of any governmental action limiting the right of the offeror to do business with that entity or any other governmental entity.
	Trading in the stock of the company has ever been suspended with the date(s) and explanation(s).
	The offeror, any officer of the offeror, or any owner of a 20% interest or greater in the offeror has filed for bankruptcy, reorganization, a debt arrangement, moratorium, or any proceeding under any bankruptcy or insolvency law, or any dissolution or liquidation proceeding.
	The offeror, any officer of the offeror, or any owner with a 20% interest or greater in the offeror has been convicted of a felony or is currently under indictment on any felony charge.

If the answer to any item above is affirmative, the offeror must provide complete details about the matter. While an affirmative answer to any of these items will not automatically disqualify an offeror from consideration, at the sole discretion of the State, such an answer and a review of the background details may result in a rejection of the Proposal. The State will make this decision based on its determination of the seriousness of the matter, the matter's possible impact on the offeror's performance under the Contract, and the best interest of the State.

4. The offeror certifies that neither it nor any of its people that may work on or benefit from the Contract through the offeror has a possible conflict of interest (e.g., employed by the State of Ohio, etc.) other than the conflicts identified immediately below:

Potential Conflicts (by person or entity affected)

(Attach an additional sheet if more space is need.)

The State may reject a Proposal in which an actual or apparent conflict is disclosed. And the State may cancel or terminate the Contract for cause if it discovers any actual or apparent conflict of interest that the offeror did not disclose in its Proposal.

5. The offeror certifies that all its and its subcontractors' personnel provided for the Work will have a valid I-9 form on file with the offeror or subcontractor, as appropriate, and will have presented valid employment authorization documents, if they are not United States citizens.

6. The offeror certifies that it's regular, fulltime employees will perform at least 30% of the Work.

7. The following is a complete list of all subcontractors, if any, that the offeror will use on the Work, if the State selects the offeror to do the Work:

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

The offeror certifies that it has obtained and submitted a subcontractor letter, as required by Attachment Three, for each subcontractor it plans to use to do the Work.

8. The offeror certifies that that any MBE program participants will provide necessary data to ensure program reporting and compliance.

Provide the following information for a contact person who has authority to answer questions regarding the offeror's Proposal:

Name:	
Title:	
Mailing Address:	
Office Phone Number:	
Cell Phone Number:	
Fax Number:	
Email Address:	

_____
Signature

_____
Name

_____
Title

_____
Company Name

_____
Company D-U-N-S Number

ATTACHMENT SEVEN
OFFEROR PROFILE

OFFEROR MANDATORY REQUIREMENTS

MANDATORY REQUIREMENT #1:

The offeror, as the prime Contractor, must be an HSPD-12 (ICAM) qualified Contractor or Service Provider as of the date of proposal submission.

HSPD-12 (ICAM) Qualified Contractor or Service Provider Name:	**Contact Name:** (Indicate Primary or Alternate) **Contact Title:**
HSPD-12 (ICAM) Qualified Contractor or Service Provider Address:	**Contact Phone Number:** **Contact Email Address:**
	Beginning Date of Qualification: / Ending Date of Qualification: **Month/Year** **Month/Year**
Describe Contractor or Service Provider Qualifications	

ATTACHMENT SEVEN
OFFEROR PROFILE

OFFEROR MANDATORY REQUIREMENTS

MANDATORY REQUIREMENT #2:

The offeror, must as part of their offer to the State include a FICAM TFS Approved Identity Service at National Institute of Standards and Technology (NIST) Levels 1, 2 or 3 as of the date of proposal submission.

FICAM TFS Approved Identity Service Contractor or Service Provider Name:	**Contact Name:** (Indicate Primary or Alternate) **Contact Title:**
FICAM TFS Approved Identity Service Contractor or Service Provider Address:	**Contact Phone Number:** **Contact Email Address:**
	Beginning Date of Approval: / Ending Date of Approval: **Month/Year** **Month/Year**
NIST Qualification Level(s) Certified:	**Level 1** **Level 2** **Level 3**
Describe Contractor or Service Provider Qualifications	

ATTACHMENT SEVEN
OFFEROR PROFILE

OFFEROR MANDATORY REQUIREMENTS

MANDATORY REQUIREMENT #3:

The offeror, as the prime Contractor, must have performed and completed a systems integration project using the proposed architecture in a production environment for at least one Public Governmental, Federal, State, Local, Institution of Higher Education, Fortune 500 or Global Fortune 500 customer within the last four years.

Agency/Company/Higher Ed Name:	**Contact Name:** (Indicate Primary or Alternate) **Contact Title:**
Agency/Company/Higher Ed Address:	**Contact Phone Number:** **Contact Email Address:**
Project Name:	**Beginning Date of Expr: / Ending Date of Expr:** **Month/Year** **Month/Year**
Software, Proposed Architecture Utilized:	**Version(s):**
Describe Related Service Provided: **Describe how the Related Service shows the offeror's experience, capability, and capacity to meet the requirements and achieve the milestones for this Project:**	

ATTACHMENT EIGHT: STANDARD AFFIRMATION AND DISCLOSURE FORM

EXECUTIVE ORDER 2011-12K

Governing the Expenditure of Public Funds on Offshore Services
All of the following provisions must be included in all invitations to bid, requests for proposals, state term schedules, multiple award contracts, requests for quotations, informal quotations and statements of work. This information is to be submitted as part of the response to any of the procurement methods listed.

CONTRACTOR/SUBCONTRACTOR AFFIRMATION AND DISCLOSURE:

By the signature affixed to this response, the Bidder/Offeror affirms, understands and will abide by the requirements of Executive Order 2011-12K. If awarded a contract, the Bidder/Offeror becomes the Contractor and affirms that both the Contractor and any of its Subcontractors shall perform no services requested under this Contract outside of the United States.

The Bidder/Offeror shall provide all the name(s) and location(s) where services under this Contract will be performed in the spaces provided below or by attachment. Failure to provide this information may subject the Bidder/Offeror to sanctions, termination or a damages assessment. If the Bidder/Offeror will not be using Subcontractors, indicate "Not Applicable" in the appropriate spaces.

1. Principal location of business of Contractor:

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

   Name/Principal location of business of subcontractor(s):

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

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

2. Location where services will be performed by Contractor:

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

   Name/Location where services will be performed by subcontractor(s):

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

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

ATTACHMENT EIGHT

STANDARD AFFIRMATION AND DISCLOSURE FORM
EXECUTIVE ORDER 2011-12K

Governing the Expenditure of Public Funds on Offshore Services

CONTINUED

3. Location where state data will be stored, accessed, tested, maintained or backed-up, by Contractor:

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

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

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

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

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

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

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

ATTACHMENT NINE
SUPPLEMENT ONE – ENTERPRISE IDENTITY VALIDATION, AUTHENTICATION AND FRAUD SERVICES COST PROPOSAL

Attachment Nine is included as an electronic form in the Opportunity Description on the State Procurement Website for this RFP. The Cost Proposal is to be submitted in Microsoft Excel workbook in native Excel format – not PDF.

ATTACHMENT TEN
MASTER CONTRACT FOR SOFTWARE LICENSING (MLA NUMBER [0000000])

THIS CONTRACT (the "Contract") is between the State of Ohio (the "State"), through the Department of Administrative Services, Investment and Governance Division, with offices at 30 East Broad Street, Columbus, Ohio 43215, and *[Company name of the Contractor]* (the "Contractor"), with offices at *[street address, city, state and zip code for the Contractor]*, and whose Federal Tax ID Number is *[the Contractor's TIN]* and D-U-N-S Number is *[the Contractor's D-U-N-S]*.

BACKGROUND

The State and the Contractor have entered into this Contract to provide the terms and conditions under which the Contractor will grant one or more perpetual, nonexclusive licenses to the State to use certain software that the Contractor publishes or markets (the "Software"). Any such licenses will be described in one or more schedules to this Contract ("Schedules") and will include a license to use the Software's user and technical documentation (the "Documentation"). It also may include a license to use the Software's source code and related material ("Source Code"), if it is so indicated elsewhere in this Contract or on the applicable Schedule. Additionally, this Contract governs the Contractor's obligation to provide the State with assistance troubleshooting the Software and with updates, correction, enhancements, and new releases of the Software ("Support").

PART I: LICENSE AND USE

1. **Grant of License.** The Contractor grants to the State a nonexclusive, nontransferable, and perpetual license to use the executable code version of the Software identified in each Schedule under this Contract, along with the related Documentation, and if indicated in an applicable Schedule, the Source Code for the Software. The license begins on the date identified in the applicable Schedule as the start date for the license (the "Start Date"). Unless indicated otherwise in this Contract, such use will be limited to use solely for the exercise of any function of State government by any State agency or political subdivision of the State ("Affiliated Entities"). The applicable Schedule governing the license will describe the scope of each license granted to the State in further detail, and the State agrees to limit its use of the Software as described in the applicable Schedule. The State may not republish the Software or the Documentation or distribute it to any third party, unless and only to the extent that this Contract or the scope of license in the applicable Schedule expressly so permits. The State will have a right to use the Software at any of its locations worldwide, subject only to applicable restrictions on export of technology from the US, the scope of license in the applicable Schedule, and the restrictions in this Contract on using the Software in hazardous environments.

2. **Generated Files.** "Generated Files" are files that the State creates using the Software and in which the State's data or results from the State's instructions are stored. Examples of such files could include, among others, text files generated with a word processor, data tables created with a database engine, and image files created with a graphics application. Applications consisting of instruction sets created with a programming language that the Contractor licensed to the State also would be considered Generated Files. As between the State and the Contractor, the State will own all Generated Files that the State prepares by using the Software, excluding such portions of the Generated Files that consist of embedded portions of the Software. The Contractor or its licensors will retain ownership of any portions of the Software embedded into Generated Files. But the Contractor grants to the State a nonexclusive, royalty-free right to reproduce and distribute to third parties any portions of the Software embedded in any Generated Files that the State creates while using the Software in the manner in which the Software is designed to be used. In the State's distribution of the Generated Files, the State may not use the Contractor's name, logo, or trademarks, except to the extent that such are incorporated in such Generated Files by the design of the Software when used as intended.

3. **License Restrictions.** The State may not reverse engineer, de-compile, or disassemble any Software for which it is not licensed to use the Software's Source Code. Additionally, the State may not assign, transfer, or redistribute the Software to any party in whole or in part, except as expressly provided by this Contract or the applicable Schedule. It also may not rent, time share, or operate a service bureau with respect to the Software. And the State may not charge a fee to any third party for access to or use of the Software, unless this Contract or the applicable Schedule permits such. (One Affiliated Entity using the Software on behalf of another Affiliated Entity is not the operation of a service bureau for purposes of this Contract, even if the Affiliated Entity charges the other Affiliated Entity for the costs of the service.) Additionally, except as authorized in this Contract or the applicable Schedule, the State may not grant any sublicense to access or use the Software. Notwithstanding the foregoing, and provided they have agreed in writing to honor the terms of this Contract, the State's Affiliated Entities may use the Software in the same manner as the State, subject to the applicable limits on the license and the obligations contained in this Contract. Further, for any Software designed for communications, such as e-commerce applications, or for Web presentations, the State may communicate with third parties using the Software and use the Software for presentations to third parties via the Internet. Additionally, the State engages various contractors to do work for it, and the State may

provide such contractors with access to and use of the Software solely for use on behalf of the State, including in a facilities management, hosting, disaster recovery, or outsourcing arrangement. But the State may not provide access to the Software to any such contractors except for use solely on behalf of the State.

4. **Locking Devices.** Some Software may require the use of a key to prevent unauthorized installation and use of the Software, but the Software may not include expiration codes, "time bombs", or similar devices that can disable the software once a proper key is provided. Further, the software may not contain any routines, functions, or devices that can or are designed to transmit or transfer any data surreptitiously to the Contractor or any other party. Nor may the software contain any routines, functions, or similar devices designed to permit the Contractor or a third party to surreptitiously access data on the State's network or on any of the State's computers. Should the State need assistance with a key or similar device to use the Software within the State's scope of license, the Contractor will assist the State at any time and without charge or fee, regardless of whether such Software is then under Support.

5. **Copies.** In addition to the copies of the Software authorized by the license in the applicable Schedule, the State may make a reasonable number of copies of the Software for backup, archival, disaster recovery, testing, development, and image management purposes. And the State may use these copies for such purposes without paying any additional fee or charge, so long as any such additional copies are not used in a production environment while the production copy or copies of the Software are used for production. No other copies of the Software may be made by or for the State. With respect to the Documentation for any Software, the State may make as many copies of it in either paper-based or electronic form as the State may reasonably require for its own internal purposes. Additionally, the State may incorporate portions of the Documentation in other materials, such as training and reference manuals, provided that such materials are used solely for the internal purposes of the State and the use bears a reasonable nexus to the State's use of the Software. Each copy of the Software or Documentation that the State makes must bear the same copyright and other proprietary notices that appear on the original copy provided to the State. If the Contractor has granted the State a license to use the Source Code for the Software, the State may make a reasonable number of copies of the Source Code, modify it, compile it, and otherwise use it as reasonably necessary to support its licensed use of the Software.

6. **Hazardous Environments.** The State recognizes that some Software may not be designed or intended for use as or with online control equipment or systems in hazardous environments requiring fail-safe performance. This includes equipment or systems such as those used in the operation of nuclear facilities, aircraft navigation, air traffic control, direct life support machines, and munitions. It also includes any other equipment or systems in which the State reasonably can foresee that failure of the Software could lead to death, personal injury, or severe physical or environmental damage. For any Software designated as not intended for hazardous environments in the applicable Schedule, the State may not use or permit the use of the Software in conjunction with any such equipment or systems.

7. **Object Reassignment.** Any Software licensed by the number of items that it may be used on, by, or in conjunction with, such as nodes, computers, users, or sites ("Objects"), may be reassigned to other, similar Objects within the State at any time and without any additional fee or charge. For example, a computer-specific license may be transferred to another computer, a site license may be transferred to another site, and a named user license may be assigned to another user. But any such reassignment must be in conjunction with termination of use by or with the previous Object, if such termination is required to keep the total number of licensed Objects within the scope of the applicable license. Should the State require a special code, a unique key, or similar device to reassign the Software as contemplated by this section, the Contractor will provide such a code, key, or similar device to the State at any time and without a fee or charge, regardless of whether such Software is then under Support. A later section in this Contract governs assignment of the State's license in any Software to a successor in interest.

8. **Upgrades, Updates, and Corrections.** All portions of the Software, including any corrections, patches, service packs, updates, upgrades, and new versions and releases are the property of Contractor, are part of the Software, and are governed by the State's license in the Software. In no event will the Software or any modification of it be deemed a work made for hire, even if the Contractor has made the modification expressly for the State, unless the parties agree otherwise in writing.

PART II: FEES AND PAYMENT

1. **Fees**. The State will pay to the Contractor the fees for licensing the Software identified in each Schedule under this Contract ("License Fees"), as well as all applicable fees for Support of the Software ("Support Fees") that are identified in any Schedule under this Contract. The License Fee for each license is due and payable on the 30th day after the later of the date on which the applicable license starts (the "Start Date") or the date the State receives a proper invoice for the License Fee at the office designated in the applicable purchase order. A Support Fee will be due payable on the 30th day after the later of the date on which the applicable period of Support (the "Support Period") begins or the date the State receives a proper invoice for the

Support Fee at the office designated in the applicable purchase order. The State will not be obligated to acquire or renew Support for any Software unless it issues a purchase order for such.

2. **Taxes**. The State is exempt from all sales, use, excise, property, and similar taxes ("Taxes"). To the extent any Taxes are imposed on the Contractor in connection with this Contract or the Software, the Contractor must pay such Taxes, together with any interest and penalties not properly disputed with the appropriate taxing authority.

3. **Invoices.** The Contractor must submit an original invoice with three copies to the office designated in the purchase order as the "bill to" address. To be a proper invoice, the invoice must include the following information:

   (1) Name and address of the Contractor, as designated in this Contract.
   (2) The Contractor's federal tax identification number, as designated in this Contract.
   (3) The Contractor's invoice remittance address, as designated in this Contract.
   (4) The purchase order number authorizing the delivery of the Software or Support.
   (5) A description of what the Contractor delivered, including, as applicable, the time period, serial number, unit price, quantity, and total price of the Software and Support. If the invoice is for Software with multiple installments of the License Fee, the Contractor also must include the payment number (e.g., 11 of 36).

   If an invoice does not meet this section's requirements, or if the Contractor fails to give proper notice of a price increase (see the Pricing section below), the State will send the Contractor written notice. The State will send the notice, along with the improper invoice, to the Contractor's address designated for receipt of purchase orders within 15 days. The notice will contain a description of the defect or impropriety and any additional information the Contractor needs to correct the invoice. If such notification has been sent, the payment due date will be 30 days after the State receives a corrected and proper invoice or the applicable Start Date in the Schedule, whichever is later.

   The date the State issues a warrant (the State's equivalent to a check) in payment of an invoice will be considered the date payment is made. Without diminishing the Contractor's right to timely payment, the payment will be overdue only if it is not received by the 30th day after the payment's due date. If the State has not issued payment by then, interest will begin to accrue under Ohio Revised Code ("Code") Section 126.30.

4. **Non-Appropriation of Funds.** The State's funds are contingent on the availability of lawful appropriations by the Ohio General Assembly. If the Ohio General Assembly fails to continue funding for the Fees due hereunder, as determined by the Director of the Department of Administrative Services, this Contract will terminate with respect to the Software or Support affected by the non-appropriation as of the date that the funding expires, and the State will have no further obligation to make any payments. This provision will not alter the rights of the State in any Software or to any Support for which the State already has made payment at the time of the non-appropriation.

5. **OBM Certification.** This Contract is subject to Code Section 126.07. All orders and Schedules under this Contract are void until the Director of the Office of Budget and Management for the State certifies that there is a balance in the appropriation available to pay for the order.

6. **Currency.** The State will make all payments under this Contract by warrant (the State's equivalent to a check) in US Dollars, regardless of the location where the Support is provided or the Software is located.

7. **Disputed Amounts.** The parties will resolve any amounts disputed under this Contract expeditiously and in good faith by having the representatives of the parties who signed this Contract enter into informal discussions. Once resolved through the dispute resolution process, the amount must be paid within 30 days of the resolution. If the State disputes any amount under this Contract in good faith, the State may withhold its payment pending resolution notwithstanding anything to the contrary elsewhere in this Contract.

8. **Pricing.** Subject to the limitations in this section, the Contractor may modify its pricing for Software or Support at any time and without notice to the State. But no such change will apply to any Software or Support that the State orders or for which it receives an invoice before the effective date of the change. Nor will any price increase apply to any Software for which the State and the Contractor have entered in to a Price-hold Addendum; the pricing for such Software will be fixed for the term of the price-hold. Additionally, for five years from the date of the State's first license of any Software, the State will be entitled to acquire additional licenses for the same Software at a discount that is equal to the discount extended to the State for the initial license of the Software, even though the list price for the Software may have increased. Such licenses will be granted under the terms contained in this Contract via the execution of a Schedule hereto. Thereafter, the State will not be obligated to pay more than the Contractor's then current, published License Fee for any such Software, less the discount described in the

following sentence. For all additional licenses acquired more than five years after the initial license in the same Software, the State still will be entitled to a discount of [redacted]% from the then current list price for the license. Support Fees under this Contract may not increase from one Support Period to the next by more than [redacted] percent for any license in the Software. Further, in no event will the Support Fee the State pays be greater than the fee paid by any other customer of the Contractor for the same type license.

PART III: CONTRACT ADMINISTRATION

1. **Term.** Once entered into, the term of this Contract will be from the date the duly authorized representative of the State signed it through June 30, 201[redacted]. Expiration of this Contract without renewal will not affect any licenses granted to the State before the expiration. It also will not affect the rights and the responsibilities of the parties with respect to such licenses.

2. **Renewal.** The State may renew this Contract for additional two-year terms, subject to and contingent on the discretionary decision of the Ohio General Assembly to appropriate funds for this Contract in each new biennium. Any such renewal of this Contract also is subject to the satisfactory performance of the Contractor and the needs of the State. The State's failure to renew this Contract will not affect any licenses granted to the State before the expiration. It also will not affect the rights and the responsibilities of the parties with respect to such licenses.

3. **Delivery.** The Contractor must deliver all Software licensed under this Contract to the State F.O.B. at the State's site specified in the applicable Schedule. If the Contractor and the State agree so in writing, the Contractor may deliver any Software licensed under this Contract via electronic transmission over the Internet, provided the Contractor maintains sufficient bandwidth to accommodate delivery in this fashion. Upon physical delivery or successful completion of an electronic transmission, title to any media on which the Software and Documentation are contained and risk of loss of the Software and Documentation will pass to the State.

4. **Schedules.** For all Software that the State licenses, the Contractor and the State will enter into a written Schedule to this Contract, signed by duly authorized representatives of both parties. The Schedule will describe the Software, the license granted in the Software, and the date the license starts ("Start Date"). It also will identify the License Fee for the license granted, the number of physical copies of the media on which the Software is shipped, and the operating system or systems for which the Software is designed. In addition, the Schedule will identify the Support Fee or the percentage of the License Fee used to calculate the Support Fee. All additional Software that the State seeks to license from the Contractor under this Contract, as well as all additional licenses that the State wishes to acquire in Software already licensed under this Contract, will be subject to the Contractor's prior, written approval in each such case. But the Contractor will consent for any Software that is covered by a Price-hold Addendum. The Contractor also must consent for any Software that is or designed to operate in conjunction with Software already acquired by the State under this Contract, if the Software at issue is generally available to other customers and the State is not in material breach of this Contract.

5. **Confidentiality.** Each party may disclose to the other written material or oral or other forms of information that it treats as confidential ("Confidential Information"). Title to any Confidential Information one party deliverers to the other will remain with the disclosing party or its licensors. Each party agrees to treat any Confidential Information it receives from the other party as secret, if it is so marked, otherwise identified as such, or when, by its very nature, it deals with matters that, if generally known, would be damaging to the best interest of the other party or its licensors.

   The Contractor's Confidential Information may include the Software and Documentation, if the Software and Documentation are the trade secrets of Contractor and marked as such in a reasonable manner. Information of the State that the Contractor must presume to be Confidential Information, regardless of whether it is marked as such, includes any proprietary documentation, materials, flow charts, codes, software, computer instructions, techniques, models, information, diagrams, know-how, data, business records, and business plans. Such also includes files containing personal information about other contractors or employees of the State, such as personnel records, and any material to which an attorney-client, physician-patient, or similar privilege may apply. It also includes any State records that Ohio law excludes from public records disclosure requirements.

   Each party agrees not to disclose any Confidential Information of the other to any third parties and to use it solely to meet its obligations under this Contract or as otherwise contemplated under this Contract. Additionally, each party will restrict circulation of Confidential Information within its organization and permit access to it only by people who have a need to know the Confidential Information for the purposes contemplated by this Contract.

   Except for Software, Source Code, or Documentation that represents Confidential Information, neither party may incorporate any portion of the other party's Confidential Information into any work or product. With respect to Software, Source Code, or

Documentation that is Confidential Information, the foregoing will not apply to any portion of the Software incorporated into Generated Files by the design of the Software when used as intended. Nor will the foregoing apply to portions of the Documentation that the State incorporates into material such as training and reference manuals in accordance with this Contract's applicable provisions. And the foregoing will not apply to any Source Code properly licensed to the State that the State modifies for use within the scope if its license in the applicable Software. Furthermore, the receiving party must cause all of its personnel who have access to any Confidential Information of the other party to execute a confidentiality agreement incorporating the obligations of this section. Additionally, for any director, officer, employee, partner, agent, or subcontractor of the Contractor ("Contractor Personnel") that require access to the State's premises, the State may require an individual non-disclosure agreement incorporating the terms of this section to reinforce the importance of such obligations. The State may bar any Contractor Personnel who refuse to execute such a non-disclosure agreement from entering the State's facilities.

The receiving party's obligation to maintain the secrecy of the Confidential Information will not apply where it:

(a) Was already in the receiving party's possession before disclosure by the other party, and the receiving party obtained it without an obligation of confidence;
(b) Is independently developed by the receiving party;
(c) Except as provided in the next paragraph, is or becomes publicly available without breach of this Contract;
(d) Is rightfully obtained by the receiving party from a third party without an obligation of confidence;
(e) Is disclosed by the receiving party with the written consent of the other party; or
(f) Is released in accordance with a valid order of a court or governmental agency, provided that the receiving party:

    (1) Notifies the other party of such order immediately upon receipt of the order; and
    (2) Makes a reasonable effort to obtain a protective order from the issuing court or agency limiting disclosure and use of the Confidential Information solely for the purposes intended to be served by the original order of production.

Information that may be available publicly through other sources about people that is personal in nature, such as medical records, addresses, phone numbers, social security numbers, and similar things are nevertheless sensitive in nature and may not be disclosed or used in any manner except as expressly authorized in this Contract. Therefore, item (3) in the preceding paragraph does not apply, and the Contractor must treat such information as Confidential Information whether it is available elsewhere or not.

Except for properly licensed Software, Source Code, or Documentation that contains Confidential Information, the receiving party must return or destroy all copies of any Confidential Information when it is no longer needed for the receiving party to perform under this Contract, but in any case, no later than on termination of this Contract. For properly licensed Software, Source Code, and Documentation that represents Confidential Information, the State may retain it for so long as the State has a valid license in it.

The receiving party may disclose Confidential Information to its contractors on a need-to-know basis, but only after they have agreed in writing to be obligated to the requirements of this section.

6. Escrow. Except for Software that the Contractor delivers to the State with its Source Code, the Contractor must escrow the Source Code for all Software with Escrow Associates, LLC (the "Agent") an NCC company under an existing escrow agreement between the State and the Agent. The Agent may release the Source Code to the State on the occurrence of any of the following:

(a) The Contractor ceases business without a successor in interest that assumes all the Contractor's obligations under this Contract;
(b) The Contractor files or has filed against it a petition in bankruptcy or similar proceeding that is not dismissed within 60 days;
(c) The Contractor stops supporting any Licensed Software;
(d) The State terminates this Contract for cause; or
(e) The Contractor materially or consistently fails to perform its Support obligations in a timely and professional manner.

The release will apply only to the Source Code for Software affected by the triggering event. The Source Code for the Software will be in the form customarily used by programmers to read and modify such Source Code. It also will include all supporting documentation and annotations reasonably required for productive use of the Source Code by a competent programmer skilled in the programming language in which the Source Code is written. The Contractor will deliver to the Agent

the Source Code for each version or release of the Software that the State acquires. The State will be solely responsible for paying all escrow fees associated with the escrow agreement, and upon any release of Source Code from escrow, the State will treat the material as Confidential Information and use it solely to maintain the Software for its own internal purposes.

The escrow agreement with the Agent is a supplementary agreement to this Contract, within the meaning of Title 11, Section 365(n), of the United States Code, and neither the Contractor nor its trustee in bankruptcy may interfere with the State's license in the Software or right to access any Source Code by virtue of any bankruptcy proceedings.

From time to time, the State may change the company it uses as the Agent. The State will do so only on written notice to the Contractor and will use only a US-based, well-recognized escrow company.

7. **Insurance.** The Contractor must provide the following insurance coverage at its own expense throughout the term of this Contract:

(a) Workers' compensation insurance, as required by Ohio law, and, if some of the Project will be done outside Ohio, the laws of the appropriate state(s) where work on the project will be done. The Contractor also must maintain employer's liability insurance with at least a $1,000,000.00 limit.

(b) Commercial General Liability insurance coverage for bodily injury, personal injury, wrongful death, and property damage. The defense cost must be outside of the policy limits. Such policy must designate the State of Ohio as an additional insured, as its interest may appear. The policy also must be endorsed to include a waiver of subrogation. At a minimum, the limits of the insurance must be:

$ 2,000,000 General Aggregate
$ 2,000,000 Products/Completed Operations Aggregate
$ 1,000,000 Per Occurrence Limit
$ 1,000,000 Personal and Advertising Injury Limit
$ 100,000 Fire Legal Liability
$ 10,000 Medical Payments

The Contractor shall, for each policy required by this Contract, provide the State with 30-days prior written notice of cancellation, material change, or non-renewal, except a 10-days notice of non-payment of premium. And the Contractor's Commercial General Liability must be primary over any other insurance coverage.

(c) Commercial Automobile Liability insurance with a combined single limit of $500,000.

(d) Professional Liability insurance covering all staff with a minimum limit of $1,000,000 per incident and $3,000,000 aggregate. If the Contractor's policy is written on a "claims made" basis, the Contractor must provide the State with proof of continuous coverage at the time the policy is renewed. If for any reason the policy expires, or coverage is terminated, the Contractor must purchase and maintain "tail" coverage through the applicable statute of limitations.

The certificate(s) must be in a form that is reasonably satisfactory to the State as to the contents of the policies and the quality of the insurance carriers. All carriers must have at least an "A-" rating by A.M. Best.

8. **Excusable Delay.** Neither party will be liable for any delay in its performance under this Contract that arises from causes beyond its control and without its negligence or fault. The delayed party must notify the other promptly of any material delay in performance and must specify in writing the proposed revised performance date as soon as practicable after notice of delay. For any such excusable delay, the date of performance or delivery will be extended for a period equal to the time lost by reason of the excusable delay. The delayed party must also describe the cause of the delay and what steps it is taking or will take to remove the cause. The delayed party may not rely on a claim of excusable delay to avoid liability for a delay if the party has not taken commercially reasonable steps to mitigate or avoid the delay.

9. **Network Security.** The Contractor may not connect to the State's internal computer network without the prior, written consent of the State, which the State will reasonably provide if necessary or appropriate for the Contractor to provide Support. But as a condition of connecting to the State's computer network, the Contractor must secure its own connected systems in a

manner consistent with the State's then-current security policies, which the State will provide to the Contractor on request. The State may audit the Contractor's security measures in effect on any such connected systems without notice. The State also may terminate the Contractor's network connections immediately should the State determine that the Contractor's security measures are not consistent with the State's policies or are otherwise inadequate given the nature of the connection or the data or systems to which the Contractor may have access.

10. **Termination**. This Contract will continue in full force and effect unless terminated according to the terms of this Contract. Either party may terminate this Contract at any time on 30 days prior written notice to the other party or in the event of any default by the other party, which the defaulting party fails to cure within 30 days after written notice. Either party also may terminate this Contract upon any sale of a majority interest in the other party to a third party or if a receiver, liquidator, trustee, or like official is appointed for the other party or any substantial portion of its property. Additionally, either party may terminate this Contract if the other party files or consents to any petition in bankruptcy or other insolvency proceedings or makes any assignment for the benefit of its creditors. Termination of this Contract will not extinguish any of the rights and obligations of a party under this Contract that, by the terms of that right or obligation, continue after the date of termination. And no termination will extinguish any of the rights or obligations that, by their very nature, must continue after termination to give full effect to the purpose of those rights and obligations. Termination of this Contract will not entitle the State to any refund of any License or Support Fee, nor will it extinguish any license or price-hold the State has acquired in any Software before the date of termination, except as provided in the next paragraph.

    With or without terminating this Contract in accordance with the paragraph above, on 30 days prior written notice to the State, the Contractor may terminate any license in any Software granted to the State under this Contract. But the Contractor may do so only if the State materially breaches any terms of this Contract with respect to the license or licenses the Contractor seeks to terminate. Such termination notice will be effective 30 days after the State receives it, provided that the State does not cure its breach of this Contract within those 30 days. All Software licenses not affected by the State's breach will remain in place and unaffected by the termination. Any such termination will be in addition to any other remedies the Contractor may have under this Contract for the State's breach.

PART IV: WARRANTIES, LIABILITIES, AND REMEDIES

1. **Warranties**. The Contractor warrants for one year from the Start Date that the Software will be free of material defects and will function in substantial conformance to its Documentation when used in the operating environment for which it is intended and in accordance with its Documentation. The Contractor also warrants that the Software will be merchantable and fit for the particular purpose for which the State acquired it**.** Moreover, the Contractor warrants that the Software will be free of viruses at the time of its delivery under this Contract. Additionally, the Contractor warrants that all media on which the Software is delivered to the State will be free from defects for one year after delivery to the State.

2. **Warranty Exclusions.** The Contractor's warranties with respect to the Software's performance in accordance with its Documentation, its fitness, and its merchantability do not cover any error caused by any change to the Software made by any party other than the Contractor and not at the Contractor's request or otherwise in accordance with this Contract or the Software's Documentation. It also does not cover damage to the Software caused by accident, neglect, or misuse of the Software by any party other than the Contractor or anyone else acting on the Contractor's behalf. Further, the State's use of the Software in an operating environment or in conjunction with a hardware platform that does not meet the Contractor's minimum specifications, as set out in the applicable Schedule or Documentation, may result in errors or failures that are outside the scope of the Contractor's warranty. Additionally, use of the Software in combination with other software, hardware, firmware, data, or technology not licensed or approved by the Contractor in writing may cause failures that also are outside the scope of the Contractor's warranty, provided that the Software is not designed or intended for use with such items.

    THE EXPRESS WARRANTIES IN THIS CONTRACT ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED.

3. **Remedies.** The Contractor's entire liability and the State's sole remedy for any breach of the above media warranty is limited to requiring the Contractor to replace the defective media expeditiously and without charge to the State. Furthermore, the Contractor's entire liability and the State's sole remedy for any breach of the above warranties of fitness, merchantability, and against defects in the Software will be limited to the Contractor expeditiously correcting the defect or issue and providing the State with a patch containing the correction. If within the times given below, the Contractor does not provide a replacement copy for defective media or Software containing a virus or fails to deliver a fix for a defect in the Software or a correction solving a fitness or merchantability issue, the Contractor must refund all License Fees paid by the State for the affected the Software. In the case of defective media or Software containing a virus, the Contractor will have 15 days after written notice to provide a replacement. In the case of other defects, merchantability issues, or fitness issues, the Contractor will have 30

days after written notice to deliver a correction that resolves the problem. Upon the Contractor's issuance of a refund, the State will return or destroy all copies of the Software and, upon the Contractor's request, certify in writing that it has done so.

THE FOREGOING REMEDIES ARE THE STATE'S EXCLUSIVE REMEDIES FOR THE WARRANTIES PROVIDED ABOVE.

4. **Indemnity.** The Contractor will indemnify the State for all direct damages to the State caused by the negligence or willful misconduct of the Contractor. The Contractor also agrees to indemnify, defend, and hold the State harmless from and against all claims, liabilities, demands, losses, expenses (including by way of example only, court costs and experts' and attorneys' fees), and causes of action of every kind and character in favor of any third party caused or arising out the activities or performance of the Contractor or the Contractor's Personnel. The foregoing obligations do not apply to the extent caused by the State's actual negligence or willful misconduct. Any defense of the State requires and is subject to the approval and consent of the Ohio Attorney General.

5. **Infringement.** The Contractor will release, protect, indemnify, defend, and hold the State harmless from and against any claims of infringement by any third parties based on the Software, Source Code, or Documentation licensed under this Contract. Any defense of the State requires and is subject to the approval and consent of the Ohio Attorney General and will be at the Contractor's sole cost and expense. Further, the Contractor will indemnify the State for any liability resulting from any such claims, demands, or suits, as well as hold the State harmless for the Contractor's liability, losses, and damages resulting from such. This obligation of defense and indemnification will not apply where the State has modified or misused the Software, Source Code, or Documentation, and the claim or the suit is based on the modification or misuse. The Contractor's obligation to hold the State harmless also will not apply if the claim, suit, liability, or damage arises out of the State's misuse of the Software, Source Code, or Documentation. The State agrees to give the Contractor notice of any such claim as soon as reasonably practicable and to allow the Contractor to control the defense of the any such claim, upon consultation with and the approval of the Office of the State's Attorney General.

   If a successful claim of infringement is made, or if the Contractor reasonably believes that an infringement or similar claim that is pending actually may succeed, the Contractor will do one of the following four things as soon as reasonably possible to avoid or minimize any interruption of the State's business:

   (a) Modify the offending Software, Source Code, or Documentation so that it is no longer infringing;
   (b) Replace the offending Software, Source Code, or Documentation with an equivalent or better item;
   (c) Acquire the right for the State to use the infringing Software, Source Code, or Documentation as it was intended for the State to use under this Contract; or
   (d) Remove the infringing Software, Source Code, or Documentation and refund the amount the State paid for the Software and the amount of any other Software or item that requires the availability of the infringing Software, Source Code, or Documentation for it to be useful to the State.

6. **LIMITATION OF LIABILITY. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS CONTRACT, NEITHER PARTY WILL BE LIABLE FOR ANY DAMAGES OTHER THAN DIRECT DAMAGES. THIS EXCLUSION OF DAMAGES INCLUDES, BY WAY OF EXAMPLE ONLY, INDIRECT, INCIDENTAL, EXEMPLARY, AND CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF PROFITS, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES. ADDITIONALLY, NEITHER PARTY WILL BE LIABLE FOR DIRECT DAMAGES IN EXCESS OF TWO TIMES THE TOTAL LICENSE AND SUPPORT FEES UNDER THIS CONTRACT. BUT THIS LIMITATION OF LIABILITY WILL NOT LIMIT THE CONTRACTOR'S OBLIGATION TO INDEMNIFY THE STATE UNDER THE INDEMNITY AND INFRINGEMENT PROVISIONS OF THIS CONTRACT FOR DIRECT DAMAGES FROM THE CONTRACTOR'S NEGLIGENCE OR WILLFUL MISCONDUCT. THIS LIMITATION OF LIABILITY ALSO WILL NOT LIMIT THE CONTRACTOR'S OBLIGATIONS UNDER THE INDEMNITY AND INFRINGEMENT SECTIONS OF THIS CONTRACT FOR CLAIMS MADE AGAINST THE STATE FOR INFRINGEMENT OR FOR NEGLIGENCE OR WILLFUL MISCONDUCT OF THE CONTRACTOR, REGARDLESS OF THE NATURE OF THE DAMAGES SOUGHT FOR ANY SUCH CLAIM. THIS LIMITATION OF LIABILITY WILL SURVIVE TERMINATION OF THIS CONTRACT.**

PART V: SOFTWARE SUPPORT

1. **Support.** Each Support Period will be one year in duration, with the first Support Period beginning on the [first anniversary of the] Start Date for the applicable license. Subsequent Support Periods will begin on each anniversary of the Start Date of the applicable license (the "Anniversary Date"). During each Support Period for which the State has paid the applicable Support Fee, the Contractor will provide the State with telephonic assistance and advice for using the Software. The Contractor also will provide remote troubleshooting and problem resolution by developing and providing fixes or patches for errors in the

Software. As part of the annual Support that the Contractor provides in exchange for the applicable Support Fee, the Contractor also will deliver to the State all service packs for the Software, as well as all updates and new releases and versions of the Software. The annual Support Fee will be calculated as a percentage of the then current License Fee for the applicable Software license not to exceed seven percent per year. The percentage used to calculate the Support Fee will be provided in the applicable Schedule governing the Software license. The manner in which the Contractor provides Support will be governed by the Contractor's policies and programs described in the applicable Software Documentation or other materials that the Contractor uses to notify its customers generally of such policies. But regardless of the Contractor's policies and programs, unless otherwise agreed in the applicable Schedule, in all cases such Support must comply with the requirements of this Contract. And the Contractor must provide the Support in a competent, professional, and timely manner.

2. **Minimum Availability.** Support for any Software licensed under this Contract must be available for a minimum of five years from the Start Date of the license. Thereafter, for so long as the Contractor makes Support available to other customers, the State will be entitled to participate in that Support under the terms of this Contract and in exchange for the Support Fee identified in the applicable Schedule.

3. **Reductions.** The State may acquire licenses that are based on the number of users, nodes, computers, processors, instances of the Software or other counts of objects covered by a license ("Objects"). In any such cases, the State may request that the Support Fees for a Support Period be calculated based on fewer Objects than included in the previous Support Period, with an appropriate adjustment in the applicable Support Fee. But patches, services packs, updates, and new versions or releases of the Software made available to the State under this Contract for such Software may be applied only to the number of Objects included in the then current Support Period. Nevertheless, the State may continue using any version of the Software that is available at the time Support was reduced on or for the unsupported Objects, provided that such is physically possible based on the Software's configuration. In any case where supported and unsupported Objects cannot be treated separately (e.g., a single server license supporting multiple concurrent connection), the State must limit its use of the Software to the supported number of Objects to take advantage of its reduction rights under this section.

4. **Lapse and Reinstatement.** If the State opts to not renew Support for some or all of the Software licensed by the State under this Contract, the State may subsequently purchase Support for such Software. But it may do so only if the Contractor continues to make it generally available to its customers when the State makes the decision to reacquire Support. Further, any such Support will require, in addition to the Support Fee for the then current Support Period, the payment of the immediately preceding year's Support Fees for that Software, or the applicable instances of it. Notwithstanding anything to the contrary in this Contract, no interest will be due on the Support Fees for the past Support Periods. In conjunction with the reinstatement of Support, the State will be entitled to any patches, service packs, upgrades, and new releases, and versions of the Software issued during the unsupported interval.

5. **Support Parameters.** The State may initiate Support requests for problems it encounters with the Software by telephone, email, Internet, or fax, and the Contractor must maintain lines of communication that support all four forms of communication. The Contractor must make Support available from at least 7:00 a.m. to 700 p.m. in each time zone where the Contractor maintains a Support center, and it must do so by staffing its Support function with an adequate number of qualified personnel to handle its traditional volume of calls. Further, the Contractor must maintain at least one Support center in North America with adequate English-speaking Support personnel. Support must be available during the business hours identified above from at least Monday through Friday throughout the Support Period, except for customary holidays. Further, subject to the State's obligation to pay the applicable Support Fees, the Contractor must support both the most recent major release of the Software as well as the immediately preceding major release of Software. The State's technical staff may contact any Support center that the Contractor maintains, and they may choose to do so based on convenience, proximity, service hours, languages spoken, or otherwise.

6. **Incident Classification.** The Contractor must classify and respond to Support calls by the underlying problem's effect on the State. In this regard, the Contractor may classify the underlying problem as critical, urgent, or routine. The guidelines for determining the severity of a problem and the appropriate classification of, and response to, it are described below.

   The Contractor must designate a problem as "critical" if the Software is functionally inoperable, the problem prevents the Software from being used in production mode or there is significant potential for data integrity problems. This classification assumes there is no existing patch for the problem. The Contractor must classify a problem as "urgent" if the underlying problem significantly degrades the performance of the Software or materially restricts the State's use of the Software in a production mode. A problem also will be considered urgent if a commonly used feature often generates application errors, causes the Software to freeze, locks up the computer on which the Software is running, or otherwise routinely does not work as intended. Classification of a problem as urgent rather than critical assumes that the State still can conduct business with the Software. As with the critical classification, the urgent classification assumes there is no existing patch or acceptable

workaround procedure for the problem. Finally, the Contractor may classify a Support call as "routine" if the underlying problem is a question on end use or configuration of the Software. It also may be classified as routine when the problem does not materially restrict the State's use of the Software in its production environment, such as when a feature or combination of features generates minor or rare errors. Also, if any problem that otherwise should be classified as critical or urgent can be solved either by a known workaround or an existing patch, the problem may be treated as routine.

The Contractor must apply the above classifications in good faith to each call for Support, and the Contractor must give due consideration to any request by the State to reclassify a problem, taking into account the State's unique business and technical environments and any special needs it may have.

7. **Incident Response.** The Contractor must respond to critical problems by ensuring that appropriate managerial personnel are made aware of the problem and that they actively track and expedite a resolution. The Contractor must assign Support or development personnel at the appropriate level to the problem, and those personnel must prepare a work plan for the problem's expeditious resolution. The work plan must assume that the Contractor's appropriate staff will work without material interruption until the problem is resolved properly. The Contractor's personnel must maintain daily contact with the State's technical staff to keep the State abreast of efforts being made to solve the problem. The Contractor also must provide the State's technical staff with direct access to the Contractor's Support personnel and product development personnel, if appropriate, who are assigned to the problem. If the resolution of the problem requires a patch, the Contractor will ship the patch electronically as soon as the patch is available.

   The Contractor must respond to urgent problems by having its product development and Support personnel work in concert to develop a fix or a workaround. The Contractor's Support personnel must maintain regular contact with the State to keep its technical staff abreast of progress toward a resolution of the problem. The Contractor's Support staff must include the problem in regular status reports to the Contractor's management team. And the Contractor's Support staff must provide the Software patch or workaround procedure as soon as it is available.

   The Contractor must respond to routine problems by providing the State with a patch or workaround on a priority basis if the problem is one for which an existing patch or workaround already exists. For newly identified problems falling into this classification, the Contractor's Support personnel must generate a problem report, and the appropriate development or Support personnel then must prioritize the problem in relation to other outstanding product issues. The assigned priority then will govern the problem solving or developmental work needed to address the problem and the schedule for delivering a solution. For routine calls that involve end usage and configuration issues rather than bugs or other technical problems, the Contractor's first or second level Support personnel must provide the State's technical staff with telephonic assistance on a non-priority basis.

8. **Response Times.** The maximum time that the Contractor takes to respond initially to a Support request may vary based upon the classification of the request. During normal hours of operation for the Contractor's Support function, the Contractor's response time for a critical Support request will be less than one hour. The Contractor's response time for an urgent request must be less than two hours during operating hours. And the Contractor's response time for a routine Support request must be less than four hours during normal operating hours.

9. **Escalation Process.** Any Support call that is not resolved must be escalated to the Contractor's management under the following parameters. Unresolved problems that are classified as critical must be escalated to the Contractor's Support manager within four hours and to the director level after one day. If a critical problem is not resolved within three days, it must escalate to the corporate officer level and then to the CEO level after five days. The Contractor's Support staff will escalate unresolved urgent problems to its Support manager within three days, to the director level after seven days, and to the corporate officer level after 14 days.

10. **State Obligations.** To facilitate the Contractor meeting its Support obligations, the State must provide the Contractor with the information reasonably necessary to determine the proper classification of the underlying problem. It also must assist the Contractor as reasonably necessary for the Contractor's Support personnel to isolate and diagnose the source of the problem. Additionally, to assist the Contractor's tracking of Support calls and the resolution of Support issues, the State must make a reasonable effort to use any ticket or incident number that the Contractor assigns to a particular incident in each communication with the Contractor. The State also must install and implement the most recently available Software updates, including service packs and patches, if the Contractor reasonably believes it to be necessary to achieve a satisfactory resolution of a problem.

11. **Limitations.** The Contractor is not responsible for the resolution of problems caused by the State's use of the Software on hardware that does not meet the minimum specifications set out in the Software's Documentation. The Contractor also is not

responsible for resolving problems caused by third party software not approved by the Contractor for use with the Software. Additionally, the Contractor need not resolve problems caused by unauthorized modifications to the Software.

12. **Updates.** The Contractor must make all Software updates and service packs, as well as new releases and new versions of it, available to the State at no additional charge and as part of its Software Support. The Contractor will notify the State of the availability of any Software updates and new versions and releases on at least a quarterly basis. The Contractor may post patches and updates on the Internet rather than delivering them to the State on physical media. The Contractor must provide Support, including upgrades, service packs, new releases, and new versions, as appropriate, to keep current with changes in the operating systems and critical applications with which the Software is designed to run for a minimum of five years from the date the Software is licensed to the State. For purposes of the last sentence, a "critical application" is any computer program that the Software is specifically designed to work in conjunction with. An example would be Software that requires an Oracle database engine to function. The Oracle database engine would be a critical application for that Software.

13. **Follow-on Software.** If the Contractor stops supporting or upgrading any Software but then offers or later releases another product that performs substantially similar functions, the State will be entitled to convert its license for the unsupported Software to a license in the new Software. Any such conversion will be without charge to the State, provided only that the State has paid all applicable Support Fees for the unsupported Software since first acquiring it through the time when the Contractor terminated Support.

14. **Functionality Migration.** If the Contractor eliminates functionality material to the use or performance of any Software licensed under this Contract ("Original Software") and then includes the functionality in a new product ("New Software"), the Contractor must grant the State a license to use the migrated functionality of such New Software, but not to any other functionality in the New Software, if (i) the State is a subscriber to Support for the Original Software at the time the New Software is available and is entitled to receive subsequent releases of the Original Software, and (ii) the New Software is available for the same operating system or technical environment as the Original Software. The license granted to the State for the New Software will be (i) pursuant to the terms and conditions of this Contract and the applicable Schedule governing the Original Software, (ii) subject to the use restrictions and other limitations for the Original Software in this Contract and applicable Schedule, (iii) granted without the payment of additional fees other than fees for Support which would otherwise be due for the Original Software.

15. **Support Location.** For each Schedule under this Contract, the Contractor must disclose the location(s) where it will perform all Support, the location(s) where any State data applicable to this Contract will be maintained or made available, and the principal place of business for the Contractor and all its subcontractors that may perform Support under this Contract. While performing under this Contract, the Contractor may not change the location(s) where Support is performed or change the location(s) where it maintains or makes the State's data available to a location outside the country of the original location(s) without prior, written approval of the State, which the State is not obligated to provide. Further, each of the Contractor's subcontractors that perform Support under this Contract must agree in writing to and be bound by this and all other provisions of this Contract that inure to the benefit of the State.

PART VI: CONSTRUCTION

1. **Entire Document.** This Contract will apply to all Software that the State acquires from the Contractor during the term of this Contract, unless the parties expressly agree otherwise in a written document signed by the duly authorized representatives of the parties. Furthermore, this Contract, along with the Schedules and Addenda entered into under it, is the entire agreement between the parties with respect to its subject matter, and it supersedes any previous statements or agreements, whether oral or written.

2. **Additional Documents.** All terms and conditions contained in any document not signed by both parties, such as a purchase order, invoice, or a click-wrap license, are excluded from this Contract and will have no legal effect.

3. **Binding Effect.** Subject to the limitations on assignment provided elsewhere in this Contract, this Contract will be binding upon and inure to the benefit of the respective successors and assigns of the State and the Contractor.

4. **Amendments.** No amendment or modification of any provision of this Contract will be effective unless it is in writing and signed by both parties.

5. **Waiver.** The failure of either party at any time to demand strict performance by the other party of any of the terms of this Contract will not be construed as a waiver or a relinquishment of any such term. Either party may at any later time demand strict and complete performance by the other party of such a term.

6. **Severability.** If any provision of this Contract is held by a court of competent jurisdiction to be contrary to applicable law, the remaining provisions of this Contract will remain in full force and effect to the extent that such does not create an absurdity or material injustice.

7. **Plain Meaning.** This Contract must be construed in accordance with the plain meaning of its language and neither for nor against the drafting party.

8. **Headings.** The headings used herein are for the sole sake of convenience and may not be used to interpret any section.

9. **Notices.** For any notice under this Contract to be effective, it must be made in writing and sent to the address of the appropriate party first appearing above, unless that party has notified the other party, in accordance with the provisions of this section, of a new mailing address for notices.

10. **Continuing Obligations.** To the extent necessary to carry out their purpose, the terms of this Contract will survive the termination of this Contract. Some such provisions that require survival to carry out their full intent include the indemnity, warranty, and limitation of liability provisions. Other examples include the confidentiality section, the escrow section, and the grant of Software licenses. Additional provisions include the Support obligations for existing licenses, and the Pricing section with respect to related Software licenses and caps on increases in Support for existing licenses.

11. **Counterparts.** This Contract may be executed simultaneously in two or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

PART VII: LAW AND COURTS

1. **Compliance with Law.** The parties will comply with all applicable federal, state, and local laws in all endeavors under this Contract.

2. **Export Restrictions.** The State may not directly or indirectly export or transmit the Software or Documentation to any country in violation of any applicable US regulation, order, or statute.

3. **UCITA.** The Uniform Computer Information Transactions Act ("UCITA") will not apply to this Contract. To the extent that UCITA, or any version of it that is adopted by any jurisdiction in any form, is applicable, the parties agree to opt out of it pursuant to the opt-out provisions contained therein. Likewise, the United Nations Convention on Contracts for the International Sale of Goods will not apply to this Contract.

4. **Injunctive Relief.** Nothing in this Contract is intended to limit either party's right to injunctive relief if such is necessary to protect its interests or to keep it whole.

5. **Governing Law.** The laws of Ohio will govern this Contract, excluding its laws dealing with conflict of law, and venue for any disputes will lie exclusively with the appropriate court in Franklin County, Ohio.

PART VIII: MISCELLANEOUS

1. **Conflict of Interest.** No Contractor Personnel may voluntarily acquire any personal interest that conflicts with their responsibilities under this Contract. Further, the Contractor will not knowingly permit any Ohio public official or public employee who has any responsibilities related to this Contract to acquire any interest in anything or any entity under the Contractor's control, if such an interest would conflict with that official's or employee's duties. The Contractor will disclose to the State knowledge of any such person who acquires an incompatible or conflicting personal interest related to this Contract. And the Contractor will take steps to ensure that such a person does not participate in any action affecting the work under this Contract. But this will not apply when the State has determined, in light of the personal interest disclosed, that the person's participation in any such action would not be contrary to the public interest.

2. **Assignment.** Neither party may assign this Contract without the prior, written consent of the other party, which the other party will not withhold unreasonably. Any such assignment, unless otherwise agreed in writing, is contingent on the assignee assuming all the assignor's rights and obligations under this Contract.

3. **Independent Contractor Acknowledgement.** It is fully understood and agreed that Contractor is an independent contractor and is not an agent, servant, or employee of the State of Ohio or the Ohio Department of Administrative Services. Contractor

declares that it is engaged as an independent business and has complied with all applicable federal, state, and local laws regarding business permits and licenses of any kind, including but not limited to any insurance coverage, workers' compensation, or unemployment compensation that is required in the normal course of business and will assume all responsibility for any federal, state, municipal or other tax liabilities. Additionally, Contractor understands that as an independent contractor, it is not a public employee and is not entitled to contributions from DAS to any public employee retirement system.

Contractor acknowledges and agrees any individual providing personal services under this agreement is not a public employee for purposes of Chapter 145 of the Ohio Revised Code. Unless Contractor is a "business entity" as that term is defined in ORC. 145.037 ("an entity with five or more employees that is a corporation, association, firm, limited liability company, partnership, sole proprietorship, or other entity engaged in business") Contractor shall have any individual performing services under this agreement complete and submit to the ordering agency the Independent Contractor/Worker Acknowledgement found at the following link: https://www.opers.org/forms-archive/PEDACKN.pdf" \l "zoom=80

Contractor's failure to complete and submit the Independent/Worker Acknowledgement prior to commencement of the work, service or deliverable, provided under this agreement, shall serve as Contractor's certification that contractor is a "Business entity" as the term is defined in ORC Section 145.037.

4. **Employees.** All Contractor Personnel are employees or contractors of the Contractor, and none are or will be deemed employees or contractors of the State. No Contractor Personnel will be entitled to participate in, claim benefits under, or become an "eligible employee" for purposes of any employee benefit plan of the State by reason of the subject matter of this Contract or work performed under this Contract. The Contractor must pay all federal, state, local, and other applicable payroll taxes and make the required contributions, withholdings, and deductions imposed or assessed under any provision of any law, rule, or regulation and measured by wages, salaries, or other remuneration paid by or which may be due from the Contractor to the Contractor Personnel. The Contractor will indemnify, defend, and hold the State harmless from and against all claims, losses, liability, demands, fines, and expenses (including court costs, defense costs, and redeemable attorney fees) arising out of or relating to such taxes, withholdings, deductions, and contributions with respect to the Contractor Personnel. The Contractor's indemnity and defense obligations also apply to any claim or assertion of tax liability made by or on behalf of any Contractor Personnel or governmental agency on the basis that any Contractor Personnel are employees or contractors of the State, that the State is the "joint employer" or "co-employer" of any Contractor Personnel, or that any Contractor Personnel are entitled to any employee benefit offered only to eligible regular fulltime and regular part-time employees of the State. Notwithstanding the foregoing, any defense of the State requires and is subject to the approval and consent of the Ohio Attorney General.

5. **Publicity.** The Contractor will not advertise or publicize that it is doing business with the State or use this Contract as a marketing or sales tool, unless otherwise agreed to in writing by the State.

6. **Cancellation.** The State may cancel this Contract without cause and on 30 days written notice or at any time if the General Assembly or any other funding source fails to continue funding. But in the case of any license of Software entered before the effective date of the cancellation, the State will have the right to continue such license after termination on the terms contained in this Contract.

7. **Deliveries.** All deliveries will be F.O.B. destination.

8. **Equal Employment Opportunity**. The Contractor will comply with all state and federal laws regarding equal employment opportunity and fair labor and employment practices, including Ohio Revised Code Section 125.111 and all related Executive Orders.

   Before a contract can be awarded or renewed, an Affirmative Action Program Verification Form must be submitted to the Department of Administrative Services Equal Opportunity Division to comply with the affirmative action requirements. Affirmative Action Verification Forms and approved Affirmative Action Plans can be found by going to the Ohio Business Gateway at: http://business.ohio.gov/efiling/.

9. **Drug Free Workplace.** The Contractor must comply with all applicable Ohio laws regarding maintaining a drug-free workplace. The Contractor will make a good faith effort to ensure that all its employees, while working on the State's property, do not possess and will not be under influence of illegal drugs or alcohol or abuse prescription drugs.

10. **Ohio Ethics Law and Limits on Political Contributions**. The Contractor certifies that it is currently in compliance and will continue to adhere to the requirements of the Ohio ethics laws. The Contractor also certifies that all applicable parties listed in Ohio Revised Code Section 3517.13 are in full compliance with Ohio Revised Code Section 3517.13.

11. **Travel Expenses.** Any travel or living expenses required by the Contractor to do its obligations under this Contract will be at the Contractor's expense. The State will pay for any additional travel that it requests only with prior, written approval. All additional travel and living expenses that the State requests in addition to what this Contract requires the Contractor to provide at the Contractor's expense will be paid in accordance with the Office of Budget and Management's Travel Rules in Section 126-1-02 of the Ohio Administrative Code.

12. **Order of Priority.** If there is any inconsistency or conflict between this Contract and any provision of anything incorporated by reference, this Contract will prevail.

13. **Record Keeping**. The Contractor must keep all financial records in accordance with generally accepted accounting principles or equivalent consistently applied. The Contractor will file documentation to support each action under this Contract in a manner allowing it to be readily located. And the Contractor will keep all related records and documents at its principal place of business.

14. **Audits.** During the term of this Contract and for three years after the payment of any fee to the Contractor under this Contract, on reasonable notice and during customary business hours, the State may audit the Contractor's records and other materials that relate to this Contract. This audit right will also apply to the State's duly authorized representatives and any person or organization providing the State with financial support related to this Contract.

    If any audit reveals any misrepresentation or any overcharge to the State, the State will be entitled to recover damages, as well as the cost of the audit.

15. **Ohio Revised Code Section 9.24.** Contractor warrants that it is not subject to an unresolved finding for recovery under Ohio Revised Code Section 9.24. If this warranty was false on the date the parties signed this Contract, the Contract is void. Further, if the Contractor is subject to an unresolved finding of the Auditor of State under Revised Code Section 9.24 on any date on which the parties renew or extend this Contract, the renewal or extension will be void.

16. **Governing the Expenditure of Public Funds on Offshore Services (EO 2011-12K).** The Service Provider affirms it has read and understands Executive Order 2011-12K and will abide by those requirements in the performance of this Agreement. Notwithstanding any other terms of this Agreement, the State reserves the right to recover any funds paid for Services the Service Provider performs outside of the United States for which it did not receive a waiver. The State does not waive any other rights or remedies provided the State in this Agreement.

    The Service Provider agrees to complete the attached Executive Order 2011-12K Affirmation and Disclosure Form (Attachment Nine of the associated RFP), which is incorporated and becomes a part of this Agreement.

17. **Security & Safety Rules.** When using or possessing State data or accessing State networks and systems, the Contractor must comply with all applicable State rules, policies, and regulations regarding data security and integrity. And when on any property owned or controlled by the State, the Contractor must comply with all security and safety rules, regulations, and policies applicable to people on those premises.

18. **Registration with the Secretary of State.** By providing a Charter Number and signature within the Certification Offer Letter, the Contractor attests that the Contractor is:

    An Ohio corporation that is properly registered with the Ohio Secretary of State; or

    A foreign corporation, not incorporated under the laws of the state of Ohio, but is registered with the Ohio Secretary of State pursuant to Ohio Revised Code Sections 1703.01 to 1703.31, as applicable.

    Any foreign corporation required to be licensed under O.R.C. § 1703.01-1703.31, which transacts business in the state of Ohio, without being so licensed, or when its license has expired or been canceled, shall forfeit not less than $250.00 nor more than ten thousand dollars. No officer of a foreign corporation http://codes.ohio.gov/orc/1703.01 shall transact business in the state of Ohio, if such corporation is required by O.R.C. § 1703.01-1803.31 to procure and maintain a license, but has not done so. Whoever violates this is guilty

of a misdemeanor of the forth degree. Questions regarding registration should be directed to (614) 466-3910, or visit http://www.sos.state.oh.us .

TO SHOW THEIR AGREEMENT, the parties have executed this Contract as of the dates appearing below.

FOR THE CONTRACTOR: **CONTRACTOR NAME**	**FOR STATE OF OHIO** **DEPARTMENT OF ADMINISTRATIVE SERVICES**
By: _____	**By:** _____
Name: _____	**Name:** Director of DAS
Title: _____	**Title:** Director
Date: _____	**Date:** _____

PRICE HOLD ADDENDUM NUMBER [0000000.00]

This license addendum ("Addendum") is between the State of Ohio (the "State"), through the Department of Administrative Services, Investment and Governance Division, with offices at 30 East Broad Street, Columbus, Ohio 43215, and *[Company name of the Contractor]* (the "Contractor"), with offices at *[street address, city, state and zip code for the Contractor]*, and is entered into under that certain Master Contract for Software Licensing between the State and the Contractor that is dated *[Date of the Contract]* and numbered [0000000] (the "Contract").

This Addendum does not represent a license of Software. Instead, it provides a price-hold for the Software listed below and permits the State to acquire the Software in exchange for the License Fees and Support Fees listed below. The State is not obligated to license any of the Software listed below, but if it does at any time during the period starting on the date this Addendum is signed and _____ thereafter (Price-hold Period), the State will be entitled to acquire such Software for the Fees specified below. The State may acquire such Software by executing a standard Schedule in the form of that attached to the Contract. The State has the right to acquire some or all of the Software listed below and to acquire the Software in increments during the Price-hold Period using multiple Schedules. Nothing in the Addendum commits the State to any volume of licensing or total expenditure. The State may acquire some, all, or none of the Software in such volumes as it determines during the Price Hold Period.

Software	Copies Delivered	License Type	# of Licenses (E.g., Users)	List License Price	Discount	Actual License Fee*	Support Percentage†	Operating System(s)	Start Date

*The License Fee [ ] does [ ] does not include the Support Fee for the first Support Period for each Software license identified above.
† The Support percentage is based on [ ] list price [ ] discounted price. Any increase in annual maintenance must be equal to or less that the annual increase in the list price of the Software and is subject to the caps specified in the Contract.

License Descriptions

License Type	Description of License
[Insert License Type]	*[Insert License Description]*
[Insert License Type]	*[Insert License Description]*
[Insert License Type]	*[Insert License Description]*
[Insert License Type]	*[Insert License Description]*

TO SHOW THEIR AGREEMENT, the parties have executed this Contract as of the dates appearing below.

FOR THE CONTRACTOR: **CONTRACTOR NAME**	**FOR STATE OF OHIO** **DEPARTMENT OF ADMINISTRATIVE SERVICES**
By: _____	**By:** _____
Name: _____	**Name:** Director of DAS
Title: _____	**Title:** Director
Date: _____	**Date:** _____

LICENSE SCHEDULE NUMBER [0000000.00]

This license schedule ("Schedule") is between the State of Ohio (the "State"), through the Department of Administrative Services, Investment and Governance Division, with offices at 30 East Broad Street, Columbus, Ohio 43215 for the beneficial use of *[agency]*, and *[Company name of the Contractor]* (the "Contractor"), with offices at *[street address, city, state and zip code for the Contractor]*, and is entered into under that certain Master Contract for Software Licensing between the State and the Contractor that is dated *[Date of the Contract]* and numbered [0000000] (the "Contract").

Granted Licenses

Software	Copies Delivered	License Type	# of Licenses (E.g., Users)	List License Price	Discount	Actual License Fee*	Support Percentage†	Operating System(s)	Start Date

*The License Fee [ ] does [ ] does not include the Support Fee for the first Support Period for each Software license identified above.
† The Support percentage is based on [ ] list price [ ] discounted price. Any increase in annual maintenance must be equal to or less than the annual increase in the list price of the Software and is subject to the caps specified in the Contract.

License Descriptions

License Type	**Description of License**
[Insert License Type]	*[Insert License Description]*
[Insert License Type]	*[Insert License Description]*
[Insert License Type]	*[Insert License Description]*

Location Information

Service Types	**Locations**
Locations where the Contractor will provide Support:	*[Insert Locations]*

Locations where the Contractor will provide services or keep the State's data or from which the data may be accessed:	*[Insert Locations]*
Locations where any subcontractor will provide support or keep the State's data or from which the data may be accessed:	*[Insert Locations]*

TO SHOW THEIR AGREEMENT, the parties have executed this Contract as of the dates appearing below.

FOR THE CONTRACTOR:
CONTRACTOR NAME

By: _____

Name: _____

Title: _____

Date: _____

FOR STATE OF OHIO
DEPARTMENT OF ADMINISTRATIVE SERVICES

By: _____

Name: Director of DAS

Title: Director

Date: _____

ATTACHMENT ELEVEN MASTER CLOUD SERVICES AGREEMENT (MCSA NUMBER [0000000])

<Service Provider>
Master Cloud Services Agreement
MCSA00__

THIS MASTER CLOUD SERVICES AGREEMENT ("Agreement") is by and between _____ ("Service Provider"), having an office at _____, and the State of Ohio ("State"), through its Department of Administrative Services ("DAS"), having its principal place of business at 30 East Broad Street, 40th Floor, Columbus, OH 43215. The State and the Service Provider also are sometimes referred to jointly as the "Parties" or individually as a "Party". The effective date of this Agreement is the date it is signed on behalf of the State ("Effective Date").

1. General Information

1.1. ORGANIZATION

This Agreement covers subscriptions to cloud services through one or more attachments ("Service Attachments") that describe the cloud offerings ("Services") that the Service Provider makes available to its Subscribing Entity by subscription and that it is authorized to sell to the State. The Service Attachments describe the Services the Service Provider offers under this Agreement, along with any special terms or conditions applicable only to those Services, descriptions of those Services, features, and all fees associated with such Services, as well as any other provisions to which the Parties have agreed with respect to the those Services. Such Service Attachments, when executed by the Parties, are incorporated into this Agreement and become a part hereof.

1.2. SUBSCRIBING ENTITIES

A "Subscribing Entity" means State agencies, boards, and commissions that place requests through the State's Ordering System described in another section ("Orders") under this Agreement for any of the Services identified by one or more Service Attachments to this Agreement. And it includes other entities of the State, such as the legislative and judicial branches of State government and the independent offices of elected State officials that place Orders under this Agreement. It also means the Cooperative Purchasing Members, defined in the next section, that place Orders under this Agreement.

1.3. COOPERATIVE PURCHASING MEMBERS

"Cooperative Purchasing Members" are entities that qualify for participation in the State's cooperative purchasing program under Section 125.04 of the Ohio Revised Code ("ORC") and that have completed the steps necessary to participate in that program. They may include Ohio political subdivisions, such as counties, townships, municipal corporations, school districts, conservancy districts, township park districts, park districts created under Chapter 1545 of the ORC, regional transit authorities, regional airport authorities, regional water and sewer districts, and port authorities. They also may include any Ohio county board of elections, private fire companies, private, nonprofit emergency medical service organizations, and chartered nonpublic schools.

1.4. TERM

The current General Assembly cannot commit a future General Assembly to any expenditure. Therefore, this Agreement along with all Service Attachments will automatically expire at the end of the State's current biennium, which is June 30, 2017.

1.5. AGREEMENT – RENEWAL

The State may renew this Agreement in the next biennium by issuing written notice to the Service Provider of the decision to do so. Renewals will be initiated by the State in writing at least 30 days before the expiration of the then current Term. This expiration and renewal procedure will also apply to the end of any subsequent biennium.

1.6. SERVICE ATTACHMENT(S) – RENEWAL

Along with renewal of this Agreement, the State may renew any or all Service Attachments for the next biennium by issuing written notice to the Service Provider of the decision to do so. Renewals will be initiated by the State at least 30 days before the expiration of the then current Term. This expiration and renewal procedure will also apply to any subsequent biennium.

After the first renewal, the Parties agree that pricing of Services under any Service Attachment may be renegotiated to reflect more favorable rates to the State. Upon termination of this Agreement, all rights of the Subscribing Entities to order new Services cease and the Service Provider may not fulfill any such requests for any Subscribing Entity under this Agreement. Further, all existing Service Attachments and all existing Orders under those Service Attachments also will terminate, except to the extent that the Service Provider has any prepaid Services to perform.

The Subscribing Entities have the option anytime during the Agreement's Term to upgrade to a new technology or Service offering with the Service Provider without incurring any charges for terminating the existing technology or Service offering before the agreed upon Term of the Subscribing Entity's Order ("Early Termination Charge"), if any such charge is provided for in the applicable Service Attachment.

1.7. RELATIONSHIP OF THE PARTIES AND SUBSCRIBING ENTITIES

The Parties are independent contractors and nothing herein creates or implies an agency relationship, joint venture, or partnership between the Parties. The Service Provider and its officers, employees, contractors, and subcontractors who may attend meetings and work in other situations where their independent contractor status is not obvious to third parties must identify themselves as such to avoid creating an impression that they are State representatives. In addition, neither the Service Provider nor its officers, employees, contractors, or subcontractors may make any representation that they are acting, speaking, representing, or otherwise advocating any position, agreement, service, or otherwise on behalf of the State or any Subscribing Entity.

1.8. DEALERS AND DISTRIBUTORS

The State authorizes the Service Provider to name one or more dealers to work with the State on behalf of the Service Provider. But if the Service Provider decides to use any dealers, the Service Provider must submit the name, principal business address, addresses for Orders and for payments, telephone number, and its federal tax identification number. The Service Provider also must submit a completed W9 form for each dealer it wishes to name under this section. The Service Provider's submission must be on its official letterhead, signed by an authorized representative, and addressed to the address listed in Section 9.26.

In doing so, the Service Provider warrants that:

i. the Service Provider has provided the dealer with a copy of this Agreement, and a duly authorized representative of the dealer has agreed, in writing, to be bound by the terms and conditions in this Agreement.
ii. such agreement specifically provides that it is for the benefit of the State as well as the Service Provider.
iii. the Service Provider will remain liable under this Agreement for the Services of its dealers and will remedy any breach of any of its dealers under this Agreement.
iv. payments under this Agreement for the Services of any dealer may be made directly to that dealer, and the Service Provider will look solely to the dealer for any payments due to the Service Provider once the State has paid the dealer.
v. to the extent that there is any liability to the State arising from doing business with a dealer that has not signed the Agreement required under this section with the Service Provider, the Service Provider will indemnify the State for such liability.

If the Service Provider wants to designate a dealer that will not receive payments (a "distributor"), the Service Provider may do so by identifying the person or organization as a distributor in the authorizing letter. In such cases, information regarding taxpayer identification and payment addressing may be omitted, as may the distributor's W9 form. All other requirements and obligations for designating a dealer apply to designating a distributor.

The State strongly encourages the participation of small and disadvantaged businesses in its contracting programs and has created certification programs for Minority Business Enterprises (MBEs) and to Encourage Diversity Growth and Equity (EDGE) in State contracting.

1.9. AUDITS AND REPORTS

During the Term of this Agreement and for three years after its termination, on reasonable notice and during customary business hours, the State may audit the Service Provider's records and other materials that relate to the Services performed under this Agreement, to any billing or invoices under the Agreement, or to pricing representations that the Service Provider made to acquire this Agreement. This audit right also will apply to the State's duly authorized representatives and any organization providing funding for any Order hereunder.

The Service Provider must make such records and materials available to the State within 15 days after receiving the State's written notice of its intent to audit the Service Provider's records and must notify the State as soon as the records are ready for audit.

If any audit reveals any material misrepresentation, overcharge to the State, or violation of the Terms of this Agreement, the State will be entitled to recover its damages, including the cost of the audit.

The State also may require various reports from the Service Provider related to the Services. Such reports include those identified in Section 7.6 and those identified in any Service Attachment. Further, the State will be entitled to any other reports that the Service Provider makes generally available to its other customers without additional charge. The State's rights under this section will apply to all Services provided to all Subscribing Entities under this Agreement, but a Subscribing Entity's rights to reports will apply solely to Services it orders or receives under this Agreement.

1.10. SUBSCRIBING ENTITIES' RELIANCE ON AGREEMENT

Subscribing Entities may rely on this Agreement. But whenever a Subscribing Entity is a Cooperative Purchasing Member and relies on this Agreement to issue an Order, the Subscribing Entity will step into the shoes of the State under this Agreement for purposes of its Order, and, as to the Subscribing Entity's Order, this Agreement will be between the Service Provider and that Subscribing Entity. The Service Provider must look exclusively to that Subscribing Entity for performance, including but not limited to payment, and must hold the State harmless with regard to such Orders and the Subscribing Entity's performance. But the State, through DAS, will have the right to terminate this Agreement and seek such remedies on termination as this Agreement provides should the Service Provider fail to honor its obligations under an Order from any Subscribing Entity, whether a Cooperative Purchasing Member or not.

1.11. THIRD-PARTY SUPPLIERS

The Service Provider must incorporate the costs of any third-party supplies and services in the Service Provider's fees identified on the applicable Service Attachment under this Agreement.

The Service Provider's use of other suppliers does not mean that the State will pay for them. The Service Provider will be solely responsible for payment of its suppliers and any claims of those suppliers for any failure of the Service Provider to meet its obligations under this Agreement in the required manner. The Service Provider will hold the State harmless and indemnify the State against any such claims.

The Service Provider assumes responsibility for all Services provided under this Agreement whether it or one of its suppliers provides them in whole or in part. Further, the Service Provider will be the sole point of

contact with regard to contractual matters, including payment of all charges resulting from the Agreement and all Service requests.

1.12. NON-EXCLUSIVITY

This Agreement is non-exclusive and is not a requirements contract. Nothing herein prevents either Party from entering into similar agreements with other entities.

1.13. COMPETITIVE PRICING AND SERVICES

For the purposes of maintaining pricing and Service competitiveness through the Term of the Agreement, the Service Provider agrees to an annual joint review of its pricing and Service offerings. The annual review will include, but need not be limited to, a like-customer review wherein the Service Provider must provide an analysis that includes both retail and wholesale prices of the similar services it provides to other customers similar to the State to ensure the State and the Subscribing Entities are receiving cost-competitive and technologically competitive Services. Written amendments to the Service Attachments to reduce fees and introduce technological Service improvements may be submitted throughout the Term of the Agreement.

1.14. CONFLICT RESOLUTION

If a Party is noncompliant with any term or condition of this Agreement or if a dispute arises under this Agreement, the Party raising the dispute may provide to the other Party written notice referencing this section and specifying the nature of the dispute (the "Dispute Notification"). The Parties then will seek to resolve the dispute in accordance with the procedures in this Section.

All disputes will be submitted first to the State's Contract Category Manager and the Service Provider's Account Manager (or equivalent) for resolution. For 15 days from receipt of the Dispute Notification ("Dispute Date"), the State's Contract Category Manager and Service Provider's Account Manager will meet in person or by telephone as often as is reasonably necessary to discuss and attempt to resolve the dispute in good faith.

If after the 15 days identified above, the State's Contract Category Manager and the Service Provider's Account Manager are unable to resolve the dispute, the Parties will then submit the dispute to the State's IT Contract Administrator and to the Service Provider's Sales Director (or equivalent) for resolution. For the next 15 days, the State's IT Contract Administrator and Service Provider's Sales Director will meet in person or by telephone as often as is reasonably necessary to discuss and attempt to resolve the dispute in good faith.

If following the 15 days in the previous section, the State's IT Contract Administrator and the Service Provider's Sales Director are unable to resolve the dispute, the Parties will then submit the dispute to the State's Chief Information Officer ("CIO") or a designee and to the Service Provider's Vice President of Sales (or equivalent executive) for resolution. For the next 15 days, the State's CIO and Service Provider's Vice President will meet in person or by telephone as often as is reasonably necessary to discuss and attempt to resolve the dispute in good faith. If the State's CIO and Service Provider's Vice President are unable to resolve the dispute within that time, the Parties will nevertheless continue to retain their rights to initiate formal proceedings hereunder.

The specific format for such discussions will be left to the discretion of the representatives of the State and Service Provider responsible for attempting to resolve the dispute, but each Party will involve the business and legal resources reasonably necessary to attempt in good faith to resolve the dispute at the earliest possible time and without undue delay.

If the Parties are unable to resolve the dispute and the dispute involves a claim that the Service Provider is noncompliant with its obligations hereunder or has overcharged for a Service, the State or affected Subscribing Entities may withhold payment for any Services that are the subject of the dispute until the Service Provider cures the noncompliance, the Parties arrive at an agreement to resolve the dispute, or a Party obtains a resolution in a court of competent jurisdiction.

Nothing in this Section is intended to limit the rights provided under Section 6 or be a prerequisite to exercising those rights.

Once the dispute has been resolved, any payments withheld will be handled in the following manner:

> If the resolution was in favor of the State or one or more Subscribing Entities, the Service Provider will issue a credit on the next invoice for the affected Subscribing Entities. If the credit exceeds the Service charges on the next invoice or an invoice will not be issued within 60 days of the resolution, the Service Provider will issue payment in the form of a check in the amount exceeding the Service charges or for the full amount if an invoice will not be issued within 60 days. Any such checks must be issued within that 60-day period.
>
> If in favor of the Service Provider, the affected Subscribing Entities will submit appropriate payment within 30 days of receiving notification of the resolution at the office designated to receive the invoice.

In either of the above cases, the amount or amounts withheld by the State or Subscribing Entity(s) will be taken into account in calculating any amount(s) due.

2. General Requirements for Cloud Services

2.1. STANDARDS

All Service subscriptions must provide a Service that maintains a redundant infrastructure that will ensure access for all of the State's enrolled users in the event of failure at any one of the Service Provider locations, with effective contingency planning (including back-up and disaster recovery capabilities) and 24x7 trouble shooting service for inquiries, outages, issue resolutions, etc. All such Services must be dependable and provide response rates that are as good as or better than industry standards. They also must meet the Service Level Agreements ("SLAs") provided in the applicable Service Attachment and be supported with sufficient connectivity and computing resources to handle reasonably anticipated peak demand, and the Service Provider must ensure that sufficient bandwidth and computing resources are dedicated to the Services to meet peak demand times without material degradation in performance.

The Services must also operate at the moderate level baseline as defined in the National Institute of Standards and Technology ("NIST") 800-53 Rev. 4 moderate baseline requirements, be consistent with Federal Information Security Management Act ("FISMA") requirements, and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications. Additionally, they must provide the State's systems administrators with 24x7 visibility into the services through a real-time, web-based "dashboard" capability that enables them to monitor, in real or near real time, the Services' performance against the established SLAs and promised operational parameters.

The Service Provider has and will continue to use its best efforts through quality assurance procedures to ensure that there are no viruses or malware or undocumented features in its infrastructure and Services and that they do not contain any embedded device or code (e.g., time bomb) that is intended to obstruct or prevent any use of or access to them by the Subscribing Entities. Notwithstanding any rights granted under the Agreement or at law, the Service Provider hereby waives under any and all circumstances any right it may have or may hereafter have to exercise electronic self-help.

User access to the Services must be capable of being integrated with a Subscribing Entity's Active Directory (or other Lightweight Directory Access Protocol (LDAP) service) to support single sign-on capability for users and to ensure that every user is tied to an Active Directory or other LDAP account and to prevent user access when a user is disabled or deleted in the applicable Subscribing Entity's Active Directory or other LDAP service.

The Service Provider must obtain an annual *Statements on Standards for Attestation Engagements* ("SSAE") No. 16, Service Organization Control 1 Type 2, audit. The audit must cover all operations

pertaining to the Services covered by this Agreement. The audit will be at the sole expense of the Service Provider and a copy of it must be provided to the State within 30 days of its completion each year.

At no cost to the State, the Service Provider must immediately remedy any issues, material weaknesses, or other items identified in each audit as they pertain to the Services.

2.2. OBJECT REASSIGNMENT

Any Service subscriptions that are provided by the number of items that may be used by or in conjunction with it, such as nodes, users, or connections ("Objects"), may be reassigned to other, similar Objects within the Subscribing Entity at any time and without any additional fee or charge. For example, a named user subscription may be assigned to another user. But any such reassignment must be in conjunction with termination of use by or with the previous Object, if such termination is required to keep the total number of licensed Objects within the scope of the applicable subscription. Should a Subscribing Entity require a special code, a unique key, or similar item to reassign the subscription as contemplated by this section, the Service Provider will provide such a code, key, or similar item to the Subscribing Entity at any time and without a fee or charge. A later section in this Agreement governs assignment of a Subscribing Entity's subscription to any Service to a successor in interest.

2.3. GENERATED FILES

"Generated Files" are files storing information, instructions, or data that a Subscribing Entity creates or modifies using the Service Provider's Services and in which the data or other information was provided or created by a Subscribing Entity. Such Generated Files are also included in the definition of "Subscribing Entity's Data" in a later section of this Agreement. Examples of such files could include, among others, text files generated with a word processor, data tables created with a database engine, and image files created with a graphics application. Applications consisting of instruction sets created with a programming language that the Service Provider provided to a Subscribing Entity also would be considered Generated Files. As between the Subscribing Entity and the Service Provider, the Subscribing Entity will own all Generated Files that the Subscribing Entity prepares by using the Services, excluding such portions of the Generated Files that consist of embedded portions of the Software. The Service Provider or its licensors will retain ownership of any portions of the Software embedded into Generated Files. But the Service Provider grants to the Subscribing Entity a nonexclusive, royalty-free right to reproduce and distribute to third parties any portions of the intellectual property embedded in any Generated Files that the Subscribing Entity creates while using the Services in the manner in which the Services are designed to be used. In the Subscribing Entity's distribution of the Generated Files, the Subscribing Entity may not use the Service Provider's name, logo, or trademarks, except to the extent that such are incorporated in such Generated Files by the design of a Service when used as intended.

2.4. SERVICE PROVIDER WARRANTIES

THE SERVICE PROVIDER WARRANTS THAT:

i. **IT HAS VALIDLY ENTERED INTO THIS AGREEMENT AND HAS THE LEGAL POWER TO DO SO,**
ii. **THE SERVICES WILL PERFORM MATERIALLY IN ACCORDANCE WITH THE APPLICABLE USER GUIDE AND THE REQUIREMENTS OF THIS AGREEMENT,**
iii. **SUBJECT TO ANY LIMITATIONS SPECIFIED IN THE APPLICABLE SERVICE ATTACHMENT, THE FUNCTIONALITY OF THE SERVICES WILL NOT BE MATERIALLY DECREASED DURING A SUBSCRIPTION TERM, AND**
iv. **IT WILL NOT TRANSMIT VIRUSES, WORMS, TIME BOMBS, TROJAN HORSES AND OTHER HARMFUL OR MALICIOUS CODE, FILES, SCRIPTS, AGENTS OR PROGRAMS ("MALICIOUS CODE") TO A SUBSCRIBING ENTITY, PROVIDED IT IS NOT A BREACH OF THIS SUBPART ,**

FOR ANY BREACH OF A WARRANTY ABOVE, THE STATE'S AND INDIVIDUAL SUBSCRIBING ENTITIES' REMEDIES WILL BE AS PROVIDED IN THE SECTION OF THIS AGREEMENT DEALING WITH TERMINATION.

Failure of the Service Provider to meet any SLAs in an applicable Service Attachment will not be considered a breach of this warranty section unless the State reasonably determines that the failure is persistent or extended in duration.

Note: Any terms and conditions that may be incorporated in a User Guide that conflicts with the MCSA or SA, the MCSA and SA will prevail.

2.5. STATE AND SUBSCRIBING ENTITIES RESPONSIBILITIES

The State and each Subscribing Entity will be responsible for their respective compliance with this Agreement. Additionally, each Subscribing Entity will:

i. be responsible for the accuracy, quality, and legality of its data and of the means by which the data was acquired,
ii. use commercially reasonable efforts to prevent unauthorized access to or use of the Services to which it subscribes and notify the Service Provider promptly of any unauthorized access or use of which it becomes aware, and
iii. use the Services only in accordance with the applicable user guide, to the extent it is not inconsistent with this Agreement, applicable laws, and government regulations.
iv. because of the sensitive nature of performing security and compliance checks on Assets, The State represents and warrants that The State has full right, power, and authority to consent to have the Service test for vulnerabilities, compliance checking, or, as applicable, malware ("scan") the Assets identified to Service Provider for scanning, whether electronically or by any other means, whether at the time of initial Registration or thereafter, and
v. The State may access the Service's user interface to reproduce solely for The State's own internal business purposes only such vulnerability, configuration checks and/or malware test results as set forth in the Reports.

A Subscribing Entity may not:

i. intentionally make the Services available to anyone other than its employees and contractors acting on the State's behalf,
ii. sell, resell, rent or lease the Services,
iii. use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights,
iv. intentionally use the Services to store or transmit Malicious Code,
v. intentionally interfere with or disrupt the integrity or performance of the Services or third-party data contained therein, or
vi. attempt to gain unauthorized access to the Services or their related systems or networks.

3. Insurance, Indemnification, Limitation of Liability

3.1. INSURANCE

The Service Provider must provide the following insurance coverage at its own expense throughout the Term of this Agreement to the State:

i. Workers' compensation insurance, as required by Ohio law, and if some work will be done outside Ohio, the laws of the appropriate states where work will be done. The Service Provider also must maintain employer's liability insurance with at least a $1,000,000.00 limit.

ii. Commercial General Liability insurance coverage for bodily injury, personal injury, wrongful death, and property damage. The defense cost must be outside of the policy limits. Such policy must designate the State of Ohio as an additional insured, as its interest may appear. The policy also must be endorsed to include a waiver of subrogation. At a minimum, the limits of the insurance must be:

$ 2,000,000 General Aggregate
$ 2,000,000 Products/Completed Operations Aggregate
$ 1,000,000 per Occurrence Limit
$ 1,000,000 Personal and Advertising Injury Limit
$ 100,000 Fire Legal Liability
$ 10,000 Medical Payments

The Contractor shall, for each policy required by this Contract, provide the State with 30-days prior written notice of cancellation, material change, or non-renewal, except a 10-days notice of non-payment of premium. And the Contractor's Commercial General Liability must be primary over any other insurance coverage.

iii. Commercial Automobile Liability insurance with a combined single limit of $500,000. The policy must be endorsed to include a waiver of subrogation.

iv. Professional Liability insurance covering all staff with a minimum limit of $1,000,000 per incident and $3,000,000 aggregate. If the Service Provider's policy is written on a "claims made" basis, the Service Provider must provide the State with proof of continuous coverage at the time the policy is renewed. If for any reason the policy expires, or coverage is terminated, the Service Provider must purchase and maintain "tail" coverage through the applicable statute of limitations.

v. If a Cloud solution is used the following Liability insurance requirements apply.

In the event Contractor, as part of the provision of Services, will control or develop information technology hardware and/or software, or otherwise control the Company's data, then Contractor shall provide Cyber Liability and/or Intellectual Property Infringement Liability insurance of not less than $5,000,000 per occurrence and $10,000,000 in the aggregate for liabilities for financial loss resulting or arising from acts, errors, or omissions, in connection with the Services provided under this agreement such as:

- Breaches of security or privacy,
- Data theft, damage, destruction, or corruption, including without limitation, unauthorized access, unauthorized use, identity theft, theft of personally identifiable information or confidential corporate information, transmission of a computer virus or other type of malicious code,
- Participation in a denial of service attack on a third party,
- Violation or infringement of any right of privacy, breach of federal, state, or foreign security and/or privacy laws or regulations,
- Intellectual property infringement arising out of software and/or content (excluding patent infringement and misappropriation of trade secrets),
- Technology errors and omissions,
- Business interruption,
- Cyber extortion, and
- Investigation, notification and related credit monitoring costs from any of the above.

All certificates must be in a form that is reasonably satisfactory to the State as to the contents of the policies and the quality of the insurance carriers and must identify this Agreement. All carriers must have at least an "A-" rating by A.M. Best.

Any Subscribing Entity that is a Cooperative Purchasing Member that Orders Services also may require a certificate of insurance from the Subscribing Entity naming it as an additional insured.

Whenever a Subscribing Entity locates its equipment at facilities owned or controlled by the Service Provider or one of its contractors, the Service Provider must maintain:

i. property insurance insuring the equipment against loss or damage by fire and all other risks covered by the standard extended coverage endorsement used by the Service Provider for its own property or that in common use in the industry, and any other risks reasonably required and covered by the Service Provider's insurance. The coverage must be in an amount at least equal to the reasonable replacement value of the equipment, and

ii. workers' compensation coverage as required by the laws of the State in which the equipment is located. The Service Provider must furnish evidence of the coverage throughout each Order's Term.

All such insurance must be with insurers that are authorized to issue such insurance in the state. All such property insurance shall name the applicable Subscribing Entity as the loss payee. All such insurance also must contain a provision to the effect that it cannot be canceled or modified without first giving written notice thereof to the Service Provider and the applicable Subscribing Entities without at least 30 days written notice. Such changes may not become effective without the applicable Subscribing Entities' prior written consent.

3.2. INDEMNIFICATION FOR BODILY INJURY AND PROPERTY DAMAGE

The Service Provider must indemnify the State and the Subscribing Entities against all liability or expense resulting from bodily injury to any person (including death) or damage to property arising out of its performance under this Agreement, provided such bodily injury or property damage is due to the negligence or other tortious conduct of the Service Provider, its employees, agents, or subcontractors.

3.3. INDEMNIFICATION FOR INFRINGEMENT

The Service Provider will release, protect, indemnify, defend, and hold the State and the Subscribing Entities harmless from and against any claims of infringement by any third parties based on any Service provided under this Agreement. Any defense of the State or a State Subscribing Entity requires and is subject to the approval and consent of the Ohio Attorney General. Any such defense will be at the Service Provider's sole cost and expense. Further, the Service Provider will indemnify the State and Subscribing Entities for any liability resulting from any such claims, demands, or suits, as well as hold the State and the Subscribing Entities harmless for the Service Provider's liability, losses, and damages resulting from such. This obligation of defense and indemnification will not apply where the State or a Subscribing Entity has modified or misused the Service and the claim or the suit is based on the modification or misuse. The State or affected Subscribing Entity or Entities agrees to give the Service Provider notice of any such claim as soon as reasonably practicable and to allow the Service Provider to control the defense of any such claim, upon consultation with and the approval of the Office of the State's Attorney General.

If a successful claim of infringement is made, or if the Service Provider reasonably believes that an infringement or similar claim that is pending actually may succeed, the Service Provider will do one of the following four things as soon as reasonably possible to avoid or minimize any interruption of the Subscribing Entities business:

i. Modify the offending Service so that it is no longer infringing but provides substantially the same functionality as before the modification;
ii. Replace the offending Service with an equivalent or better offering;
iii. Acquire the right for the Subscribing Entities to use the infringing Service as it was intended for the Subscribing Entities to use under this Agreement; or
iv. Terminate the infringing Service and refund the amount the Subscribing Entities paid for the Service and the amount of any other Service that requires the availability of the infringing Service for it to be useful to the Subscribing Entities.

3.4. LIMITATION OF LIABILITY - STATE

The State's and Subscribing Entities' combined total liability for damages, whether in contract or in tort, will not exceed two times the amount of compensation payable to Service Provider for the previous 12 months of Service related to the Service Attachment under which the damages occurred or the amount of direct damages incurred by the Service Provider, whichever is less.

3.5. LIMITATION OF LIABILITY - SERVICE PROVIDER

The Service Provider will be responsible for any liability, claims, losses and damages arising out of the performance of this Agreement provided such liability, claim, loss or damage is due to the fault or negligence of the Service Provider, its employees, agent, subcontractors or affiliates.

NOTWITHSTANDING THE PREVIOUS SENTENCE AND EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, NEITHER PARTY, ITS AFFILIATES OR CONTRACTORS WILL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, EXEMPLARY, OR CONSEQUENTIAL DAMAGES,

INCLUDING LOST PROFITS, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES.

4. Confidentiality and Handling of Data

4.1. CONFIDENTIALITY

The State may disclose to the Service Provider written material or oral or other information that the State treats as confidential ("Confidential Information"). Title to the Confidential Information and all related materials and documentation the State delivers to the Service Provider will remain with the State. The Service Provider must treat such Confidential Information as secret if it is so marked, otherwise identified as such, or when, by its very nature, it deals with matters that, if generally known, would be damaging to the best interests of the public, other contractors or potential contractors with the State, or individuals or organizations about whom the State keeps information. The Service Provider may not disclose any Confidential Information to third parties and must use it solely to perform under this Agreement.

If any Service delivered under this Agreement contains data, documentation, or other written information that is confidential in nature and properly labeled as such, then it also will be Confidential Information for purposes of this section. The State will keep all such Confidential Information in confidence and will not use it other than as authorized under this Agreement. Nor will the State disclose any such Confidential Information to any third party without first obligating the third party to maintain the secrecy of the Confidential Information.

If one party discloses Confidential Information ("Disclosing Party") to the other party to this Agreement ("Receiving Party"), the Receiving Party's obligation to maintain the confidentiality of the Confidential Information will not apply where such:

i. was already in the possession of the Receiving Party without an obligation of confidence;
ii. is independently developed by the Receiving Party, provided documentary evidence exists to support the independent development;
iii. except as provided in the next paragraph, is or becomes publicly available without a breach of this Agreement;
iv. is rightfully received by the Receiving Party from a third party without an obligation of confidence;
v. is disclosed by the Receiving Party with the written consent of the Disclosing Party; or
vi. is released under a valid order of a court or governmental agency, provided that the Receiving Party:

    a. Notifies the Disclosing Party of the order immediately upon receipt of it, unless it is legally prohibited from doing so; and
    b. Makes a reasonable effort to obtain a protective order from the issuing court or agency limiting the disclosure and use of the Confidential Information solely for the purposes intended to be served by the original order of production.

Information that may be available publicly through other sources about people that is personal in nature, such as medical records, addresses, phone numbers, social security numbers, and similar things, is nevertheless sensitive in nature and may not be disclosed or used in any manner except as expressly authorized in this Agreement. Therefore, item (iii) in the preceding paragraph does not apply, and the Service Provider must treat such information as Confidential Information whether it is available elsewhere or not.

The Receiving Party must return all originals of any Confidential Information and destroy any copies it has made on termination or expiration of this Agreement.

The disclosure of the Confidential Information of the Disclosing Party in a manner inconsistent with the Terms of this provision may cause the Disclosing Party irreparable damage for which remedies other than injunctive relief may be inadequate, and each Receiving Party agrees that in the event of a breach of the Receiving Party's obligations hereunder, the Disclosing Party will be entitled to seek temporary and permanent injunctive relief to enforce the provisions of this Agreement without the necessity of proving actual damages. However, this provision does not diminish or alter any right to claim and recover damages.

This Agreement is not Confidential Information. All its terms and conditions, including pricing and any attachments, represent public information.

4.2. PUBLIC RECORDS REQUESTS.

Should the Service Provider receive any public records request with respect to any Subscribing Entity's Data, the Service Provider will immediately notify the affected Subscribing Entity or Entities and fully cooperate with the affected Subscribing Entity or Entities as it or they direct.

4.3. HANDLING OF SUBSCRIBING ENTITY'S DATA

"Subscribing Entity's Data" is any information, data, files, or software that a Subscribing Entity uses or stores on or in conjunction with the Services, including but not limited to Generated Files. The Service Provider must use due diligence to ensure computer and telecommunications systems and Services involved in storing, using, or transmitting Subscribing Entity's Data are secure and to protect that data from unauthorized disclosure, modification, or destruction. To accomplish this, the Service Provider must comply with all applicable National Institute of Standards and Technology ("NIST") standards for Moderate Impact systems and:

i. apply appropriate risk management techniques to ensure security for all sensitive data, including but not limited to any data identified as Confidential Information elsewhere in this Agreement.
ii. ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability.
iii. 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.
iv. maintain appropriate identification and authentication process for information systems and services associated with Subscribing Entity's Data.
v. maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with Subscribing Entity's Data.
vi. implement and manage security audit logging on information systems, including computers and network devices.

The Service Provider 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 Subscribing Entity's Data, limiting access to only these points, and disabling all others. To do this, the Service Provider 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. The Service Provider must use two-factor authentication to limit access to systems that contain Subscribing Entity's Data.

Unless a Subscribing Entity instructs the Service Provider otherwise in writing, the Service Provider must assume all Subscribing Entity's Data is both confidential and critical for Subscribing Entity operations, and the Service Provider'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. As part of the Service Provider's protection and control of access to and use of data, the Service Provider must employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access Subscribing Entity's Data, as well as attacks on the Service Provider's infrastructure associated with Subscribing Entity's Data. Further, the Service Provider 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 Subscribing Entity's Data.

The Service Provider must use appropriate measures to ensure that Subscribing Entity's Data is secure before transferring control of any systems or media on which Subscribing Entity's Data is stored. The method of securing the data must be appropriate to the situation and may include erasure, destruction, or encryption of the data before transfer of control. The transfer of any such system or media must be reasonably necessary for the performance of the Service Provider's obligations under this Agreement.

The Service Provider must have a business continuity plan in place. The Service Provider must test and update the IT disaster recovery portion of its business continuity plan 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 Service Provider maintains Subscribing Entity'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 Subscribing Entity's Data in the case of a disaster or other business interruption. The Service Provider'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 Subscribing Entity's Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Service Provider also must provide for reviewing, testing, and adjusting the plan on an annual basis.

The Service Provider may not allow Subscribing Entity's Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Agreement properly. Even then, the Service Provider may permit such only if adequate security measures are in place to ensure the integrity and security of the 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. At a minimum, portable computing devices must have anti-virus software, personal firewalls, and system password protection. In addition, Subscribing Entity'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. The Service Provider also must maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

Any encryption requirement identified in this provision must meet the NIST standards identified above.

The Service Provider must have reporting requirements for lost or stolen portable computing devices authorized for use with Subscribing Entity's Data and must report any loss or theft of such to the State in writing as quickly as reasonably possible. The Service Provider also must maintain an incident response capability for all security breaches involving Subscribing Entity's Data whether involving mobile devices or media or not. The Service Provider must detail this capability in a written policy that defines procedures for how the Service Provider will detect, evaluate, and respond to adverse events that may indicate a breach or attempt to attack or access Subscribing Entity's Data or the infrastructure associated with Subscribing Entity's Data.

In case of an actual security breach that may have compromised Subscribing Entity's Data, including but not limited to loss or theft of devices or media, the Service Provider must notify the Subscribing Entity in writing of the breach within 24 hours of the Service Provider becoming aware of the breach, and fully cooperate with the Subscribing Entity to mitigate the consequences of such a breach. This includes any use or disclosure of the Subscribing Entity's Data that is inconsistent with the Terms of this Agreement and of which the Service Provider becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this Agreement by an employee, agent, or subcontractor of the Service Provider.

The Service Provider must give affected Subscribing Entities full access to the details of the breach and assist each Subscribing Entity in making any notifications to potentially affected people and organizations that the affected Subscribing Entities deem are necessary or appropriate. The Service Provider must document all such incidents, including its response to them, and make that documentation available to the affected Subscribing Entities on request. In addition to any other liability under this Agreement related to the Service Provider's improper disclosure of Subscribing Entity's Data, and regardless of any limitation on liability of any kind in this Agreement, the Service Provider 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 Service Provider's possession. Such identity theft protection must be reasonably acceptable to the State.

All Subscribing Entity's Data will remain the property of the Subscribing Entity. The Service Provider must ensure that the Subscribing Entity retains access and download capability for purposes of retrieving its data for research, investigation, transfer, or migration to other systems.

All Subscribing Entity's Data at rest in systems supporting the Service Provider's Services must reside within the contiguous United States with a minimum of two data center facilities at two different and distant geographic locations and be handled in accordance with the requirements of this section at all Service Provider locations.

4.4. SUBSCRIBING ENTITY RESPONSIBILITIES

Each Subscribing Entity will be responsible for its compliance with this Agreement, be responsible for the accuracy, quality, and legality of its Subscribing Entity's Data and of the means by which it acquired that Subscribing Entity's Data, use commercially reasonable efforts to prevent unauthorized access to or use of the Services, and notify the Service Provider promptly of any unauthorized access or use of which it becomes aware. Further, the Subscribing Entity will use the Services only in accordance with the applicable user guide(s), to the extent not inconsistent with the Subscribing Entity's rights under this Agreement and any applicable Service Attachments, and applicable laws and government regulations.

Further, a Subscribing Entity may not intentionally make the Services available to anyone other than its employees and its contract personnel, unless the applicable Service or Services are designed to be publically facing or intended for interaction with clients of the Subscribing Entity (e.g., hosted web sites), sell, resell, rent, or lease the Services, use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights. The Subscribing Entities also may not intentionally use the Services to store or transmit Malicious Code, intentionally interfere with or disrupt the integrity or performance of the Services or third-party data contained therein, or attempt to gain unauthorized access to the Services or their related systems or networks.

5. Orders, Requesting Service, Delivery, Acceptance, Termination, and Modification

5.1. ACCEPTANCE

The acceptance procedure for setup or installation of the Services will be a review by the Subscribing Entity acquiring the Service to ensure that it meets the performance standards and other requirements in the applicable Service Attachment and that the setup or installation has been done in a professional manner and that the Service itself meets all requirements. For other Services, the acceptance procedure will be a review by the Subscribing Entity to ensure the Service complies with the performance requirements in the applicable Service Attachment. In addition to the requirements of the applicable Service Attachment, if ordering documents such as a Statement of Work (SOW) are authorized in that Service Attachment, the review will include any additional requirements in that Order. The Subscribing Entity will have up to 15 days after the setup, installation, or establishment of the Service to do this. The Subscribing Entity will not issue a formal letter of acceptance, unless otherwise specified in the applicable Service Attachment, and passage of 15 days will imply acceptance, though the Subscribing Entity will issue a notice of noncompliance if set up or installation or other Service does not meet the requirements in this Agreement.

If the Subscribing Entity issues a noncompliance letter, the Service Provider will have 30 days to correct the problems listed in the letter. If the Subscribing Entity has issued a noncompliance letter, the Service, installation, or set up will not be accepted until that Subscribing Entity issues a letter of acceptance indicating that each problem noted in the noncompliance letter has been cured. If the problems have been fixed during the 30-day period, the Subscribing Entity will issue the acceptance letter within 15 days after all defects have been fixed. If the Service Provider fails to correct the defect(s), the applicable Order(s) will terminate without cost or obligation to the Subscribing Entity.

The applicable Service Attachment may provide additional or alternative acceptance procedures, but no Order may change the acceptance process.

5.2. SERVICE, TERMINATION, OR MODIFICATION

All Orders for Service, as well as any termination of an Order or modification to an Order, including termination, must be made through the State's Ordering System.

Therefore, the Service Provider must notify the State when an Order is received that was placed outside the State's Ordering System and the Service Provider will not accept the Order. If a Service Provider accepts an Order outside the State's Ordering System the State or the Subscribing Entity may either withhold payment for the unverified Order or require termination of the Service under the unverified Order without cost or obligation to the State or the Subscribing Entity.

The Service Provider agrees to keep Subscribing Entities' Orders updated and current in the State's Ordering System.

The Service Provider is responsible for processing all Orders, billing, payments, cancellations, changes, and receiving and managing all Service calls in a consolidated manner. In this regard, the Service Provider must act as the sole point of contact for all Services under this Agreement and any related Service Attachments for all Subscribing Entities. The Service Provider may not require a Subscribing Entity to contact any of the Service Provider's third-party suppliers or otherwise transact business directly with such suppliers for any Services ordered under this Agreement, and in all respects, the Service Provider must maintain a seamless, single-point-of-contact business relationship with each Subscribing Entity for the Services ordered under this Agreement.

6. Termination – Agreement, Service Attachments, Orders

6.1. TERMINATION BY THE STATE

The Service Provider must comply with all terms and conditions of this Agreement. If the Service Provider fails to perform any one of its obligations under this Agreement, it will be in default, and the State may proceed in any or all of the following ways:

I. the State may terminate this Agreement, the applicable Service Attachment(s), or the affected Order(s) under this Agreement;
II. the State may withhold payment for any affected Service until the Service Provider cures the noncompliance or the Parties arrive at an agreement as to the corrective action for the noncompliance; or
III. the State may file a complaint for damages with a court of competent jurisdiction in Ohio.

The State also may terminate this Agreement or any Service Attachments for its convenience with 30 days written notice to the Service Provider. In any such event, each Subscribing Entity must pay for all accrued and unpaid charges for Services and any fee specified in the affected Service Attachment(s) for early termination ("Early Termination Charge"), if applicable.

If the termination of the Agreement or any Service Attachment(s) is for cause, then neither the State nor any Subscribing Entities will be liable for any Early Termination Charge outlined in any affected Service Attachments. And the Service Provider will fully cooperate in any disentanglement efforts any Subscribing Entity reasonably requests at no cost to the requesting Subscribing Entity or Entities.

The State's funds are contingent upon the availability of lawful appropriations by the Ohio General Assembly. If the General Assembly fails at any time to continue funding for the payments and other obligations due as part of this Agreement, the State's obligations under this Agreement will terminate as of the date the funding expires without further obligation of the State, including but not limited to any Early Termination Charge outlined in any affected Service Attachments.

6.2. TERMINATION OF ORDERS BY SUBSCRIBING ENTITY OR SERVICE PROVIDER

Under this Agreement, specific Orders also may be terminated by either a Subscribing Entity or the Service Provider, as follows:

6.2.1. BY A SUBSCRIBING ENTITY

A Subscribing Entity may terminate Service under any Order it has placed, and it may do so at any time for any or no reason. The Subscribing Entity will be liable for charges accrued but unpaid as of the termination date, as well as any Early Termination Charge outlined in the appropriate Service Attachments.

If the Subscribing Entity's funds are contingent upon the availability of lawful appropriations by the Ohio General Assembly or other governmental body, and the General Assembly or other governmental body fails at any time to continue funding for the payments and other obligations due under an Order, the Subscribing Entity's obligations with respect to that Order will terminate as of the date the funding expires, and the Subscribing Entity will have no further obligation with respect to such Order, including but not limited to any Early Termination Charge outlined in any affected Service Attachments.

If a termination of any Service under one or more Orders is for cause or non-appropriation of funds, as described in this Section 6, the Subscribing Entity will not be liable for any Early Termination Charge, if such are otherwise applicable to the Service or Services so terminated. If the termination is for cause, the Service Provider will fully cooperate in any disentanglement efforts the Subscribing Entity reasonably requests at no cost to the Subscribing Entity.

6.2.2. BY THE SERVICE PROVIDER

If a Subscribing Entity materially defaults in the performance of any of its duties or obligations under this Agreement, the Service Provider, by giving at least 30 days prior written notice, may cancel any affected Services provided to that Subscribing Entity under this Agreement.

If the Subscribing Entity cures the default to the satisfaction of the Service Provider and before the cancellation of Service date, the Order will remain in full force and effect.

If the Subscribing Entity fails to cure, then the Subscribing Entity will remain liable for charges accrued but unpaid as of the cancellation date and any Early Termination Charge as outlined in the appropriate Service Attachment(s), if applicable.

7. Financial – Fees, Claims and Disputes, Billing, and Payment

7.1. FEES

All applicable charges are fully documented in the appropriate Service Attachment(s). The Subscribing Entity will not be responsible for any charges not documented in the applicable Service Attachment(s) nor will the Subscribing Entity be responsible for any charges waived by the Service Provider in this Agreement or the applicable Service Attachment(s).

Subscribing Entities are not subject to increases in fees during the Term of this Agreement.

Subscribing Entities are not responsible for any charges from the Service Provider's third-party suppliers for any Services ordered under this Agreement, unless an applicable Service Attachment expressly provides otherwise. In this regard, the Service Provider is the seller or reseller of all Services covered by this Agreement, and any payments due to the Service Provider's third-party suppliers for Services under this Agreement are included in the Service Provider's fees specified in the applicable Service Attachment, unless that Service Attachment expressly provides otherwise.

7.2. BILLING

Invoices will be issued at the Order level, but the Subscribing Entity may require a recap at the agency, division, or district level based on the organizational structure of the Subscribing Entity.

Invoices must be submitted to the office designated in the State's Ordering System as the "bill to address". The invoice must be submitted within 60 days of the Service. If the Subscribing Entity does not receive the invoice within the 60 days of the date of Service, the Subscribing Entity will be entitled to deny payment of the invoice.

A proper invoice must include the following information and/or attached documentation:

i. name and address of the Service Provider as designated in this Agreement;
ii. Federal Tax Identification Number of the Service Provider as designated in this Agreement;
iii. invoice remittance address as designated in the Agreement; and
iv. a sufficient description of the Services to allow the Subscribing Entity to identify the Services and perform an audit of the Services.

7.3. PAYMENT

Payments for Services under this Agreement will be due on the 30th calendar day after the actual receipt of a proper invoice in the office designated to receive the invoice.

The Service Provider agrees to receive payment from approved vouchers by electronic fund transfer ("EFT") for Subscribing Entities that rely on them to make payment. The Service Provider will cooperate with Subscribing Entities in providing the necessary information to implement EFT. The date the EFT is issued in payment will be considered the date payment is made, or if a Subscribing Entity does not use an EFT process, the date its check or warrant is issued in payment will be considered the date payment is made.

7.4. STATE REPORTING REQUIREMENTS

The Service Provider must provide the State with a recap of all Services provided to the Subscribing Entities on a monthly basis. Additional, specific reporting data requirements may be outlined in the Service Attachment(s).

7.5. SERVICE LEVEL GUARANTEE AND CREDITS

The Service Provider will issue a credit allowance to any Subscribing Entity affected by a Service outage, as defined in the Service Level Agreement contained in the applicable Service Attachment. The credit will appear on the affected Subscribing Entity's next invoice, or if the Subscribing Entity so requests, the Service Provider will issue a check to the Subscribing Entity as payment within 30 days of the request.

7.6. COST RECOVERY

The Service Provider must pay a Cost Recovery Fee to the State to cover the estimated costs the State will incur administering this Agreement and the Services offered under it.

The Cost Recovery Fee will be 2% of the total quarterly sales reported under this Agreement to all Subscribing Entities, including all State-level entities and all Cooperative Purchasing Members. The Cost Recovery Fee is included in the prices reflected on the Service Attachment and the Service Provider may not add a surcharge to orders under this contract to cover the amount of the Cost Recovery Fee. The State will generate notification to the Service Provider via email on the last day of the calendar quarter advising the Service Provider to complete a revenue reporting form provided by the State within 30 days after the close of the quarter. The State may compare the form provided by the Service Provider to information in the State's accounting system, the State's Ordering System, and other records for purposes of verifying the accuracy of the form.

- Examples of calculation of a Cost Recovery Fee:
  (Log-In and Password Established for Cost Recovery Contact to Report Sales)

1) (State Entities Only Example)

FY14				
Quarter	Revenue State Agencies	Revenue Local Governments	Revenue Share Due	Reported by
Q1	$ 79,193	$ 0	$ 1,584	"Name of Contact"
Q2	$ 10,392	$ 0	$ 208	"Name of Contact"

Q3	$ 209,105	$ 0	$ 4,182	"Name of Contact"
Q4	$ 74,970	$ 0	$ 1,499	"Name of Contact"

2) (State Entities and Cooperative Purchasing Member Sales Example)

FY14				
Quarter	Revenue State Agencies	Revenue Local Governments	Revenue Share Due	Reported by
Q1	$ 79,193	$ 20,963	$ 2,003	"Name of Contact"
Q2	$ 10,392	$ 4,197	$ 292	"Name of Contact"
Q3	$ 209,105	$ 63,210	$ 5,446	"Name of Contact"
Q4	$ 74,970	$ 1,471	$ 1,529	"Name of Contact"

3) (Reporting $0 Sales to both State Entities and Cooperative Purchasing Members)
Note: Reporting still required although sales reported for quarter - $0

FY14				
Quarter	Revenue State Agencies	Revenue Local Governments	Revenue Share Due	Reported by
Q1	$ 0	$ 0	$ 0	"Name of Contact"
Q2	$ 0	$ 0	$ 0	"Name of Contact"
Q3	$ 0	$ 0	$ 0	"Name of Contact"
Q4	$ 0	$ 0	$ 0	"Name of Contact"

The Service Provider must remit to the State the 2% Cost Recovery Fee within 30 days of receipt of the notice from the State by check to the State of Ohio, Office of Information Technology. The check must be made payable to the Treasurer, State of Ohio, and must be sent to the State at the following address:

Department of Administrative Services
L-3686
Columbus, OH 43260-3686

The State will direct the Service Provider to the State's in-house reporting system to enter all reporting information to include all State entity sales as well as Cooperating Purchasing sales. To ensure that the payment is credited properly, the Service Provider must identify the check as a State of Ohio Cost Recovery Fee and reference this Master Cloud Service Agreement and the supporting Cost Recovery Report. Credit of the Cost Recovery Fee will begin in the month of execution of this Agreement.

If the full payment of the Cost Recovery fee is not paid within 30 days after the end of the applicable reporting period, the non-payment will constitute a contract debt to the State. The State may offset any unpaid cost recovery from any amount owed to the Contractor under this Contract and employ all other remedies available to it under Ohio law for the non-payment of Cost Recovery. Additionally if the Contractor fails to pay the Cost Recovery in a timely manner, the failure will be considered a breach of this Contract, and the State may terminate this Contract for cause and seek damages to the full extent of applicable Ohio law.

8. Support

8.1. Service Support Generally

During the Term of any Order, the Service Provider will provide the Subscribing Entity with telephonic assistance and advice for using all Services covered by the Order. The Service Provider also will provide troubleshooting and problem resolution by developing and providing fixes or patches for errors in any software it provides and contract with any third party providing software that supports the Services for the same. As part of the support the Service Provider provides in exchange for the applicable fee, the Service Provider also will keep all software current by installing all relevant service packs and patches as well as

all updates and new releases and versions of the software as soon as reasonably possible. The Service Provider also will keep its own software offering compatible with any updated third-party software that is part of the Services or supports the Services. The manner in which the Service Provider provides support will be governed by the Service Provider's policies and programs described in the applicable documentation or other materials that the Service Provider uses to notify its customers generally of such policies. But regardless of the Service Provider's policies and programs, unless otherwise agreed in the applicable Service Attachment, in all cases such support must comply with the requirements of this Agreement and the applicable Service Attachment(s). And the Service Provider must provide the support in a competent, professional, and timely manner.

8.2. EQUIPMENT SUPPORT GENERALLY

For any equipment used to provide the Services, remedial equipment maintenance by the Service Provider will be completed within eight business hours after notification by the Subscribing Entity that maintenance is required. In the case of preventative maintenance, the Service Provider will perform such in accordance with the manufacturer's published schedule and specifications. If maintenance is not completed within eight hours after notification by the Subscribing Entity, the Service Provider will be in default. Failure of the Service Provider to meet or maintain these requirements will provide the Subscribing Entity with the same rights and remedies as specified elsewhere in this Agreement for default, except that the Service Provider will only have eight hours to remedy a default. Nothing contained herein will limit the application of any credits for failure to meet any service level agreements in the applicable Service Attachment. The Service Provider will provide adequate staff to provide the maintenance required by this Agreement.

8.3. ADJUSTMENTS

A Subscribing Entity may acquire subscriptions that are based on the number of users, nodes, computers, processors, or other counts of Objects covered by an Order ("Objects"). In any such cases, the Subscribing Entity may request that the fees for a subscription renewal be calculated based on fewer Objects than included in the previous Order, with an appropriate adjustment in the applicable fee(s). Despite the reduction, fees for the remaining Objects may not be increased over the applicable fees from the previous Order.

During an Order's duration ("Order Term"), a Subscribing Entity may increase the volume of its Order (e.g., add additional users) without increasing the Order Term. The cost of any addition Objects or similar increase in usage must be prorated to reflect the time remaining in the Order Term rather than be based on the full Order Term.

8.4. SUPPORT PARAMETERS

A Subscribing Entity may initiate support requests for problems it encounters with the Software by telephone, email, Internet, or fax, and the Service Provider must maintain lines of communication that support all four forms of communication. The Service Provider must make support available 24 hours a day, seven days per week (the "Support Window"), and it must do so by staffing its support function with an adequate number of qualified personnel to handle its traditional volume of calls. Further, the Service Provider must maintain at least one support center in North America with adequate English-speaking support personnel. The applicable Service Attachment(s) may provide for different support periods. A Subscribing Entity's technical staff may contact any support center that the Service Provider maintains, and they may choose to do so based on convenience, proximity, service hours, languages spoken, or otherwise.

8.5. INCIDENT CLASSIFICATION

The Service Provider must classify and respond to support calls by the underlying problem's effect on a Subscribing Entity. In this regard, the Service Provider may classify the underlying problem as critical, urgent, or routine. The guidelines for determining the severity of a problem and the appropriate classification of and response to it are described below.

The Service Provider must designate a problem as "critical" if the Service is functionally inoperable, the problem prevents the Service or a major component or function of it from being used in production mode or there is significant potential for data integrity problems. This classification assumes there is no existing

patch for the problem. The Service Provider must classify a problem as "urgent" if the underlying problem significantly degrades the performance of the Service or a major function or component of it or materially restricts a Subscribing Entity's use of the Service in a production mode. A problem also will be considered urgent if a commonly used feature often generates application errors, causes the Service to freeze, locks up the computer on which the Service is running, or otherwise routinely does not work as intended. Classification of a problem as urgent rather than critical assumes that an affected Subscribing Entity still can conduct business with the Service and response times are consistent with the needs of the Subscribing Entity for that type of Service. As with the critical classification, the urgent classification assumes there is no existing patch or acceptable workaround procedure for the problem. Finally, the Service Provider may classify a support call as "routine" if the underlying problem is a question on end use or configuration of the Service. It also may be classified as routine when the problem does not materially restrict a Subscribing Entity's use of the Service in its production environment, such as when a feature or combination of features generates minor or rare errors. Also, if any problem that otherwise should be classified as critical or urgent can be solved either by a known workaround or an existing patch that does not materially interfere with a Subscribing Entity's use of the Service, the problem may be treated as routine.

The Service Provider must apply the above classifications in good faith to each call for support, and the Service Provider must give due consideration to any request by a Subscribing Entity to reclassify a problem, taking into account the Subscribing Entity's unique business and technical environments and any special needs it may have.

8.6. INCIDENT RESPONSE

The Service Provider must respond to critical problems by ensuring that appropriate managerial personnel are made aware of the problem and that they actively track and expedite a resolution. The Service Provider must assign support or development personnel at the appropriate level to the problem, and those personnel must prepare a work plan for the problem's expeditious resolution. The work plan must assume that the Service Provider's appropriate staff will work without material interruption until the problem is resolved properly. At the request of an affected Subscribing Entity, the Service Provider's personnel must maintain daily contact with the Subscribing Entity's technical staff to keep the Subscribing Entity abreast of efforts being made to solve the problem. The Service Provider also must provide the Subscribing Entity's technical staff with direct access to the Service Provider's support personnel and product development personnel, if appropriate, who are assigned to the problem.

The Service Provider must respond to urgent problems by having its product development and support personnel work in concert to develop a fix or a workaround. If requested, the Service Provider's support personnel must maintain regular contact with the affected Subscribing Entities to keep their technical staff abreast of progress toward a resolution of the problem. The Service Provider's support staff must include the problem in regular status reports to the Service Provider's management team. And the Service Provider's support staff must provide the fix or workaround procedure as soon as it is available.

The Service Provider must respond to routine problems by providing the affected Subscribing Entities with a fix or workaround on a priority basis if the problem is one for which an existing patch or workaround already exists. For newly identified problems falling into this classification, the Service Provider's support personnel must generate a problem report, and the appropriate development or support personnel then must prioritize the problem in relation to other outstanding product issues. The assigned priority then will govern the problem solving or developmental work needed to address the problem and the schedule for delivering a solution. For routine calls that involve end usage and configuration issues rather than bugs or other technical problems, the Service Provider's first or second level support personnel must provide the Subscribing Entity's technical staff with telephonic assistance on a non-priority basis.

8.7. RESPONSE TIMES

The maximum time that the Service Provider takes to respond initially to a support request may vary based upon the classification of the request. During the Support Window, the Service Provider's response time for a critical support request will be less than one hour. The Service Provider's response time for an urgent request must be less than two hours during the Support Window. And the Service Provider's response time for a routine support request must be less than four hours during the Support Window. The applicable Service Attachment may provide for shorter response times, and nothing contained herein will limit the

application of any credits for failure to meet any service level agreements in the applicable Service Attachment.

8.8. ESCALATION PROCESS

Any support call that is not resolved must be escalated to the Service Provider's management under the following parameters. Unresolved problems that are classified as critical must be escalated to the Service Provider's support manager within one hour and to the director level after four hours. If a critical problem is not resolved within one day, it must escalate to the CEO level after two days. The Service Provider's support staff will escalate unresolved urgent problems to its support manager within three hours, to the director level after one day, and to the CEO level after two days.

8.9. SUBSCRIBING ENTITY OBLIGATIONS

To facilitate the Service Provider meeting its support obligations, Subscribing Entities must provide the Service Provider with the information reasonably necessary to determine the proper classification of the underlying problem. They also must assist the Service Provider as reasonably necessary for the Service Provider's support personnel to isolate and diagnose the source of the problem. Additionally, to assist the Service Provider's tracking of support calls and the resolution of support issues, Subscribing Entities must make a reasonable effort to use any ticket or incident number that the Service Provider assigns to a particular incident in each communication with the Service Provider.

8.10. RELATIONSHIP TO SLAS

The Service Provider's support obligations are in addition to the SLAs in the Service Attachment(s). Furthermore, the SLAs may provide for credits to the Subscribing Entities even though the Service Provider is meeting its support obligations hereunder.

9. Standard Provisions

9.1. CERTIFICATION OF FUNDS

None of the rights, duties, or obligations in this Agreement will be binding on the State or a Subscribing Entity, and the Service Provider will not begin its performance under any Order, until all the following conditions occur for that Order:

i. all statutory provisions under the ORC, including Section 126.07, have been met;
ii. all necessary funds are made available by the appropriate State agencies;
iii. if required, approval of this Agreement or the applicable Order is given by the Controlling Board of Ohio; and
iv. if the Subscribing Entity is relying on federal or third-party funds for its Order, the Subscribing Entity gives the Service Provider written notice that such funds have been made available.

Additional or alternate legal requirements may apply to political subdivisions that are a Subscribing Entity for an Order to be binding on it.

9.2. EXCUSABLE DELAY

Neither Party will be liable for any delay in its performance that arises from causes beyond its control and without its negligence or fault. The delayed Party will notify the other promptly of any material delay in performance and will specify in writing the proposed revised performance date or dates as soon as practicable after notice of delay. The proposed date or dates must be reasonable and cannot exceed the actual delay caused by the events beyond the control of the Party. In the case of such an excusable delay, the dates of performance or delivery affected by the delay will be extended for a period equal to the time lost by reason of the excusable delay. The delayed Party must also describe the cause of the delay and what steps it is taking to remove the cause.

The delayed Party may not rely on a claim of excusable delay to avoid liability for a delay if the delayed party has not taken commercially reasonable steps to mitigate or avoid the delay. Things that are controllable by the Service Provider's suppliers will be considered controllable by the Service Provider.

In the case of subscriptions to Services for a Term that an excusable delay interrupts, the Term of that subscription will be extended at no additional cost to affected Subscribing Entities by the same amount of time as the excusable delay.

9.3. EMPLOYMENT TAXES

Each Party will be solely responsible for reporting, withholding, and paying all employment related taxes, contributions, and withholdings for its own personnel, including, but not limited to, federal, state, and local income taxes, and social security, unemployment and disability deductions, withholdings, and contributions, together with any interest and penalties.

9.4. SALES, USE, EXCISE, AND PROPERTY TAXES

The State and most Subscribing Entities are exempt from any sales, use, excise, and property tax. To the extent sales, use, excise, or any similar tax is imposed on the Service Provider in connection with any Service, such will be the sole and exclusive responsibility of the Service Provider, and the Service Provider will pay such taxes (together with any interest and penalties not disputed with the appropriate taxing authority) whether they are imposed at the time the Services are rendered or a later time.

9.5. EQUAL EMPLOYMENT OPPORTUNITY

The Service Provider will comply with all state and federal laws regarding equal employment opportunity and fair labor and employment practices, including ORC Section 125.111 and all related Executive Orders.

Before this Agreement can be awarded or renewed, an Affirmative Action Program Verification Form must be submitted to the DAS Equal Opportunity Division to comply with the affirmative action requirements. Affirmative Action Verification Forms and approved Affirmative Action Plans can be found by to the Ohio Business Gateway at: http://business.ohio.gov/efiling/

The State encourages the Service Provider to purchase goods and Services from Minority Business Enterprises ("MBEs") and Encouraging Diversity, Growth and Equity ("EDGE") contractors.

9.6. DRUG-FREE WORKPLACE

The Service Provider must comply with all applicable state and federal laws regarding keeping a drug-free workplace. The Service Provider must make a good faith effort to ensure that all its employees, while working on State property or the property of any Subscribing Entity, will not have or be under the influence of illegal drugs or alcohol or abuse prescription drugs in any way.

9.7. CONFLICTS OF INTEREST

No Service Provider personnel may voluntarily acquire any personal interest that conflicts with the Service Provider's responsibilities under this Agreement.
Additionally, the Service Provider will not knowingly permit any public official or public employee who has any responsibilities related to this Agreement to acquire an interest in anything or any entity under the Service Provider's control, if such an interest would conflict with that official's or employee's duties. The Service Provider will disclose to the State knowledge of any such person who acquires an incompatible or conflicting personal interest related to this Agreement. The Service Provider will take all legal steps to ensure that such a person does not participate in any action affecting the work under this Agreement, unless the State has determined that, in the light of the personal interest disclosed, that person's participation in any such action would not be contrary to the public interest.

9.8. ASSIGNMENT

The Service Provider may not assign this Agreement or any of its rights or obligations under this Agreement without the prior, written consent of the State.

9.9. GOVERNING LAW

This Agreement will be governed by the laws of Ohio, and venue for any disputes will lie with the appropriate court in Ohio.

9.10. FINDING FOR RECOVERY

The Service Provider warrants that the Service Provider is not subject to an unresolved finding for recovery under ORC §9.24. If the warranty is false on the date the parties signed this Agreement, the Agreement is void *ab initio*.

9.11. ANTI-TRUST

The Parties recognize that, in actual economic practice, overcharges resulting from antitrust violations are usually borne by the State and the Subscribing Entities. The Service Provider therefore assigns to the State all state and federal antitrust claims and causes of action that the Service Provider now has or may acquire relating to the Services that are covered by this Agreement.

9.12. USE OF NAME

Neither Party will use the other Party's name in any marketing material, advertisement, or press release without the other Party's written consent. Further, neither Party may use any contact information collected from the other in the performance of this Agreement for general marketing or sales purposes, such as using email addresses to send mass marketing material, and must use such information solely for purposes of administering this Agreement.

9.13. EXECUTIVE ORDER 2011-12K COMPLIANCE

The Service Provider affirms it has read and understands Executive Order 2011-12K and will abide by those requirements in the performance of this Agreement.

Notwithstanding any other Terms of this Agreement, the State reserves the right to recover any funds paid for Services the Service Provider performs outside of the United States for which it did not receive a waiver. The State does not waive any other rights or remedies provided the State in this Agreement.

The Service Provider agrees to complete the attached Executive Order 2011-12K Affirmation and Disclosure Form, which is incorporated and becomes a part of this Agreement.

9.14. CAMPAIGN CONTRIBUTIONS

The Service Provider, by signature affixed on this document, hereby certifies that all applicable parties listed in ORC Section 3517.13 are in full compliance with ORC Section 3517.13.

9.15. EXPORT COMPLIANCE

The Services and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Both the Service Provider and the State represent that it is not named on any U.S. government denied-party list. Neither party will permit others to access or use the Services in a US-embargoed country or in violation of any U.S. export law or regulation.

9.16. SAFETY AND SECURITY RULES

When accessing State networks and systems, the Service Provider must comply with all applicable State policies and regulations regarding data security and integrity. And when on any property owned or controlled by the State, the Service Provider must comply with all security and safety rules applicable to people on those premises. Subscribing Entities may have policies and regulations that are specific to them that the Service Provider must also comply.

9.17. OHIO ETHICS LAW

The Service Provider certifies that it is currently in compliance with and will continue to adhere to the requirements of the Ohio ethics laws.

9.18. ENTIRE AGREEMENT

This Agreement, together with any Service Attachments and all additional documents expressly incorporated herein, sets forth the entire agreement of the Parties with respect to the subject matter hereof and supersedes any prior agreements, promises, representations, understandings, and negotiations between the Parties with respect to the subject matter hereof.

Only executable Order attached to a Service Attachment as an exhibit and identified as such in the applicable Service Attachment may be executed by a Subscribing Entity to evidence a transaction under this Agreement. Further, the Subscribing Entity may not add or require additional Terms as part of any authorized Order. Documents attached to a Service Agreement as exhibits to be executed by a Subscribing Entity typically identify authorized Service options the Subscribing Entity has selected, provide information about a Subscribing Entity, identify installation or configuration requirements or similar Statements of Work to be done by the Service Provider, set schedules for performance, and similar matters.

9.19. SEVERABILITY

If any provision hereunder is declared or held invalid, illegal, or unenforceable by a court of competent jurisdiction, this Agreement will be revised only to the extent necessary to make that provision legal and enforceable or, if impossible, the unaffected portions of this Agreement will remain in full force and effect so long as the Agreement remains consistent with the Parties' original intent.

9.20. SURVIVAL

Any Terms, conditions, representations, or warranties contained in this Agreement that must survive termination or expiration of this Agreement to be fully effective will survive the termination or expiration of the Agreement, unless expressly provided otherwise in this Agreement. Additionally, no termination or expiration of the Agreement will affect the State's right to receive Services for which the State has paid before expiration or termination, but no subscription to a Service will continue beyond the period paid for before termination or expiration of the Agreement.

If any Service Attachment should expire or be terminated, the remaining portions of this Agreement will survive.

9.21. NO WAIVER

The failure of either party at any time to demand strict performance by the other Party of any terms or conditions of this Agreement may not be construed as a waiver of any of those terms or conditions, and either Party may at any time demand strict and complete performance by the other Party.

9.22. ORDER OF PRECEDENCE

A. In event of a conflict related to the general Terms and Conditions between the Agreement and the Service Attachment(s), the Agreement shall prevail.

B. In the event of a conflict related specifically to the service, between the Agreement and the Service Attachment(s), the Service Attachment(s) shall prevail.

9.23. HEADINGS

The headings herein are for convenience only and are not intended to have any substantive significance in interpreting this Agreement.

9.24. GOVERNMENTAL AUTHORIZATION, REGULATORY CHANGES

This Agreement is subject to all applicable federal, state, and local laws, rules, orders, and regulations, and each Party must comply with all applicable federal, state, and local laws, rules, regulations, and orders in performing its obligations hereunder. To the extent any provision of this Agreement conflicts with any such law, rule, order, or regulation, such law, rule, order, or regulation will supersede the conflicting provision. The Service Provider may discontinue, limit, or impose additional requirements to the provision of Service, upon no less than 30 days written notice, if required to meet federal, state or local laws, rules, or regulations. But if any such action materially affects any Subscribing Entity's use of a Service, the Subscribing Entity may on written notice to the Service Provider terminate its use of the Service without an Early Termination Charge and receive a pro rata refund any amounts paid in advance for the Service.

9.25. NOTICES

Except as otherwise provided in this Agreement, all notices hereunder must be in writing and sent by:

i. registered or certified mail, postage prepaid;
ii. facsimile transmission;
iii. overnight courier;
iv. or email, upon confirmation of receipt.

Alternatively, such notices may be hand delivered if confirmation of receipt is attained at delivery.

The State's address for notification is:

Department of Administrative Services
Office of Information Technology
Enterprise IT Contracting
30 E Broad Street, 39th Floor
Columbus, Ohio 43215
Attention: Contracts Category Manager

The Service Provider's address for notification is:

With a copy to:

9.26 IRS 1075 Technology Services.

In consideration of the mutual promises and obligations contained in the Agreement and this Amendment, the parties agree to add language to the Agreement as follows:

In order to protect risk of loss, breach, or misuse of Federal Tax Information ("FTI") held by government agencies, the Internal Revenue Service issued Publication 1075 which includes specific language to include in any State contract in which FTI may be disclosed.

I Performance

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

(1) All work will be done under the supervision of the Contractor or the Contractor's employees.
(2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Disclosure to anyone other than an officer or employee of the Contractor will be prohibited.
(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
(4) The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
(5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
(6) All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operations, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
(7) No work involving Federal Tax Information furnished under this Contract will be subcontracted without prior written approval of the IRS.
(8) The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
(9) The agency will have the right to void the Contract if the Contractor fails to provide the safeguards described above.

II Criminal Sanctions

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of the officer or employee (United States for Federal employees) in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence,

punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.

(3) Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (See Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III Inspection

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

9.27 Registration with the Secretary of State.

In consideration of the mutual promises and obligations contained in the Agreement and this Amendment, the parties agree to add language to the Agreement as follows:

By providing a Charter Number and signature within the Certification Offer Letter, the Contractor attest that the Contractor is:

- An Ohio corporation that is properly registered with the Ohio Secretary of State; or
- A foreign corporation, not incorporated under the laws of the state of Ohio, but is registered with the Ohio Secretary of State pursuant to Ohio Revised Code Sections 1703.01 to 1703.31, as applicable.

Any foreign corporation required to be licensed under O.R.C. § 1703.01-1703.31, which transacts business in the state of Ohio, without being so licensed, or when its license has expired or been canceled, shall forfeit not less than $250.00 nor more than ten thousand dollars. No officer of a foreign corporation http://codes.ohio.gov/orc/1703.01 shall transact business in the state of Ohio, if such corporation is required by O.R.C. § 1703.01-1803.31 to procure and maintain a license, but has not done so. Whoever violates this is guilty of a misdemeanor of the forth degree. Questions regarding registration should be directed to (614) 466-3910, or visit http://www.sos.state.oh.us

WITNESS WHEREOF, the Parties have executed this Agreement which shall be effective on the date signed by the State, 'Effective Date'.

<SERVICE PROVIDER>	**STATE OF OHIO, DEPARTMENT OF ADMINISTRATIVE SERVICES**
Signature	Signature
Printed Name	Robert Blair Printed Name DAS Director
Title	Title
Date	Effective Date

JOHN R. KASICH
GOVERNOR
STATE OF OHIO

Executive Order 2011-12K

Governing the Expenditure
of Public Funds for Offshore Services

WHEREAS, State of Ohio officials and employees must remain passionately focused on initiatives that will create and retain jobs in the United States in general and in Ohio in particular, and must do so especially during Ohio's continuing efforts to recover from the recent recession.

WHEREAS, allowing public funds to pay for services provided offshore has the potential to undermine economic development objectives in Ohio.

WHEREAS, the expenditure of public funds for services provided offshore may deprive Ohioans and other Americans of critical employment opportunities and may also undermine efforts to attract businesses to Ohio and retain them in Ohio, initiatives in which this State has invested heavily.

NOW THEREFORE, I, John R. Kasich, Governor of the State of Ohio, by virtue of the authority vested in me by the Constitution and the laws of this State, do hereby order and direct that:

1. No State Cabinet Agency, Board or Commission ("Executive Agency") shall enter into any contract which uses any public funds within its control to purchase services which will be provided outside the United States. This Executive Order applies to all purchases of services made directly by an Executive Agency and services provided by subcontractors of those providing services purchased by an Executive Agency.

2. This Executive Order will be personally provided, by the Director, Chair or other chief executive official of each Executive Agency, to the Chief Procurement Officer or other individual at that entity responsible for contracts for services.

3. The Department of Administrative Services, through Ohio's Chief Procurement Officer, shall have in place, by July 1, 2011, procedures to ensure all of the following:

    a. All agency procurements officers (APOs), or the person with equivalent duties at each Executive Agency, have standard language in all Executive Agency contracts which:

        i. Reflect this Order's prohibition on the purchase of offshore services.

ii. Require service providers or prospective service providers to:

1. Affirm that they understand and will abide by the requirements of this Order.
2. Disclose the location(s) where all services will be performed by any contractor or subcontractor.
3. Disclose the locations(s) where any state data associated with any of the services they are providing, or seek to provide, will be accessed, tested, maintained, backed-up or stored.
4. Disclose any shift in the location of any services being provided by the contractor or any subcontractor.
5. Disclose the principal location of business for the contactor and all subcontractors who are supplying services to the state under the proposed contracts.

b. All APOs confirm that all quotations, statements of work, and other such proposals for services affirm this Order's prohibition on the purchase of offshore services and include all of this Order's disclosure requirements.

i. Any such proposal for services lacking the affirmation and disclosure requirements of this Order will not be considered.
ii. Any such proposal where the performance of services is proposed to be provided at a location outside the United States by the contractor or any subcontractor will not be considered.

c. All procurement manuals, directive, policies, and procedures reflect the requirements of this Order.

d. All APOs have adequate training which addresses the terms of this Order.

4. Nothing in this Order is intended to contradict any state or federal law. In addition, this Order does not apply to:

a. Services necessary to support the efforts of the Department of Development to attract jobs and business to the state of Ohio;
b. Academic, instructional, educational, research or other services necessary to support the international missions of Ohio's public colleges and universities; or
c. Situations in which the Director of the Department of Administrative Services, or the Director's designee, shall determine that it is an emergency or that it is necessary for the State to waive some or all of the requirements of this Order. The Director shall establish standards by which Executive Agencies may request a waiver of some or all of the requirements of this Order and by which such requests will be evaluated and may be granted.

5. Executive Order 2010-09S is hereby rescinded.

I signed this Executive Order on June 21, 2011 in Columbus, Ohio and it will expire on my last day as Governor of Ohio unless rescinded before then.

John R. Kasich, Governor

ATTEST:

Jon Husted, Secretary of State

Master Cloud Service Attachment

This Service Attachment (the "Service Attachment"), is between _____ ("Service Provider") having an office at _____, and the State of Ohio, through the Department of Administrative Services, Office of Information Technology ("the State"), having its principal place of business at 1320 Arthur E. Adams Drive, 3rd Floor, Columbus, OH 43221 (jointly referred hereto as the "Parties"), and it is effective as of the date signed by the State. It amends that certain Master Cloud Services Agreement ("MCSA") between the Parties dated _____.

1. Definitions. [None.]

The defined terms in the Master Cloud Services Agreement will have the same meanings in this Service Attachment as they do in the MCSA. There may be additional definitions contained herein.

2. Services.

Overview. [Provide a list of all Services available under this Service Attachment and a description of each. A separate Services Attachment should be used for each major Service of the Service Provider.]

STANDARD SERVICE FEATURES. [LIST AND PROVIDE A DESCRIPTION OF ALL SERVICE FEATURES THAT ARE INCLUDED AS PART OF THE STANDARD COST.]

Optional Service Features. [List and provide a description of all optional Service features that are not included as part of the standard cost, such as costs associated with bandwidth, page views, storage, organizations ("Orgs"), domains, sandboxes, full sandboxes, and such. Otherwise it will be agreed and stated that all such items are free of charge and will be provided in unlimited quantities.]

Provision of Services. The Service Provider will make the Services available to the Subscribing Entities pursuant to the Agreement, this Service Attachment, and the applicable Order Forms during each Order Term. The State agrees that purchases hereunder are neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public comments made by the Service Provider regarding future functionality or features.

The Service Provider Responsibilities. The Service Provider must: (i) provide the Service Provider's basic support for the Services to the Subscribing Entities at no additional charge, and/or upgraded support if available and if purchased, (ii) use commercially reasonable efforts to make the Services [available 24 hours a day, 7 days a week], except for: (a) planned downtime (of which the Service Provider must give at least 8 hours' notice via the Services and which the Service Provider must schedule [10 p.m. and 6 a.m. Eastern Time and on Saturdays], or (b) any unavailability covered by the Agreement's Excusable Delay clause or by the Service Level section later herein, and (iii) provide the Services in full accordance with applicable laws and government regulations.

3. Fees and Payment

Fee Structure. [Provide pricing information for all Services and all optional features. Include all parameters, such as length of subscription, volume discounts, discount from list price, and payment intervals and due dates. Include a professional services rate card or a blended rate, if applicable, for such things as training, consulting, etc.]

Fees. The Subscribing Entities will pay all fees specified in all Order Forms hereunder, subject to the terms of the Agreement. Except as otherwise specified herein or in an Order Form, fees are based on Services purchased and not actual usage, and the number of Object subscriptions (e.g., the number of users) purchased cannot be decreased during the relevant Order Term, except as provided in the Agreement. They may, however, be increased during an Order Term. Object subscription fees are based on [monthly] periods that begin on the subscription start date and each [monthly] anniversary thereof; therefore, fees for Object subscriptions added in the middle of a [monthly] period will be charged for that full [monthly] period and the [monthly] periods remaining in the subscription term. Additions of Object subscriptions during a term does not extend that term. No Order Form may specify a subscription term not identified and priced in this Attachment. Nor may it cover any billable services not listed in this Service Attachment as a Service.

After 90 days, the Service Provider may suspend the delinquent Subscribing Entity's access to the unpaid Services until all delinquent amounts are paid, notwithstanding the prohibition against self-help provided for elsewhere in the Agreement, but the Service Provider may not do so if the Subscribing Entity is disputing the applicable charges reasonably and in good faith and is cooperating diligently to resolve the dispute.

Invoicing and Payment. Fees will be invoiced [monthly in arrears] and otherwise in accordance with the Order Form and the Agreement. Fees are due in accordance with the terms of the Agreement, which no Order Form may alter. The Subscribing Entity is responsible for providing complete and accurate billing and contact information to the Service Provider and notifying the Service Provider of any changes to such information.

4. Proprietary Rights

Reservation of Rights in Services. Subject to the limited rights expressly granted hereunder, the Service Provider reserves all rights, title, and interest in and to the Services, including all related intellectual property rights. No rights are granted to the State or Subscribing Entities hereunder other than as expressly set forth herein or elsewhere in the Agreement.

Restrictions. Subscribing Entities will not intentionally permit any third party to access the Services, except as permitted herein or in an Order Form, create derivative works based on the Services except as permitted herein or elsewhere in the Agreement, reverse engineer the Services, or access the Services to build a competitive product or service or to copy any features, functions, or graphics of the Services. Nothing herein prohibits a Subscribing Entity from porting and hosting Generated Code, as defined in this Agreement, to other sites to support its own business purposes during and after any term of an Order.

State Applications and Code. If a Subscribing Entity, a third party acting on a Subscribing Entity's behalf, or a user creates applications or program code using the Services, such will be part of the Subscribing Entity's Data. The Subscribing Entity authorizes the Service Provider to host, copy, transmit, display, and adapt such applications and program code, solely as necessary for the Service Provider to provide the Services in accordance with this Agreement. Subject to the above, the Service Provider acquires no right, title or interest from the Subscribing Entity or its licensors under this Agreement in or to such applications or program code, including any intellectual property rights therein, and the Subscribing Entity is entitled to port, use, and host such anywhere.

Subscribing Entity Data. Subject to the limited rights granted by a Subscribing Entity hereunder, the Service Provider acquires no right, title, or interest from a Subscribing Entity or its licensors under this Agreement in or to the Subscribing Entity Data, including any intellectual property rights therein.

5. Service Levels

SLAs for the Services. This Agreement includes SLAs that will be used to monitor and manage the Service Provider's performance of Services. The minimum SLAs are listed below, but the Service Provider may supplement them with additional SLAs that are generally applicable to its other Services customers, so long as those additional SLAs cover parameters not addressed in the below SLAs or are more stringent than those listed below. Modifications to the SLAs provided below may only be made by the written agreement of the State and the Service Provider, except with respect to SLAs the Service Provider offers generally to other customers that are more stringent or in addition to those below.

Availability. "Availability" or "Available" means the Subscribing Entity's users are able to access a Service and use all material features and functions of the Service effectively and efficiently and the Service meets all the SLAs contained in this Attachment. "Unavailable" or "Unavailability" means the Subscribing Entity's users are unable to access the Service or use all the Service's features and functions effectively and efficiently or they do not otherwise meet all SLAs in this Service Attachment, subject to the following:

> A Service may be inaccessible to a Subscribing Entity's users during scheduled downtime. Scheduled downtime will occur for less than [one hour] between [10 p.m. and 6 a.m. Eastern Time and on Saturdays], but not more than once [monthly]. The Service Provider may change the scheduled downtime to other non-business hours upon reasonable notice to the affected Subscribing Entities. Scheduled downtime will not be considered times when the Services are Unavailable.

In addition to scheduled downtime, the following will not be considered times when a Service is Unavailable:

(i) Outages resulting from a Subscribing Entity's equipment or its Internet service provider;
(ii) A Subscribing Entity's negligence or breach of its material obligations under this Agreement; and
(iii) Excusable Delays, as provided for and handled in accordance with the Agreement.

SLA Credits.

The "Target Availability Level" is the Service's Availability Level that the Service Provider plans to meet or exceed during each calendar month. The "Service Availability Level" is the number of hours during a particular period that the Service was Available to the Subscribing Entity, excluding scheduled downtime permitted above, and divided by the total number of hours during such period. The Target Availability Level is provided in the next section.

The Service Provider must actively monitor and report to the State and each Subscribing Entity any and all Unavailability of a Service monthly, along with reasonable details regarding such Unavailability. The Service Provider also must provide each Subscribing Entity that uses the Service a credit within 30 days of any calendar month in which the Service Availability Level is below the Target Availability Level, calculated as set forth herein.

The applicable credit will be calculated as follows: If the Service Provider fails to meet the Target Availability Level by up to four hours, each affected Subscribing Entity will be entitled to the equivalent of one day's fee for the Service. That is, if the fee is an annual fee, the credit would be 1/365th of that annual fee, or if it is a monthly fee, the Subscribing Entity would be entitled to 1/30th of its monthly fee as a credit. Further, the credit will double if the Target Availability Level is missed by more than four but less than eight hours for any calendar month. And if the failure to meet the Target Availability Level is greater than eight hours, the Subscribing Entity will be entitled to the entire fee applicable to that month.

Any such credits must be paid to the Subscribing Entity within 30 days after the month in which the Service Provider fails to meet the Target Availability Level.

If the Service Provider fails to meet the Target Availability Level for three consecutive calendar months, any affected Subscribing Entity may terminate any or all Orders for that Service for cause.

Specific SLAs.

The Target Availability Level is [99.9%] in any calendar month. For a Service to be considered Available, the following parameters also must be met:

[Insert SLAs for performance parameters such as response time, page refresh rate, a permissible window for disaster recover, etc.]

6. Terms and Termination

Term of Subscriptions. Subscriptions commence on the start date specified in the applicable Order Form and continue for the subscription term specified therein, subject to relevant provisions in the MCSA, such as termination and the non-appropriation provisions. Should a Subscribing Entity elect to renew a subscription, provided this Agreement remains in effect or is renewed, the renewal will be at the Subscribing Entity's option and will be for the same or greater discount from list as the subscription being renewed and under the same terms and conditions, unless a change in governmental law, rules, or regulations requires a modification, in which case the Parties will in good faith negotiate the modifications necessitated by such a change in governmental law, rules, or regulations.

7. Miscellaneous

RETURN OF SUBSCRIBING ENTITY DATA

At no additional cost to the Subscribing Entity, upon request made at anytime during a Service term or within 90 days after the effective date of termination or expiration of a Subscribing Entity's Order for that Service, the Service Provider will make available to the Subscribing Entity for download its Subscribing Entity Data covered by that

terminated or expired Service, including any Generated Files, in native format or any other format the Subscribing Entity reasonably requests within one day of the request and at no additional charge to the Subscribing Entity. After such 90-day period, the Service Provider will have no obligation to maintain the Subscribing Entity Data covered by an expired Service Order and must thereafter, unless legally prohibited, delete the applicable Subscribing Entity Data in its systems or otherwise in its possession or under its control.

[Add anything not covered by the above sections.]

In Witness Whereof, the Parties have executed this Service Attachment, which is effective on the date the State's duly authorized representative signs it on behalf of the State, ("Effective Date").

SERVICE PROVIDER	**STATE OF OHIO, DEPARTMENT OF ADMINISTRATIVE SERVICES**
Signature	Signature
Printed Name	Printed Name
Title	Title
Date	Effective Date

JOHN R. KASICH
GOVERNOR
STATE OF OHIO

Executive Order 2011-12K

Governing the Expenditure
of Public Funds for Offshore Services

WHEREAS, State of Ohio officials and employees must remain passionately focused on initiatives that will create and retain jobs in the United States in general and in Ohio in particular, and must do so especially during Ohio's continuing efforts to recover from the recent recession.

WHEREAS, allowing public funds to pay for services provided offshore has the potential to undermine economic development objectives in Ohio.

WHEREAS, the expenditure of public funds for services provided offshore may deprive Ohioans and other Americans of critical employment opportunities and may also undermine efforts to attract businesses to Ohio and retain them in Ohio, initiatives in which this State has invested heavily.

NOW THEREFORE, I, John R. Kasich, Governor of the State of Ohio, by virtue of the authority vested in me by the Constitution and the laws of this State, do hereby order and direct that:

1. No State Cabinet Agency, Board or Commission ("Executive Agency") shall enter into any contract which uses any public funds within its control to purchase services which will be provided outside the United States. This Executive Order applies to all purchases of services made directly by an Executive Agency and services provided by subcontractors of those providing services purchased by an Executive Agency.

2. This Executive Order will be personally provided, by the Director, Chair or other chief executive official of each Executive Agency, to the Chief Procurement Officer or other individual at that entity responsible for contracts for services.

3. The Department of Administrative Services, through Ohio's Chief Procurement Officer, shall have in place, by July 1, 2011, procedures to ensure all of the following:

    a. All agency procurements officers (APOs), or the person with equivalent duties at each Executive Agency, have standard language in all Executive Agency contracts which:

        i. Reflect this Order's prohibition on the purchase of offshore services.

ii. Require service providers or prospective service providers to:

1. Affirm that they understand and will abide by the requirements of this Order.
2. Disclose the location(s) where all services will be performed by any contractor or subcontractor.
3. Disclose the locations(s) where any state data associated with any of the services they are providing, or seek to provide, will be accessed, tested, maintained, backed-up or stored.
4. Disclose any shift in the location of any services being provided by the contractor or any subcontractor.
5. Disclose the principal location of business for the contactor and all subcontractors who are supplying services to the state under the proposed contracts.

b. All APOs confirm that all quotations, statements of work, and other such proposals for services affirm this Order's prohibition on the purchase of offshore services and include all of this Order's disclosure requirements.

i. Any such proposal for services lacking the affirmation and disclosure requirements of this Order will not be considered.
ii. Any such proposal where the performance of services is proposed to be provided at a location outside the United States by the contractor or any subcontractor will not be considered.

c. All procurement manuals, directive, policies, and procedures reflect the requirements of this Order.

d. All APOs have adequate training which addresses the terms of this Order.

4. Nothing in this Order is intended to contradict any state or federal law. In addition, this Order does not apply to:

a. Services necessary to support the efforts of the Department of Development to attract jobs and business to the state of Ohio;
b. Academic, instructional, educational, research or other services necessary to support the international missions of Ohio's public colleges and universities; or
c. Situations in which the Director of the Department of Administrative Services, or the Director's designee, shall determine that it is an emergency or that it is necessary for the State to waive some or all of the requirements of this Order. The Director shall establish standards by which Executive Agencies may request a waiver of some or all of the requirements of this Order and by which such requests will be evaluated and may be granted.

5. Executive Order 2010-09S is hereby rescinded.

I signed this Executive Order on June 21, 2011 in Columbus, Ohio and it will expire on my last day as Governor of Ohio unless rescinded before then.

John R. Kasich, Governor

ATTEST:

Jon Husted, Secretary of State

STANDARD AFFIRMATION AND DISCLOSURE FORM

EXECUTIVE ORDER 2011-12K

Governing the Expenditure of Public Funds on Offshore Services

All of the following provisions must be included in all invitations to bid, requests for proposals, state term schedules, multiple award contracts, requests for quotations, informal quotations, and statements of work. This information is to be submitted as part of the response to any of the procurement methods listed.

By the signature affixed hereto, the Service Provider affirms, understands and will abide by the requirements of Executive Order 2011-12K. If awarded a contract, both the Service Provider and any of its subcontractors will perform no Services requested under this Agreement outside of the United States.

The Service Provider will provide all the name(s) and location(s) where Services under this Agreement will be performed in the spaces provided below or by attachment. Failure to provide this information may subject the Service Provider to sanctions. If the Service Provider will not be using subcontractors, indicate "Not Applicable" in the appropriate spaces.

3. Principal location of business of Service Provider:

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

   Name/Principal location of business of subcontractor(s):

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

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

4. Location where Services will be performed by Service Provider:

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

   Name/Location where Services will be performed by subcontractor(s):

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

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

5. Location where state data will be stored, accessed, tested, maintained or backed-up, by Service Provider:

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

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

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

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

Service Provider also affirms, understands and agrees that Service Provider and its subService Providers are under a duty to disclose to the State any change or shift in location of Services performed by Service Provider or its subcontractors before, during and after execution of any Agreement with the State. Service Provider agrees it will so notify the State immediately of any such change or shift in location of its Services. The State has the right to immediately terminate the contract, unless a duly signed waiver from the State has been attained by the Service Provider to perform the Services outside the United States.

On behalf of the Service Provider, I acknowledge that I am duly authorized to execute this Affirmation and Disclosure form and have read and understand that this form is a part of any Agreement that Service Provider may enter into with the State and is incorporated therein.

By: _____
Service Provider

Print Name: _____

Title: _____

Date: _____

Supplement 1

Enterprise Identity Validation, Authentication and Fraud Services

Table of Contents

1.0 Enterprise Identity, Authentication and Fraud: Background and Overview 3

1.1 General State Enterprise Goals 3
1.2 State Agency Adoption Goals 4
1.3 General Solution Scope 4

2.0 State Objectives and General Organization of Requirements 5

2.1 State Summary Objectives 5
2.2 Conceptual Organization of Requirements 6

3.0 Enterprise Architecture and Integration Standards and Conventions 9

3.1 Design, Integration and Scalability Considerations 9
3.2 Technical Standards Requirements 10
3.3 Enterprise Directory Support 11
3.4 APIs, Workflow and State Development Tool Support 12
3.5 Directory Services and Provisioning 12
3.6 Audit and Logging Requirements 13
3.7 Account Management and Linking Requirements 13
3.7.1 General Application Use and Integration Requirements 13
3.7.2 Agency Application Use and Integration Requirements 14
3.8 User, Portal and Certificate Administration Requirements 14
3.8.1 User Administration and Provisioning Requirements 14
3.8.2 Single Sign-On Support 15
3.8.3 Certificate and Encryption Key Management 15
3.8.4 Solution Administration Portal: Users, Relying Parties and State 15

4.0 Multi-Factor Definitive Identity Proofing 16

4.1 General Requirements 17
4.2 Privacy Requirements 18
4.3 FICAM Compatibility and Evolution Currency 19
4.4 Protocol Standards and Support 19
4.5 Service Provider Diversity and Extensibility Requirements 20
4.6 Attribute Proofing Requirements 20
4.7 Auditing and Reporting Requirements 21
4.7.1 Auditing Requirements 21
4.7.2 Reporting Requirements 22
4.8 Compliance Requirements 22
4.9 General State Integration Requirements 22

5.0 State Systems Integration Services 23

5.1 State, Government and Commercial Identity Data Sources 24

6.0 Solution Pilots - General Requirements and Considerations 26

6.1 Pilot Agency 1: Ohio Enterprise eLicensing System (Identity Proofing, 2FA) 27
6.1.1 eLicensing Platform Sizing Considerations 28
6.2 Pilot Agency 2: Ohio Business Gateway 3.0 (Business Identities and 2FA) 28
6.2.1 General OBG 3.0 Considerations 30
6.2.2 Specific OBG 3.0 Requirements on the Services/Solution in this RFP 30
6.3 Pilot Agency 3: Ohio Department of Taxation (Identity and Attribute Proofing) 31
6.4 Post Pilot Activities: Development of Extensible Enterprise Standards 33

7.0 Implementation of Two Factor Authentication (2FA) 34

7.1 User Authentication 34
7.2 Standards Compliance 35
7.3 Technical, Operations, Change and Scalability 35
7.3.1 General Technical Requirements 35
7.3.2 Performance and Scalability Requirements 36
7.3.3 Operations, Maintenance and Change Management 36
7.4 Authentication and Access Logging and Reporting 37
7.4.1 Authentication/Access Reporting and Logging 37
7.4.2 System Operational Reporting, Alerts and Notifications 37

8.0 Implementation of Enterprise Logging, Audit and Fraud Detection 37

8.1 Programmatic Fraud Detection and Fraud Analytics 38
8.2 Identifying and Remanding Suspicious Identities to Proofing and Other Methods 39
8.3 Integration with Enterprise Security, Notification and Tracking Services 40
8.3.1 General Identification and Integration Requirements 40

8.3.2 State Enterprise Security Event Management System Integration 40
8.3.3 Other Notification Capabilities 41
8.4 Incorporating Fraudulent Identities and Entities in State Data Stores, Onward Sharing within the State 41
8.5 Auditing and Reporting Requirements 41

9.0 State Project Delivery, Management, Methodology and Approach Requirements 42

9.1 Project Management and Coordination Services 43
9.2 Create and Maintain Project Plan 44
9.3 Project Review Check Point. 45
9.4 Meeting Attendance and Reporting Requirements. 46
9.5 Utilize OIT's Document Sharing/Collaboration Capability 47
9.6 Production/Version Control and Release Management 47
9.7 Maintaining Solution and Operations Documentation 48
9.8 Project Delivery, Role and Responsibility Requirements 48
9.9 System/Environment Administration Support of the Project 49
9.10 Establish and Manage a Program Management & Master Release Calendar 49
9.11 Cooperation with State and State Contractors 49
9.12 Requirements Confirmation and Analysis (for each Pilot Agency) 49
9.13 Analyze Phase Requirements (for each Pilot Agency) 49
9.14 Design Phase Requirements (for each Pilot Agency) 50
9.15 Build Phase Requirements (for each Pilot Agency) 50
9.16 Test Phase Requirements (for each Pilot Agency) 51
9.17 Deploy Phase Requirements (for each Pilot Agency) 52
9.18 Knowledge Transfer and Production Handoff 53
9.19 Project Completion Activities, Final Documentation and Post Implementation Support Obligations 54
9.20 Future Project Services Pricing Response and Rate Card 54

10.0 Schedule of Deliverables and Work Products 54

10.1 Delivery and Deliverable Standards 55
10.2 Schedule of Key Project Management Deliverables and Work Products 55

11.0 Assumptions 58

11.1 Support Requirements 58
11.2 Pre-Existing Materials 59
11.3 Commercial Materials 59

12.0 State Staffing Requirements 59

12.1 Contract Staffing and Key Activities 60
12.2 Staffing Plan and Time Commitment 61
12.3 Background Checks 62

13.0 Service Level Requirements: Identity Proofing & 2FA Service Providers 63

13.1 Service Availability 63
13.2 Priority 1 Outage Resolution Time 63
13.3 System Performance and Timeliness 63
13.4 Service Level Specific Performance Credits 63

14.0 Service Level Requirements: State Systems Integration Projects 63

14.1 Service Level Specific Performance Credits 64
14.2 Overall Contract Performance 65
14.3 Monthly Service Level Report 66
14.4 Service Level Commitments – Project Implementation Services 66
14.5 Service Level Specifications 68
14.5.1 Defect Resolution – Mean Time to Repair/Resolve (Priority 1 Items) 68
14.5.2 Defect Resolution – Mean Time to Repair/Resolve (Priority 2 Items) 69
14.5.3 Defect Resolution – Mean Time to Repair/Resolve (Priority 3 Items) 70
14.5.4 Service Levels – Testing Performance 71
14.5.5 Blocking Issues – Identification and Removal 72
14.5.6 Regression Testing Performance – Issue Find/Fix Rate 73
14.5.7 Code Coverage – Automated Test Beds 74
14.5.8 Service Levels – Project Performance 75
14.5.9 Issue Reporting 76
14.5.10 Deliverable Acceptance 77
14.5.11 Support of State User Acceptance Testing Activities 78
14.5.12 Service Levels – Development Methodology Compliance 79
14.5.13 Service Levels–Project Delivery–Build/Test Activities as a Percentage of Overall Activities 80
14.5.14 Service Levels – Project Completion – Issues Detected and Resolved In Production 81

1.0 Enterprise Identity, Authentication and Fraud: Background and Overview

The State, as part of its continual efforts to review, revise and enhance the capabilities of its information technology environment, systems and processes recently conducted an analysis of several large Cabinet Agencies to better understand system capabilities to manage user identities, identify personal information and financial fraud origins and defenses and methods to better protect sensitive data maintained in the State's IT systems portfolio. The goal of the State via this project and its implementation is to specify, design and implement a core set of capabilities as an Enterprise Framework to allow Individuals (citizens and businesses) and State Agencies to utilize secure, efficient, easy-to-use, and interoperable identity solutions to access State online services and applications in a manner that promotes confidence, privacy, choice, and innovation.

Due to the nature of the data contained in this analysis, the details of this analysis shall remain confidential to the State, but in summary, the analysis determined that:

- Sensitive Data is maintained in almost every Agency across the State and more than half of all State systems maintain some form of Sensitive Data;
- A significant number of State systems maintain Sensitive Data that would have a direct public impact in the event of a data breach or loss;
- While most data maintained by the State is at State data processing centers there remain a substantial number of systems at Agency locations and State contracted Service Provider locations that require regular review and monitoring for physical, system and other access exposures;
- Many systems that contain Sensitive Data are not under the sole purview of State Employees;
- High value ($ financial) and high volume (e.g., millions of citizens) represent the highest relative risk which require enhanced capabilities to establish, verify, authenticate, log and monitor from a security/privacy perspective;
- The State has an opportunity to establish enterprise capabilities and services for State systems that maintain sensitive data as well as a programmatic capability to provide for identity or financial fraud protection; and

This work is to augment the State's efforts to secure computing locations, networks, servers, storage and data (e.g., physical access, validation and secure encryption) and migrate to more service oriented methods for data exchange that minimizes the "physicalization" of data (data at rest) and tie into other efforts currently underway.

1.1 General State Enterprise Goals

The Service from an end-to-end perspective (i.e., establishing identities, managing them, integrating with State systems and services, and authenticating access) must foster simpler, more trustworthy and secure interactions between the State and our constituents.

The Service or System must demonstrate an improved user experience (e.g., less passwords to remember and no need to go through laborious credentialing processes for each Agency and each system within an Agency).

The Service or System must reduce cost and complexity to State Agencies through economies of scale from an Identity, Integration and Authentication perspective.

The Service or System must result in enhanced security for the State in the form of fraud protection for personal, financial and other sensitive information contained in State systems.

The Service or System must be an enabler of the State for the increased use of on-line services and increasingly mobile services, thus reducing manual costs.

The Service or System must integrate with and extend the State's security event monitoring capability both within Agencies and across the State enterprise to enhance the State's ability to detect and identify real or suspected fraudulent access to State systems, services, applications and data stores through a variety of access means – online users, internal to the state and within the technical infrastructure that supports these systems and services.

1.2 State Agency Adoption Goals

For the Service to be successful it must demonstrate reduced cost to agencies (single interface) and increase the speed of identity integration, management and fraud detection/prevention.

The Service must complement efforts currently underway to physically centralize and secure State infrastructure, networks and hardware as well as the data contained on Storage media.

The Service must result in and support enhanced citizen privacy through pseudonymous identifiers and blinding of credential usage to those not involved in conducting business with the State (e.g., ID and Authentication providers won't know which Agency service the user is accessing or what details are shared during transactions and interactions).

The Service must complement and support State and Federal IT laws and policies regarding the protection of data and privacy while being easy for agencies to consume, incorporate into their systems and services (both new and existing) and utilize as a cost-effective Enterprise standard.

1.3 General Solution Scope

Through this RFP, the State requires the design, implementation and production deployment (i.e., live commercial use) of an **Identity Assurance Model** that allows for authorized identity providers from both the private and public sector to be utilized and be certified on levels 1 through level 4.

These **Assurance Levels** must adhere to established Industry conventions and standards and are defined as:

Level 1 – No identity proofing is required for this level. There is typically some assurance that the person who created the account is the one who is using it but little beyond that.

Level 2 – Provides single factor remote network authentication. Identity proofing requirements are introduced, requiring presentation of identifying materials or information.

Level 3 - Provides multi-factor remote network authentication. At least two authentication factors are required. At this level, identity-proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of the allowed types of tokens through a cryptographic protocol.

Level 4 - Is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. At this level, in-person identity proofing is required. Level 4 is similar to Level 3 except that only "hard" cryptographic tokens are allowed.

Based on the State's determination of risk factors and Agency needs and the capabilities of a State system to support the aforementioned Identity Assurance Model, the State will determine the appropriate Level of Identity Assurance for systems. This RFP contains provisions for a Pilot Implementation for the State and utilizes one or more of these Assurance Levels.

The State maintains a variety of **User Populations** in the course of serving the public and providing necessary services as part of its public remit. These populations vary by system and Agency but for definitional and simplicity purposes, this RFP considers these Populations as follows:

State Worker – Known State Agency employees, Known State Contingency workers, and Known Agency staff, State Contractors and Vendors.

State Privileged User - Known State Agency employees, Known State Contingency workers, and Known Agency staff who maintained elevated systems or infrastructure (facilities, network, server, storage and security) access to State systems. These users would include (but are not be limited to) those State users who maintain some form of deep technical access to State systems or infrastructure such as database administrators, operating system "administrator or root" equivalent, network/firewall administrators, security and privacy personnel or those users who process high value financial or large amounts of personally identifiable data.

Business – An entity that represents a business and who is authorized to conduct business with the State on behalf of that entity.

Citizens - An individual or individuals conducting business with the State for themselves or on the behalf of an individual.

Based on the above, the State requires the implementation of **Access, Authorization and Accounting Protocols** that are designed to assure that an authorized identified user is in fact who they assert to be. These Protocols include:

Identity Proofing – the e-authentication process, by which an assertion of an identity is verified, including:

- **Risk-Based Authentication** – a technique that uses both contextual and historical customer information, along with data supplied during a transaction, to assess authenticity of a customer interaction; and
- **Out-of-Wallet Data** – refers to private data used for authentication activities, e.g., any personal information that cannot be found in a person's wallet. "Out-of-wallet" data may be drawn from public, publicly available and non-public proprietary databases. The State believes that some "out of wallet" data may no longer be the state of the art as many attributes can be easily found on the web. Some drivers license data includes factors which are designed to be preventative, and then only so if the individual has limited attempts to provide this data. For instance, if asked "color of hair or eyes" and given more than one attempt, this is too easy to guess to utilize as "out of wallet" verification, therefore additional methods must be included in the proposed solution.

Two Factor Authentication – Two-factor authentication adds a second level of authentication to an account log-in. Use of only a username and one password, is considered a single-factor authentication. Two Factor Authentication requires a user to have two out of three types of credentials before being able to access an account. The three types are:

1. Something known by the user, such as a personal identification number (PIN), password or a pattern.
2. Something the user possesses, such as an ATM card, phone, or fob.
3. Something that is part of the user, such as a biometric like a fingerprint or voice print.

2.0 State Objectives and General Organization of Requirements

2.1 State Summary Objectives

The State's Summary Objectives are in light of increasingly public breaches of data from public and private institutions. The State wishes to significantly increase its capabilities through the acquisition and implementation of services and systems to:

1. Establish and thereafter maintain **Identity Proofing Services** through one or more Service Providers that support access by the Public (both Citizens and Businesses) in the State through the use of User Identification credentials that are verified using a combination of Private Data (i.e., that data not known by the State, but known to an individual and State Data (i.e., that data known to the State and the individual).
2. Work to ensure that the aforementioned service **balances ease of use** in creating, establishing and maintaining Identities by the Public with provisions to reduce or eliminate these Identities being **compromised or used for fraudulent or not-authorized purposes** by a third party.
3. Develop a set of **Enterprise Frameworks** and implement Agency Systems as a meaningful Pilot that is suitable to address the variety of risk profiles associated with accessing State systems (e.g., accessing non-sensitive data, routine administrative systems use, accessing high-risk data types such as those that contain personal, private, confidential or monetary/financial details).

4. Migrate State critical systems access – by the Public, State Employees, Contractors and State Privileged Users to a seamless **two-factor ID Authentication and Accounting environment** that positions the State to move away from a login/password paradigm to a trusted and validated operation that reduces risk.

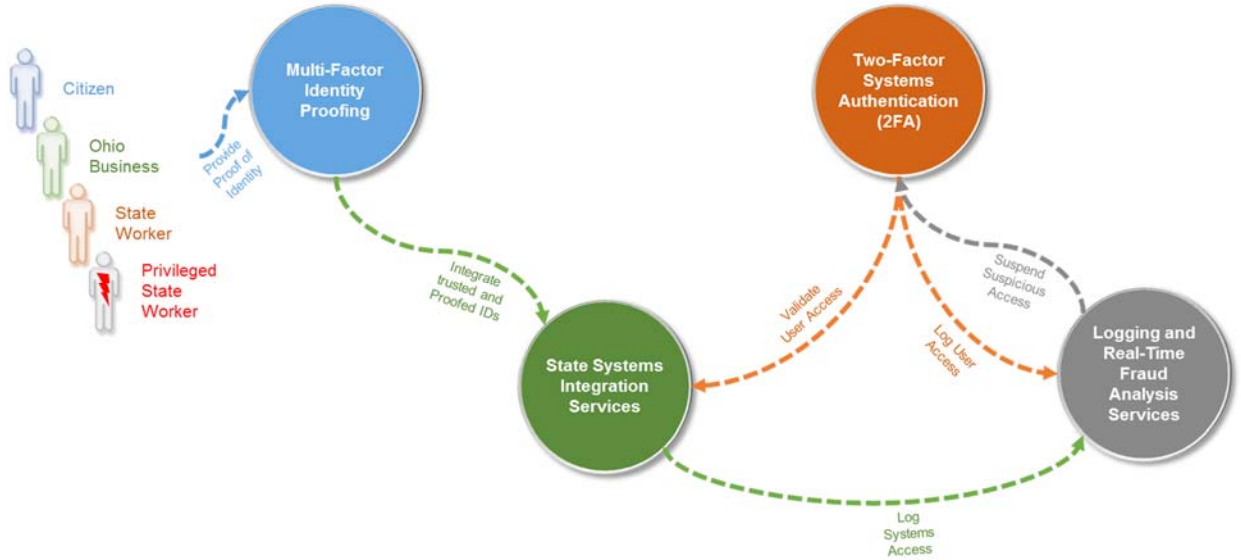
5. Implement programmatic **Fraud Identification and Monitoring** services that work in conjunction with the aforementioned capabilities as well as with State infrastructure elements (e.g., networks, firewalls, security/authentication methods) to programmatically log, analyze, report and alert on real or suspected fraud and threats to State systems and infrastructure via Identities, access or other means to defraud the State, our citizens and businesses.

6. Implement the above capabilities in a **phased approach that demonstrates end-to-end capabilities** for a set of Pilot Systems **in a full production environment** and create a repeatable capability to deploy the solution as an Enterprise Framework Service for all new and existing systems that are considered high risk by the State.

2.2 Conceptual Organization of Requirements

This Supplement is organized as follows: specific Enterprise (i.e., the State as an Enterprise or as a whole) requirements (e.g., suitable for both new system specifications and deployments as well as incorporation into existing systems and processes) and Pilot Requirements (i.e., Initial Agency systems that have an immediate need and have been identified by the State as candidates to immediately leverage key elements of the Enterprise requirement set) which are contained later in this Supplement with requirements specific to those systems.

Conceptual Organization and Relationships of Requirement Areas in this Supplement



Detailed requirements and specifications appear later in this Supplement, but in **general** these requirement areas are organized as follows:

Multi-Factor Identity Proofing Services

The Contractor will specify, design and implement a solution, which will utilize public, and private data sources to identity proof individuals, compliant with NIST 800-63 guidelines and use multiple verification methods to accurately verify identity traits. At a minimum, this data must include name, date of birth, address, and financial account information and incorporate secondary data including other personal information and must be “out-of-wallet” data. The State may require upon request a verification score based on State customized set of business

rules used to verify the individual (include a past history of fraud and State provided data in this scoring routine). As part of the specification, design and implementation of this service, the Contractor will provide State with recommendations for other personal information that can be used for identity proofing (for example, prior addresses) as well as inclusion of State known fraudulent identities maintained by Agencies.

The service should be designed and implemented to offer real-time identity verification while ensuring security and privacy of customer data. The service should also provide a seamless experience for the Public while not requiring a significant change to the Agency Web and Application experience. As part of this effort, the Contractor must utilize a cross-industry compilation of identity information (e.g., financial information, property, telephone, address, etc.) as part of its analysis of a transaction. The service shall not rely upon State for identity verification information.

The service shall dynamically generate multiple-choice questions sufficiently unique to the individual to be used for authentication purposes and be capable of identifying fraudulent and/or stolen identities. The information to detect these identities must be updated regularly, preferably on a daily basis and utilize a wide variety of data to be effective with emerging market segments, such as younger generations, which may not have public record data or credit history data.

If the service detects a suspicious transaction (defined as a risk score below the State defined threshold), it shall provide the State with additional ID proofing questions in real time to allow end customers to quickly confirm their identity. The State will send the customer's responses back to the service for verification.

The service will generate a risk score, which will be transmitted in real time to State. State will not serve as a data provider within the scope of the solution beyond providing the minimum authentication data required to initiate generation of a risk score. The service shall be transparent to the customer and not store customer data. Information required to authenticate customers shall not be kept longer than is required to complete the authentication transaction and be implemented as to not adversely impact established service levels or existing performance standards (See Service Level Requirements – Identity Proofing Service Provider Requirements) for additional performance and availability requirements.

State Systems Integration Services

The Contractor will provide those services designed to conduct a full-systems-lifecycle integration project between State identified systems in the pilot and the Identify Proofing Service Provider(s) and Two Factor Authentication (2FA) Services to deliver a complete solution inclusive of the:

- Verification of State Requirements, and if necessary elaboration of these requirements in such a manner as to fully implement in production the commercial use of the services;
- Development of Functional and Technical Designs for the State Enterprise (i.e., a fully implemented Enterprise capability) as well as initial Agency system(s) participating in the Pilot project described later in this Supplement;
- Completion of implementation and integrations required to incorporate the Identity Proofing and 2FA functions into State Agency systems included in the Pilot, and for additional State Agency systems upon State written request under an amendment or Interval Development Agreement following the successful completion of the Pilot project;
- Completion of all Unit, Service Integration and System Tests required to demonstrate that the system as implemented, end-to-end, comply with the State's requirements in their totality;
- Completion of all deliverables pertinent to this section as identified later in this Supplement; and
- Completion of all System Performance and Reliability Tests as required to demonstrate that the system as implemented, end-to-end, complies with the State's Service Level Agreements contained later in this Supplement.

Two-Factor Authentication (2FA) Services

The Contractor is responsible for the specification, design, installation and configuration of a Third Party Two-Factor Authentication (2FA) service that includes Token Origination Services(e.g., the creation of a Token, either one-time, physical, device, or Fob based), Token Authentication Services (e.g., validation of the authenticity of a user provided Token) and Token Management Services (e.g., cancellation, replacement or device based registrations) that will be used in concert with Multi-Factor Identity Proofing Services, Integration with a State System and a user transaction to validate the authentication of authorized users within the State (or a State system's) policy management capability.

The two-factor authentication solution will be designed and implemented to require a user to provide two unique factors: something they know, like a password or PIN, and something they possess like an authenticator, a hardware or software token with a code that changes randomly every sixty seconds. This two-factor authentication must ensure that it is far more difficult for an unauthorized or illegitimate party to gain access to State system authentication credentials. The State requires a solution based on the practicalities of supporting the general public that have a variety of capabilities including mobile based devices, Physical or Fob based, emerging biometric based (e.g., fingerprint, voice and IR imaging based) as well as voice response unit (VRU) based. The proposed solution should support all methods mentioned above to provide the State as much flexibility as possible to balance the practicalities, distribution and economics of this second factor with the relative risk profile of the interaction between a State system and a system user (e.g., Citizen, Business, Vendor, State Worker or Privileged State Worker) as appropriate.

In general, these Services must be highly available, and provide fully redundant and fully diverse network access and support the State's multi-Agency, multi-system environment as well as emerging cloud-based offerings that the State utilizes for Enterprise systems and services.

Access Logging and Real-Time Fraud Analysis Services

The Contractor is responsible for the specification, design, installation and configuration, and production deployment of a data analytics product or cloud service, which analyzes data for patterns that might reveal an organized attempt to defraud the State via Identity Fraud, or compromised Identities. The State requires a fraud analytics solution which allows staff to both be alerted programmatically as well as to query an aggregate dataset that is populated from Agency data sources (with existing law and privacy conventions) as well as those provided by the Multi-Factor Service Provider(s), 2 Factor Authentication Provider(s) and other State sources of data as provided (e.g., known fraudulent identity lists or "blacklists") stored in the solution to conduct real-time ad hoc analysis. The solution must utilize techniques that allow information to be filtered and sorted in varying levels of detail. The technology must allow end-users to conduct analysis without programming and with no advanced knowledge of the underlying data sources and structures.

This portion of the overall solution is for the procurement, design and implementation of a data analytics product or cloud based service with the following general requirements:

- Verification of Fraud Identification State Requirements, and if necessary elaboration of these requirements in such a manner as to fully implement in production for commercial use the services;
- Development of Functional and Technical Designs for the State Enterprise (i.e., a fully implemented Enterprise capability) as well as initial Agency system(s) participating in the Pilot project described later in this Supplement;
- Completion of implementation and integrations required to incorporate State identified data sources included in the Pilot, and for additional State Agency sources upon State written request under an amendment or Interval Development Agreement following the successful completion of the Pilot project;
- Completion of all Unit, Service Integration and System Tests required to demonstrate that the system as implemented, end-to-end, comply with the State's requirements in their totality;

- Completion of all deliverables identified later in this Supplement; and
- Completion of all System Performance and Reliability Tests as required to demonstrate that the system as implemented, end-to-end, complies with the State's Service Level Agreements contained later in this Supplement.

The solution must provide the functionality and meet the requirements for the general groupings of constituents listed below:

- Citizens and Businesses and filers on the behalf of these entities;
- Employers;
- Internal State Staff and Workers;
- Public Assistance Provider/Retailer; and
- Other Groups identified by the State (e.g., State agencies, boards, commissions, etc.).

The State has made significant investment in a number of enterprise and Agency specific applications. The proposed solution must take into account:

- that investment and leverage State capabilities and functions;
- when the solution meets the technical and functional requirements identified in this RFP; and
- where the solution results in costs savings to the State in cost categories such as software licensing, Service Subscription costs, maintenance, or support.

While the State includes some solution components (as described throughout the RFP), the State is willing to entertain a variety of justifiable solutions to satisfy the full requirements of this RFP. Offerors must not feel restricted in proposing innovative and forward thinking solutions that must still satisfy the RFP requirements.

The Ohio Enterprise Identity and Authentication Services Project must follow the State of Ohio Project Management Requirements contained later in this Supplement. The Deliverables are defined as part of these State requirements.

Additionally, this RFP contains State Security, Privacy and Data Handling requirements in Supplement 2, all of which must be strictly adhered to as part of the response to this RFP and in the course of delivery of Services to the State. Offerors must not take exception to or request to negotiate any items in Supplement 2.

3.0 Enterprise Architecture and Integration Standards and Conventions

3.1 Design, Integration and Scalability Considerations

State Enterprise Service Bus Agency systems and systems architectures have been built over the years with a variety of middleware or service bus architectures. For purposes of this Supplement and general Enterprise use across the State, Offerors shall base their solution on the assumption that SOA, Web Services (in general) and Oracle Enterprise Bus® and IBM/WebSphere® ESB are prominent service bus architectures that will require interoperability and integration to the Enterprise offering and as such are acceptable and preferred unifying technologies for this Enterprise offering. Should an offeror require or propose alternate ESB methods or software, Offerors are to provide the rationale for this selection and notwithstanding this selection ensure that the alternative can integrate fully with established standards (i.e., Oracle and IBM) within the State. In addition, and pertinent to one of the Pilot projects contained within this Supplement (eLicensing) the use of MuleSoft™ ESB within the Salesforce.com platform is currently utilized.

Existing Directory Services the State's directory for general and administrative purposes (e.g., email, productivity and general identity purposes) is Microsoft Active Directory. In addition to system specific identity stores, there are significant concentrations of IBM/Tivoli, LDAP and other common directories.

Existing Cloud Services and Systems the State has based several service offerings and has active development on a number of Cloud Based Services and Systems. Most prominent, and therefore must be a demonstrated factor in the overall solution are VMWare® (State cloud provisioning, orchestration and management); Salesforce.com® (CRM, Licensing Applications and some Revenue Collection); ServiceNow® (enterprise service management, delivery and billing); and Microsoft® Office365 (applications, productivity, email).

Emerging Cloud Services the State continuously reviews the merits and use of a variety of Cloud based system and service offerings. Offerors should indicate what parties and mechanisms their solution supports (generically) standard 2 factor authentication using open TOTP standards or extensible to proprietary solutions such as Amazon AWS MFA, Microsoft Azure MFA, Google Authenticator, OpenID (e.g., Google, Paypal) or other ICAM or Federal Bridge/FICOM Certified Providers of Token Management and Authentication Services.

Mobile Interoperability and Emerging Biometrics the State acknowledges the increasing importance of mobile devices across the State and by our constituents. Many of these devices maintain provisions for two-factor biometric based authentication such as Apple iDevice based TouchID, Android based Fingerprint, Microsoft FIDO and other emerging standards. Offerors should indicate who and through what devices and mechanisms that their solution supports 2 factor authentication using mobile devices and computing platforms that offer similar biometric (fingerprint, voice and IR image) based factors.

General Enterprise User Counts and Sizing Considerations Contractors are to design and implement the proposed system to directly support the sizing required in the Agency pilots specified elsewhere in this Supplement, but be capable of from an architectural/sizing perspective to be scalable to address the following **approximate** populations:

Measure / Sizing Points	Approximate Count
Ohio Population (All Citizens)	11.6M
Ohio Households	4.5M
Ohio Registered Businesses	7.5M
State of **Ohio Worker** Population	54,000
Extended State Workforce (Contracted Services, Service Providers and Other Personnel) that may require some form of the services contained in this RFP	15,000 (estimate)
State of Ohio State, County and Local Government Worker Population	738,000
Agency Systems Inventory (Total)	2,600
Agency Systems that Maintain some form of sensitive personal or financial information	1,500
State Systems with immediate needs (high volume, high financial value, high public impact)	36
Pilot State Systems Contained within the Initial Scope of this RFP	3

Specific sizing considerations for Pilot State systems are contained later in this Supplement.

As part of the work, the Contractor will develop the following deliverable(s):

Deliverable 001. Enterprise Identity Master Design Document inclusive of:

- Use of State Standard Enterprise Service Bus Architectures and Elements
- Use of State Enterprise Active Directories and Agency/Application Specific Identity Stores
- Federation and Trust Frameworks
- Use of 3rd Party Cloud Software Directories and Federation Method(s)
- Mobile Interoperability Standards
- Sizing and Scalability Requirements and Considerations

3.2 Technical Standards Requirements

The proposed system and service must comply with the following technical standards and requirements:

- Provide a secure channel for real time data transmission between State and the proposed Service Provider(s).
- Use standards-based web services technology, including SOAP, WS-Security, and XML.
- Be in compliance with all Federal standards and guidelines, including:
  - OMB M 04-04: E-Authentication Guidance for Federal Agencies;
  - NIST SP 800-63: Identity Proofing at Assurance Level 3;
  - FIPS 140-2: Encryption for backend data verification calls;
  - NIST SP 800-30: Risk Management Guide for Information Technology Systems; and
  - NIST SP 800-95: Secure Web Services for backend data verification calls.
- Provide data exchange in compliance with NIST encryption standards.
- The software solution shall be Section 508 compliant, see http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/guide-to-the-section-508-standards, for applicable definitions, standards, etc.
- The Software solution shall be able to take as input, a financial account number and verify that the identity information provided by the customer (claimant) is consistent with the data associated with the financial account number through a record check with the applicable institution or credit bureau. The minimum data elements verified shall include, but are not limited to: 1) Name, 2) Date of Birth, and 3) Address provided by the customer (claimant).
- Additionally, as part of the Offeror response, the types of financial account numbers the software solution is capable of verifying and the minimum identity data elements (e.g., Name, DoB, Address) required must be provided as well as a description of any limitations related to the scope of the verification.
- The Offeror will describe how tolerance levels are applied to the identity data elements (e.g., married vs. single surnames, extra spaces, variance in address – street vs. avenue, etc.).

As part of the work, the Contractor will develop the following deliverable(s):

Deliverable 002. Enterprise Identity Interoperability Standards inclusive of:

- Trust and Encryption Levels
- Mandatory Data Elements and Agency Specific Options
- Maintaining Public Privacy
- Private Data Handling and Disposal Standards
- Data Physicalization and Duplication Standards
- State Tolerance Considerations

3.3 Enterprise Directory Support

LDAP v3 inclusive of Application Program Interface (API) calls:

- IBM/Tivoli Single Sign On;
- Microsoft Active Directory (all OEM Supported Versions);
- External radius server;
- Two factor authentication;
- Novell IDM v3.5 or higher;
- User ID and Passwords; and

- State Provided Access control lists and files.

The System must support the following two factor authentication (2FA) methods:

- Biometrics;
- Directories;
- Smart cards;
- Tokens;
- PKI and Certificates;
- Voice recognition; and
- Shared secrets.

As part of the work, the Contractor will develop the following deliverable(s):

Deliverable 003. Enterprise Identity Directory Support Capabilities inclusive of:

- Use of Existing Directory Stores
- Master Directory Federation Strategy
- Integration Methods
- Legacy Directory Retirement/Replacement Strategy and Checklist
- Published APIs and Integration Method(s)
- Identity Provisioning
- Audit and Logging Capabilities

3.4 APIs, Workflow and State Development Tool Support

Offerors must identify, select and propose a Solution that meets the following requirements at a minimum. Should an Offeror's solution exceed the standards, Offerors should highlight the perceived merits, rationale and (if applicable) limitations of the proposed solution:

- The solution must provide a clear development path for integrating web-based applications for reverse proxy portal integration or equivalent functionality.
- The solution must provide a software development kit (SDK) for extensions surrounding workflow, custom provisioning, and triggers.
- The solution must support the use of open source or well supported leading industry development tools, subject to State approval as well as support for integration with State applications and services, which support authentication methods that are LDAP and Active Directory capable.
- The solution must support both Java based development activities using J2EE and current supported JDK version and Microsoft Windows specific development using .NET based methods. Offerors are to indicate any additional methods for Java and Windows specific development activities that the State may utilize using the proposed solution.

3.5 Directory Services and Provisioning

The system must support custom attributes of the offeror's LDAP or Active Directory.

The solution should provision and de-provision identities in non-LDAP or Active Directory targets.

The solution shall not allow anonymous access to the production LDAP or Active Directory.

The solution must provide the ability to support self-registration and user originated application requests with an approval queue for application administrators.

Solution must allow for self-requests for automated password reset where appropriate.

Solution must support multiple workflow paths, depending on the type of user such as, but not limited to state employee, identified citizen, customized web experiences, etc.

Solution must support the development of customized workflows.

Solution must support notification workflow capabilities.

The system should support workflow approvals from secure authorized mobile devices.

3.6 Audit and Logging Requirements

System must provide full and configurable auditing capabilities, including the creation/deleting of users, password resets, role/privilege assignment, token assignments, 2 factor method(s) and devices, etc.

System must provide full auditing of access to applications, access to resources, and access to individual users accounts.

All auditing logs must be reviewable by state security administrators and security policy staff using access to system logs and via the Programmatic Fraud Detection system(s) proposed by the Offeror.

The system must support real-time replication or integration of audit logs to the State's Security Information and Event Management (SIEM) solution based upon an industry leading Security Intelligence Platform which will be disclosed by the State upon award, for audit reporting, alerting and management by State Security and Privacy Personnel.

The system must be configurable for auditing events and be extensible to support situational analysis of events and breeches (active and retrospectively) as to support incorporation of new rules, methods, tools and techniques to further enhance the State's overall security posture in the future.

All system activity must be attributed and logged to a single, unique system user, identifiable by individual persons.

3.7 Account Management and Linking Requirements

3.7.1 General Application Use and Integration Requirements

The solution shall be capable of linking multiple customer third party credentials to a single State identifier for the customer. If an Offeror believes that this requirement conflicts with other requirements, please describe its implications.

The solution shall be capable of presenting a single State identifier to a specific relying party, regardless of which third party provider the customer successfully authenticated with. If an Offeror believes that this requirement conflicts with other requirements, please describe its implications.

The solution shall present customers with an option to register third party credentials with their State unique identifier. If an Offeror believes that this requirement conflicts with other requirements, please describe its implications.

The solution shall allow customers to link multiple third party credentials together into a single State identifier to access the same customer account at a relying party.

The solution shall allow customers to unlink their third party credentials from their State identifier. If an Offeror believes that this requirement conflicts with other requirements, please describe its implications.

The solution shall allow customers to decline registration of multiple third party credentials with the State. If an Offeror believes that this requirement conflicts with other requirements, please describe its implications.

The solution shall allow customer to un-register their third party credentials with the State and destroy the State identifier. If an Offeror believes that this requirement conflicts with other requirements, please describe its implications.

3.7.2 Agency Application Use and Integration Requirements

Application authentication and authorization must be by individual user. User account information must be stored securely in a database. Users may belong to multiple groups and roles.

The application will enforce the DAS/OIT standards or specific Agency system requirements, whichever are more restrictive for individual passwords for allowable characters, length and expiration period.

The application must follow the DAS/OIT standards or specific Agency system requirements, whichever is more restrictive to lock out users after invalid login attempts.

The application must provide the system administrators with the capabilities to define different roles with different privileges.

The application will provide the system administrators with the capabilities to create groups whose members can be either role-based or individual login account names.

Deliverable 004. Enterprise Application Use Standards inclusive of:

- Use of Existing Directory Stores
- Master Identity Federation Strategy
- Integration Methods
- Published APIs and Integration Method(s)
- Audit and Logging Capabilities

3.8 User, Portal and Certificate Administration Requirements

3.8.1 User Administration and Provisioning Requirements

The proposed Solution will allow the ability for local State administrators with rights to add, delete, disable, and modify user for their Agency.

The proposed Solution will allow users to centrally provision and de-provision; meaning accounts are enabled or disabled Statewide from the Contractor's identity vault.

User and account provisioning and de-provisioning within the State's Identity Domain (AD) will continue unchanged as a result of this RFP.

The proposed Solution must support one identity per entity, with users possessing rights to multiple applications and resources. Users should have a single password with other factors such as PINS, tokens, biometrics, etc., as required. The same entity may have more than one identity depending on context, such as a State of Ohio employee who also logs in as a Citizen or as a Business.

The system must provide central administration for manually manipulating identities, including password reset, user creation, granting roles/privileges, etc. and log all of these actions for auditing purposes.

The system must have a single web and web service interface that allows for the management and administration of identity management systems.

The system must have the ability to enforce password policies including:

- Expiration of passwords;
- Challenge/response capabilities for forgotten passwords; and
- Password strength policies.

The system shall use preset values to reduce the time to create, provision, suspend and terminate an account correctly.

The solution must support the ability to assign security attributes based on the user's context.

3.8.2 Single Sign-On Support

The proposed Solution must include support for a reverse proxy access control or equivalent functionality, authenticating the user for all applications for which the user has been granted access.

The proposed Solution must provide a migration path for the existing Single Sign-On (SSO) solution should the State determine that alternative methods and tools be required to augment or replace existing methods.

The solution must support integrated workflows to enable automated provisioning and de-provisioning based on feeds from authoritative sources.

Solution must support delegated administration for applications accessible through the Service Provider's portal.

3.8.3 Certificate and Encryption Key Management

System must provide administration tools for managing certificates and encryption keys needed to support the system where appropriate and provide for limited and secure access to key stores, consistent with constraints of applicable Federal and State law.

System must support the use of the State's VPN and two-factor authentication for any permitted remote Administrative access to the State's internal resources.

3.8.4 Solution Administration Portal: Users, Relying Parties and State

On user login, the Solution will support the ability to present a custom web portal to the user that shows application links to which the user has rights of access. This Portal:

- must be designed for multiple interfaces (desktop/laptop, tablet, phone, mobile devices);
- must have the ability to allow/disallow users to modify the user's portal home page;
- must have user's self-care capabilities, such as, but not limited to, user's changing passwords, challenge response and personal information;
- must provide for System Administrators to post communications/notifications; and
- must allow dynamic additions and deletions of applications to the portal without impacting other applications.

Administration of the Solution Portal:

- must provide configurable attributes by location, object classification, applications and other attributes;
- must have a uniform interface across the Service Provider's solution for State Administrators;
- must provide a web-based user interface for administrative tasks. Please describe the administrative tasks supported with and without a web-based user interface;
- must provide role-based access control capabilities for administrators and administrative tasks;
- must enforce separation of duty (SoD) and operate on least privilege policy for administrator access;

- must provide a web-based user interface to manage third party providers; and
- must provide a web-based user interface to manage relying parties.

4.0 Multi-Factor Definitive Identity Proofing

The State has more than 2,600 applications and services. These are accessed by a variety of constituents including “end-users” (e.g., members of the public accessing State systems, State Workers (e.g., processor of transactions, viewer of data) and Privileged State Worker (e.g., processor of exceptions, “root” or “administrative” level access to technical platforms and underlying data stores). In general, the Offeror proposed solution must support all Proofing requirements of the Enterprise in the context of these user constituent groups, which are summarized as:

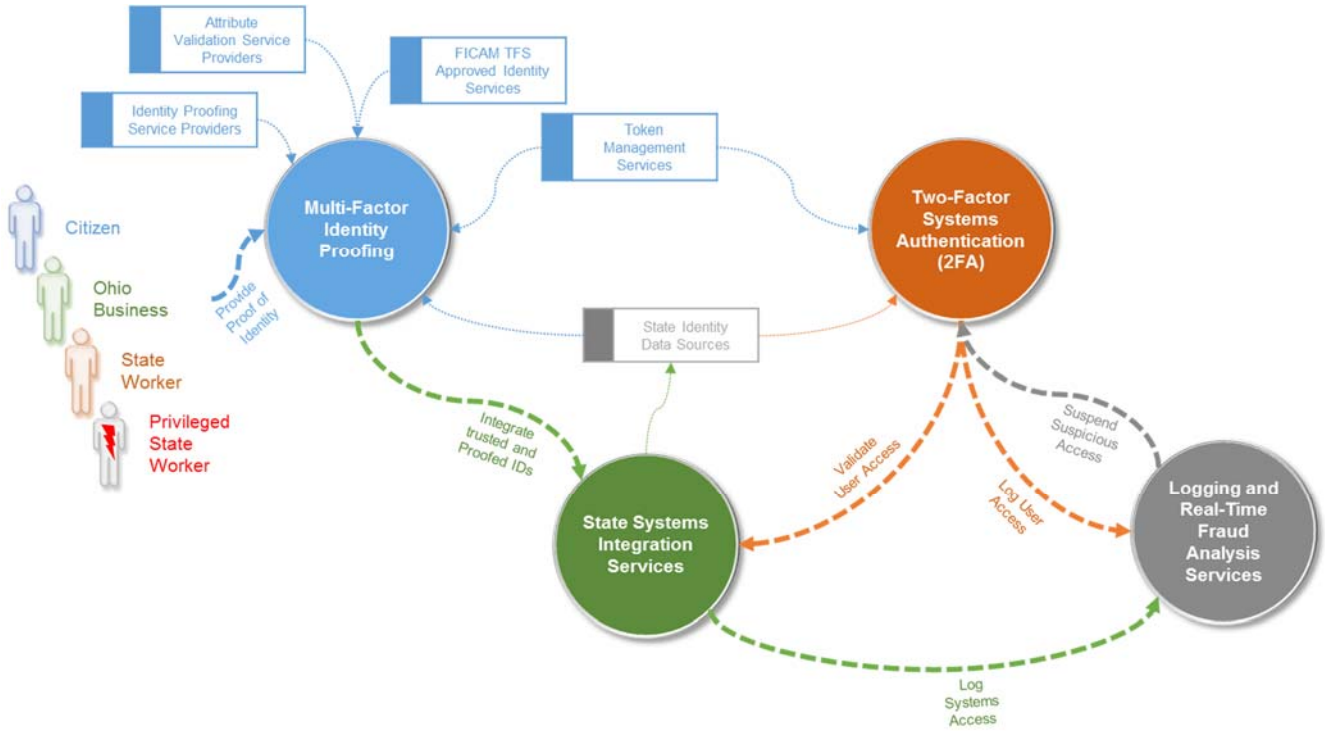
- Citizens and the General Public;
- Emerging, Small, Medium and Large Enterprise Businesses;
- State Workers that access systems to perform their job duties; and
- Privileged State Workers that maintain elevated security privileges to support, operate and maintain these systems.

As part of this area, the Offeror will propose, and subsequently as Contractor design, implement and deploy, an overall solution that:

- Allows the Proofing of any identity (State or Public) via a variety of means and data sources to definitively establish the validity and authenticity of an Identity prior to onward access or use by the State;
- Includes 3rd Party Verification Sources or Service Providers in consideration of Identity Proofing for Public User Identities (i.e., non-State workers) including citizens (as individuals), primary care givers (e.g., entities authorized to transact on behalf of a citizen such as elderly, disabled, minors and other such groups);
- Integrates and includes existing State Identity Sources such as State employee databases, State worker databases, Agents of the State, State data sources such as driver’s license, vehicle titling, business registration, taxation databases and the like, as well as other databases that the State may provide that comprise a federated “known good” or “known bad” compendium of identities;
- Supports the bi-directional integration or federation with FICAM TFS approved identity sources, which initially will be used as a proofing source by the State, but should be architecturally compliant with and facilitate the State’s participation in, and in the future if necessary and only at the direction of the State, certification as a Trusted FICAM identity source;
- Support the State’s validation of attributes based on citizen or business submitted forms (paper, electronic or otherwise) to ensure the authenticity of identities and help prevent the filing of forms, taxes, certifications and other artifacts by non-authorized or fraudulent parties; and
- Given a proven identity, and dependent on State authentication requirements, initiate provisioning workstreams to distribute or authorize any physical or device based tokens as appropriate in the context of a State system and the identity authentication requirements of that system.

Conceptually, these requirements can be viewed in the context of this overall Supplement as follows:

Conceptual View of Identity Proofing Scope
(within overall solution context)



4.1 General Requirements

The Offeror proposed Solution will enable user identity authentication, establishment, management and federation and support access management of State of Ohio systems and services through integration of State System(s) to Service Provider(s) who provide these services.

The Offeror will propose and provide an adoption solution that encourages adoption and use for initial Pilot applications and onward to State identified Agency systems based on State priorities and other factors.

The Solution will provide an internal identity store that provides support for federation for use for both internal and external State applications. The solution will support separate protected Directory (i.e., Active Directory or LDAP) compatible sources for internal only access and external public access. It is not the intent of the State to use an external identity store (LDAP or Active Directory) for internal system user access when users are connecting from within the State network. The State conceptually views this solution as an internal identity store that provides support for federation for use for both internal and external applications.

The Solution must support federation between the trusted State systems and Trusted External Parties, particularly FICAM TFS Approved Identity Sources and National Strategy for Trusted Identities in Cyber Space.

The Solution shall accept FICAM-approved third party credentials including PKI.

The Solution shall accept PIV and PIV-I credentials for both customer authentication and administrator authentication. In this situation, FCCX shall support ability to directly validate PKI credentials including revocation checking, trust path validation and policy validation.

The Solution shall accept all FICAM-approved third party credentials at NIST LOA 1 through 4, as defined in NIST SP 800-63.

The Solution shall proxy successful authentication assertions from FICAM approved third party providers to requesting customers.

The Solution shall proxy authentication assertions, including third party provided attributes to the relying party via the customer's browser.

The Solution shall direct the customer to the relying party resource after successful authentication at the third party provider.

The Solution shall communicate with FICAM-approved third party providers using standards, profiles, and schemes approved by FICAM as of the release of this solicitation.

The Solution shall provide the ability to implement last mile integration with agency applications using SAML 2.0 and optionally using a REST/JSON over a secure channel and shall provide first mile integration with credential providers using FICAM approved protocols and approaches.

The Solution shall be capable of displaying a list of acceptable third party providers at or above the LOA required by the integrated relying party via a web graphical customer interface.

The Solution shall be capable of storing the configuration data needed for each third party provider.

The Solution shall not store identities, except for FCCX unique identifier when the customer uses account-linking functionality.

The Solution shall not provide access control services for relying parties.

The Solution shall provide the ability to display branding as defined by the government on user interfaces, including 'splash pages' that could be added during the third party provider selection or authentication request processes.

The Solution shall provide security controls to detect, prevent, and mitigate attacks against FCCX and the user. Please describe the controls and potential attacks (e.g., assertion replay attacks).

The Solution shall have the ability to provide attributes from a third party provider within the authentication assertions to relying parties.

Deliverable 005. Identity Validation Standards inclusive of:

- Standard Reference Architecture
- Documented Integration Methods and Standards
- Inclusion of Additional / Future Validation Services
- Agency Integration Handbook
- State Procurement Standards for inclusion in Future State Systems Specifications

4.2 Privacy Requirements

The Identity Proofing Service shall prevent third party providers' visibility into customer transactions with relying parties.

Identity Proofing Service shall prevent third party providers' visibility into customer transactions with other third party providers.

Identity Proofing Service shall prevent relying parties' visibility into customer transactions with third party providers.

Identity Proofing Service shall prevent relying parties' visibility into customer transactions with other relying parties.

Identity Proofing Service shall not be able to decrypt/access authentication requests from the relying party or assertions from the third party providers. The required flow is analogous to how the United States Postal Service delivers mail envelopes to its customers without opening the envelopes. Offerors are to indicate how this may impact use of standard protocols or the proposed architecture.

Identity Proofing Service shall not store Personally Identifiable Information (PII) of any kind.

Identity Proofing Service shall not have visibility into customer identity data unless required by law.

4.3 FICAM Compatibility and Evolution Currency

The System shall support all currently approved FICAM Protocol Profiles for browser based SSO. (OpenID 2.0 and SAML 2.0 required; IMI 1.0 support is optional).

The Offeror shall provide a detailed plan for supporting any newly approved or future FICAM Protocol profiles within 90 days of final approval by the ICAMSC. The implementation of any such plan must be approved by the State and implemented by the Contractor under an approved statement of work.

The solution must be capable of supporting all FICAM Adopted Trust Framework Provider Approved Credential Providers.

The solution must be capable of supporting PIV (for Government-to-Government use cases) and PIV-I Authentication. This support must include Trust Path Discovery and Trust Path Validation functionality.

4.4 Protocol Standards and Support

If the solution implements a SAML 2.0 Attribute Query/Response mechanism, it shall support the FICAM SAML 2.0 Identifier and Protocol Profiles for BAE v2.0 and the associated FICAM SAML 2.0 Metadata Profile for BAE v2.0.

The Solution shall, at a minimum, support the following protocols and assertion formats for communication between itself and the relying party Agency application: Protocols: HTTP(S), SAML 2.0 and Assertion Formats: SAML 2.0, XML, JSON.

The Solution must support full and policy or filtered interfaces with other directories, including at least Tivioli, Active Directory (AD), eDirectory and Lightweight Directory Access Protocol (LDAP) or equivalent Active Directory functionality.

The Solution must provide support for a minimum of 256-bit TLS encryption for transport and must be configured to communicate using TLS/ SSL or other appropriate forms of encryption.

The Solution must provide encryption for all data at rest at level no less strong than that offered by Advanced Encryption Standard (AES)-256.

The Solution must support strong one-way encryption (hashed) of passwords.

The Solution must support Public key Infrastructure (PKI) where appropriate.

The Solution shall support standard attribute sharing protocols including but not limited to the following:

- SAML 2.0 (Mandatory); and
- OpenID 2.0 (Desirable).

The solution shall support the following for communications between itself and the relying party application:

- ICAM SAML 2.0 Web Browser SSO Profile; and
- ICAM OpenID 2.0 Profile (Desirable).

The solution shall support the following protocols between the State and the PKI Certificate Authority but it is not limited to these:

- OCSP over HTTP;
- CRL over LDAP and HTTP; and

- SCVP over HTTP.

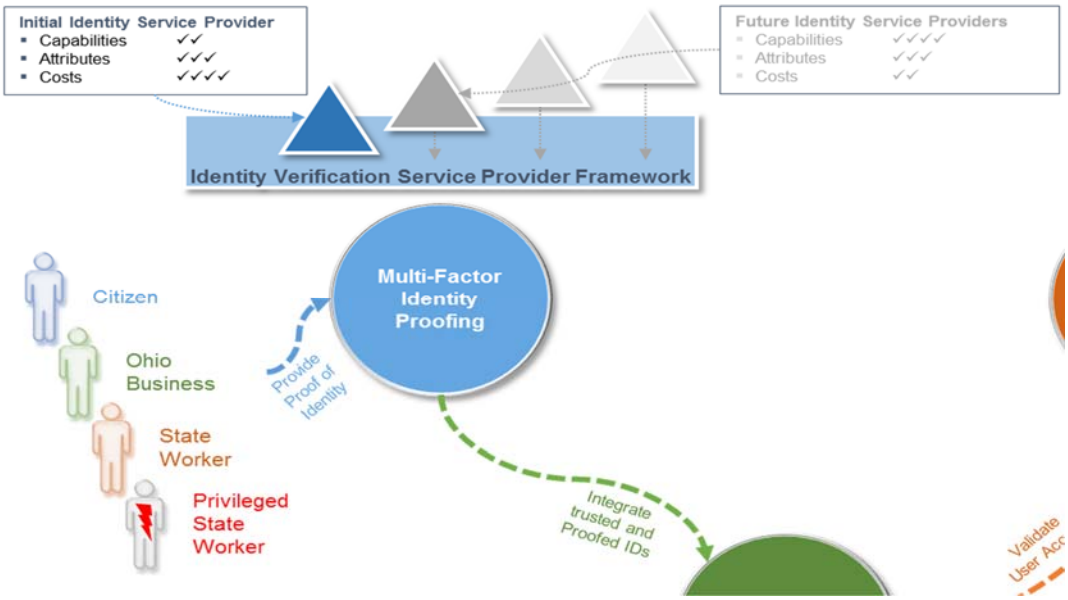
FCCX shall support HTTP/S protocols between the State and a State Customer (e.g., Citizen, Business, Agency, etc.) but not be limited to HTTP/S exclusively. Additionally the solution shall have the ability to integrate with additional protocols within 60 days of State request.

4.5 Service Provider Diversity and Extensibility Requirements

The Offeror must include **at least one** Identity Service Provider (IDSP) that meets the FICAM/Federal Bridge approved identity requirements, and in the course of delivering the work contained in this Supplement ensure that all requirements are specified, designed and implemented in support of State requirements.

Conceptually, this capability can be viewed (in the partial context of the overall solution) as:

Identity and Attribute Verification Framework Architecture



From a practical, architectural, risk management, technical, attribute, capability and cost perspective, the State requires that the proposed architecture and design be implemented to support more than one IDSP at a future date. So that in the future at the State's sole discretion the State may either augment or replace the initial IDSP contracted under this RFP with additional IDSPs. Therefore the proposed solution must adhere to established standards and be developed in a manner as to support multiple concurrent IDSPs to allow the State supplier diversity and ensure the system is extensible as to not preclude replacement or augmentation of the initial IDSP at a future date.

4.6 Attribute Proofing Requirements

The State processes a variety of on-line, paper based, and "walk-in" transactions with its constituents. As a large number of these transactions (electronic or otherwise) require some form of validation of data that may or may not be online identity based, the Offeror will propose a solution inclusive of the Identity Proofing Solution Provider that allows the State to construct authentication frameworks between a State system or business process to validate certain attributes of a transaction and make a determination as to the authenticity of the requested (or requestor) of the transaction before proceeding. As a representative use case to illustrate the general requirement: a tax payer completes a paper form and mails the return to the State, prior to processing any refund or disbursement, the State Agency may require validation of the identity represented on the form in question prior to processing the transaction and releasing the return refund. Offerors are to note, and factor in their response, considerations

pertaining to personal, health, financial and other data types that the State may require in validating transactions via the attributes pertinent and as provided by citizens and businesses in the State.

- The solution shall be capable of identifying the third party provider within an authentication assertion.
- The solution shall be able to locate an attribute provider that has additional attributes for an identity or entity based on Agency determined identifying and validation attributes.
- The solution shall be able to add and manipulate attributes to the assertions received from a third party provider prior to sending to the relying party. For example, the solution may modify the unique identifier used by the third party provider (does not include attribute values).
- The solution shall be able to map or rename the attributes in the assertion received from the third party provider to support a consistent naming of common attributes (e.g., email address) to all relying parties regardless of how the third party provider chooses to name and convey/communicate their attributes (does not include attribute values).

Deliverable 006. Enterprise Attribute Proofing Standards and Design Document inclusive of:

- File Based Method(s)
- Online Based Methods
- Error Detection / Correction
- Positive / Negative Response Handling
- Performance and Scalability Considerations
- Operational Run Book for Batch / High Volume Operations
- Maintaining Public Privacy

4.7 Auditing and Reporting Requirements

4.7.1 Auditing Requirements

The solution shall log and make available by reports and the Enterprise Logging, Audit and Fraud Detection capabilities under Section 8.0 of this Supplement all activities related to:

- the customer authentication request;
- the third party provider authentication results;
- the assertion to a relying party;
- the relying party attribute request;
- the attribute provider communication;
- the customer account linking of third party providers;
- changes in third party providers;
- notification date and time stamps;
- onboarding and off-boarding of third party providers;
- onboarding and off-boarding of relying parties; and
- administrative functions.

In addition to the above as a set of Administrative and Technical requirements, the solution shall:

- allow administrators to view audit logs in a web user interface;

- store audit logs online for a minimum of one year;
- store audit logs offline for a minimum of seven years and six months and provide programmatic data archive and purge capabilities for the management of all logs;
- support near real-time analysis of events (see Section 8.0 of this Supplement);
- store all logs from all redundant instances of the Service in a centralized database;
- log activities related to notice and opt-in; and
- have the ability to define and configure logging activities including types of data and maximum storage time.

4.7.2 Reporting Requirements

The solution shall be capable of producing audit reports via either Offeror provided web reporting tools or State access via State standard reporting tools (IBM/Cognos).

The solution shall have the capability to generate ad-hoc business reports that can support internal State invoicing needs including Agency use/consumption, application level access and proration of the entire Service based on Agency actual use/consumption.

The solution shall be capable of producing a web accessible report dashboard with the ability to export the report in CSV, PDF and Excel as appropriate to the content of the report.

The solution shall not display or maintain sensitive personal of financial information in logs or administrative messages.

The solution shall be capable of generating a report for a specific customer pseudonymous identifier when the identifier is required to support other functionality.

4.8 Compliance Requirements

The solution shall be designed and implemented to become FISMA certified at moderate security category and plan to attain certification at the State's direction and nothing provided by the Offeror shall be designed, implemented or deployed as to preclude or confound such certification.

The solution shall be designed and implemented to allow the State to pursue FedRAMP certification in the future and in the interim comply with or exceed current FedRAMP requirements for a moderate system.

4.9 General State Integration Requirements

System components must be deployable in tiers or (if appropriate) scalable modules, such as putting the reverse proxy server, the portal server, and identity stores on separate physical servers, limiting the exposure of secure resources. The actual tiers should depend on best practices for the Offeror proposed solutions and solution elements.

The solution must provide a user login through a web portal for application access or enable integration with an existing portal environment through open standards.

The solution shall:

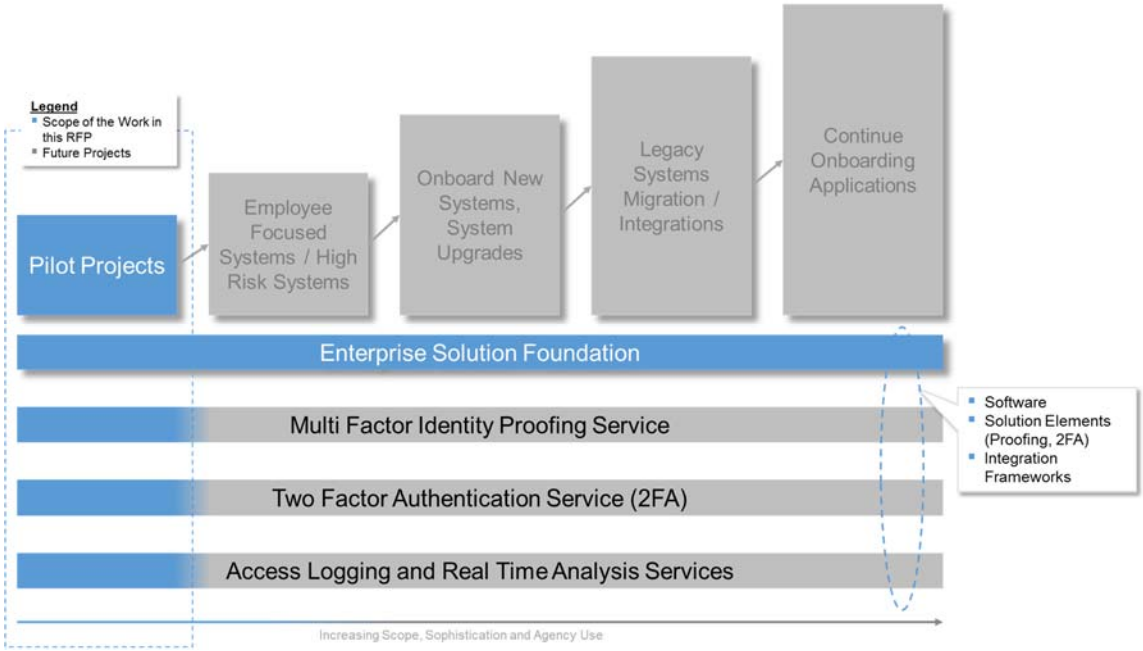
- be designed and implemented to function as a relying party to the third party providers;
- be designed and implemented to function as a third party provider to the relying parties;
- ensure the authentication assertions are routed to the requesting relying party;
- not make authorization decisions for the relying party. If an Offeror believes that this requirement conflicts with other requirements, please describe its implications;

- not manage sessions for the third party providers or relying parties. If an Offeror believes that this requirement conflicts with other requirements, please describe its implications;
- interface with the relying party to provide credential verification options, assertions and attribute requests;
- interface with customers to allow the linking of third party credentials. If an Offeror believes that this requirement conflicts with other requirements, please describe its implications;
- have the ability to interface with FICAM third party providers that can provide assurance level escalation services to relying party web applications. Note that FCCX is not required to make the authorization decision for assurance level escalation; and
- interface with attribute providers to retrieve additional attributes about a customer.

5.0 State Systems Integration Services

The State has identified a need across the Enterprise for the services and capabilities contained within this RFP. The following is a conceptual overview of the organization of the services required by this RFP in total, and initially in a live Pilot and onwards implementation and adoption by State Agencies based on State established priorities and identified opportunities:

General Scope of RFP, Pilot Agencies and Post Pilot Implementation Approach



The implementation approach is summarized as follows:

1. Implement a meaningful set of **Pilot Agencies** to demonstrate the overall efficacy of the system as it relates to an emerging class of State applications (e.g., Cloud Based Enterprise offering) and an existing high profile system that requires legacy integration and high volume requirements (e.g., Cabinet Agency with high relative risk parameters).
2. Identify a solution foundation that allows for the integration or use of **multiple Identity Proofing Service Providers** and implement at least one Service Provider suitable to the scope of the Pilot Agencies, but extensible from an architecture to additional State Agency systems post-Pilot and (if required by the State) extensible to additional Service Providers in the future.

3. Identify a solution foundation that allows for the integration or use of **multiple Two-Factor Authentication (2FA) Service Providers** and implement at least one Service Provider suitable to the scope of the Pilot Agencies, but extensible from an architecture to additional State Agency systems post-Pilot and (if required by the State) extensible to additional Service Providers in the future.

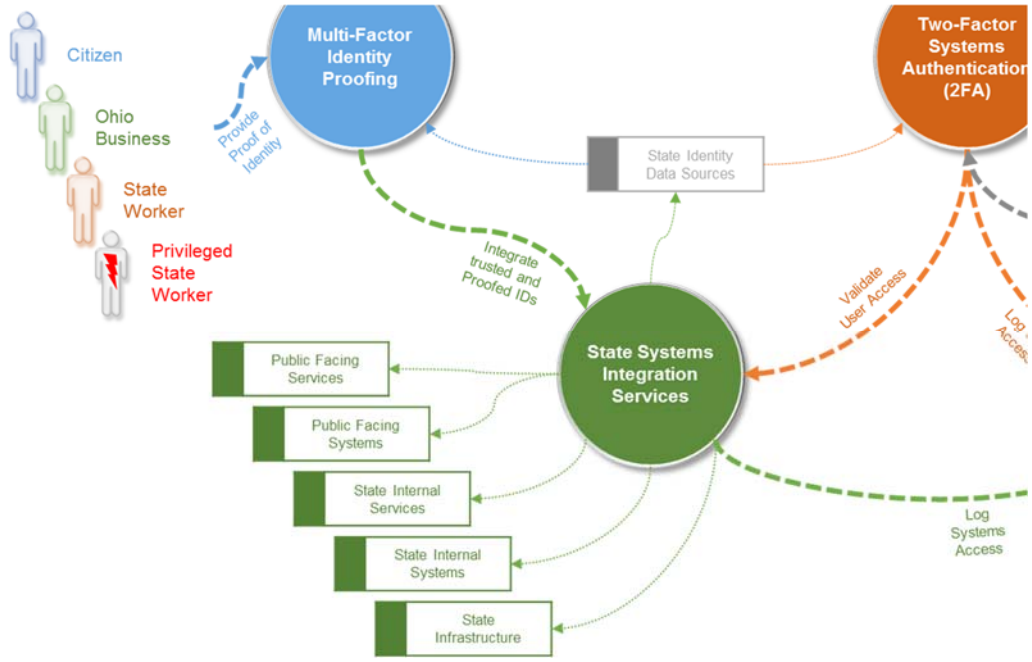
4. Establish Post-Pilot development standards, reference architecture, software and service elements suitable to the State Enterprise to accommodate and incorporate new systems, legacy systems and systems identified by the State as high-risk as a vendor neutral implementation methodology that could be included in State policies, system specifications and procurements in the future as required.

The Systems Integration Service will design, implement and deploy at a minimum the integration of the following:

- a Proven Identity arising from the Multi Factor Definitive Identity Proofing Service as contained in Section 4.0 of this Supplement;
- a Pilot State System as defined inclusive of all requirements of Section 5.0 of this Supplement;
- the Two-Factor Authentication Service as defined under Section 7.0 of this Supplement; and
- Additionally, as part of the work, the Contractor will implement Enterprise Logging, Audit and Fraud Detection capabilities as contained in Section 8.0 of this Supplement in support of the requirements of the defined Pilot Agencies.

Conceptually, this work can be viewed as:

Conceptual Organization of State Systems Integration Services
(within the overall Context of this RFP, selected view)



5.1 State, Government and Commercial Identity Data Sources

The State maintains a variety of definitive data sources pertinent to Citizens, Businesses, Vendors, Employees and other data sets that can be used to augment or supersede those commonly available on the marketplace. As illustrative examples of types of data sources that may be used on an Enterprise level:

Active Employee Data contained in the State's ERP system (known as OAKS) which is based on Oracle® PeopleSoft technology inclusive of general details such as "active", "on-leave", "on temporary assignment", "suspended" and "terminated" and other elements and onward replicated to the State's Microsoft Active Directory™.

Active Vendor Data also contained in the State's ERP system used for a variety of State interactions with State vendors inclusive of status, identifying information, payment/banking information, invoice and purchase order history and other elements.

Ohio Business Data contained in a variety of Agency and Elected Official systems business registration, filing, payments, delinquencies and other factors and elements.

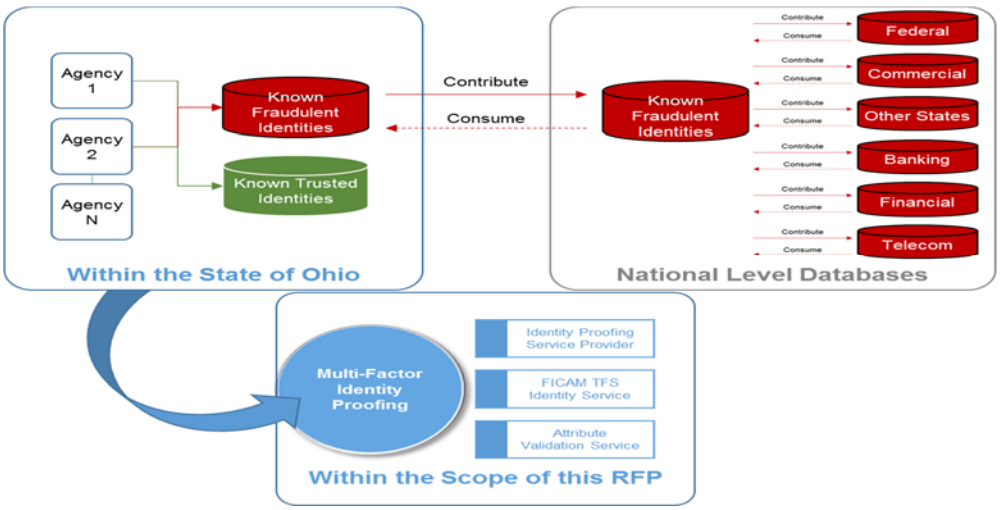
General Citizen Data contained in a variety of Agency systems including data such as driver's licenses, vehicle titling and registration information.

In addition, the State also maintains a variety of lists of "known or compromised" user accounts, identifying details, fraudulent identities and other lists of individuals and entities who, for reasons known to the State shall be prevented from attempting to access State systems and services with compromised credentials - collectively, and conceptually referred to as a "**Black List**".

In addition to the above, there are existing and **emerging national fraud databases** available to the Federal Government and financial/banking institutions that are designed to facilitate the sharing of known fraudulent identities (persons) and entities (businesses) between industries and contributing members of such databases. Fundamentally, these databases are designed to increase the probability of cross-industry, cross border fraud detection through incorporation of multi-member data - generally addresses, social security numbers, driver's licenses and phone numbers of known fraudulent identities.

Conceptually this architecture is represented as:

Context: Integration of State, Federal and External Sources of Fraudulent Identities



The Offeror, as part of the overall provision, design, implementation and deployment of the solution will:

- provide for inclusion of the aforementioned State provided data and other State data types and elements;
- specify open formats and standards for State Agencies to contribute to a central State registry of known fraudulent credentials;
- design and implement methods to edit, update and refresh this data from both State internal sources and that data external to the State that is shared at the Federal level as well as through the collaboration of multiple States;
- design and implement methods to both contribute and accept known fraudulent entity data from both State internal sources and that data external to the State that is shared at the Federal level as well as through the collaboration of multiple States;
- provide for State programmatic and secure access methods to add, delete and modify this data without incorporation of any personal, financial, other sensitive or confidential details that will augment 3rd Party Identity proofing data as one or more of an additional reference point (e.g., triangulation) for data known to the State;
- include the capability to include State determined rules for the consideration of State data in consideration of the risk profile and other factors associated with the Identity Proofing requirements of the State;
- include state provided data access in all auditing, reporting, access and other requirements as included elsewhere in this Supplement;
- design and implement identity proofing methods, logic and workflows to consider State internal sources first (as appropriate) before referring to external Identity Proofing providers for ID Proofing services. By way of an example use case, if the State maintains data on a known fraudulent entity or identity, "proofing" this identity may not be required;
- design and implement identity proofing methods, logic and workflows to consider National level sources (as appropriate) before referring to external Identity Proofing providers for ID Proofing services. By way of an example use case, if the State has access to shared data on a known fraudulent entity or identity, "proofing" this identity may not be required; and
- design and implement identity proofing methods, logic and workflows to consider State level sources (as appropriate) in consideration of a known and acceptable risk profile before referring to external Identity Proofing providers for ID Proofing services. By way of an example use case, proofing a State employee or established State vendor for email access using an external service provider may not be required.

Deliverable 007. Enterprise Data Sharing Capability inclusive of:

- Known Fraudulent Identities
- Protection of Public Privacy
- Updates / Corrections to Fraudulent Identity Data Stores
- Integration and Data Sharing Framework with National or State Level Databases
- Integration Requirements
- Cross Agency Data Sharing Scope, Approach and Design Standards

6.0 Solution Pilots - General Requirements and Considerations

The State has selected Pilot Agencies to participate in the work for a variety of reasons that include, but are not limited to, those of strategic or directional value to the State Enterprise, Agency support and sponsorship, pragmatic, functional and technical considerations. Each of the selected systems are to be considered live production systems and in the public eye. Each of these systems are supported by a variety of State Contractors (generally systems integrators) who will be directed by the State to support and participate in this effort without prejudice.

Therefore, the Contractor will cooperate with the State and State contractors in the specification, design, implementation, transfer, replacement or augmentation of existing services and capabilities to those contained herein, and following the completion of the work, to the State or another provider in a manner so as to not adversely affect the provision of ongoing services.

In addition to the requirements in this section, the Contractor will:

- design and deliver a knowledge transfer program at the completion of the Pilots to State employees or contractors designed to convey operational and technical knowledge associated with the ongoing operation of the system elements that comprise the overall solution; and
- conduct knowledge and documentation transfers for the then current operational processes and tasks and work to ensure an overall continuity of services until such time as State employees or contractors can reasonably perform the roles in keeping with service levels and other operational quality, timeliness and accuracy considerations associated with the delivery of the system.

6.1 Pilot Agency 1: Ohio Enterprise eLicensing System (Identity Proofing, 2FA)

The Department of Administrative Services (DAS), Office of Information Technology (OIT) has recently implemented an eLicensing system for the application, renewals, enforcement and inspections of a variety of professional and operating Licenses for the State's 120+ Agencies, Boards and Commissions that is based upon the Safesforce.com platform. Based on recent developments, and the State's desire to position itself as one of the most individual/business friendly States in the country to start and operate a business or get licensed, the State has determined that a more flexible and easy-to-use licensing process has been developed.

In general, the State's eLicensing strategy and platform contains the following elements:

- Standardization of the Enterprise's approach to eLicensing based on a configurable platform (Salesforce.com and Basic.gov);
- Removal of "programming based" custom software applications to a more "configuration driven" approach that allows OIT, and Agencies, to more efficiently design and deploy new License categories while migrating from the legacy application set;
- Enablement of OIT employees to design, configure, operate and maintain the eLicensing platform wherever possible while (if needed) leveraging external Systems Integrators for those functions that require specialized assistance; and
- Leverage of a modern SaaS/Cloud platform as a viable and sustainable development and operating platform for eLicensing needs for all Agencies with regard to time to market, agility in responding to new or changing requirements and cost effective from a development and operations perspective.

As this capability is public, businesses facing and contains a variety of personal and financial information considered sensitive, the State seeks to significantly improve the capabilities of the system through the implementation of Identity Proofing and Two Factor Authentication.

The State's Enterprise eLicensing system, based on **Salesforce.com** and **Basic.Gov** cloud software is currently in production and implementing subsequent phases to support the first 26 Boards and Commissions, over 960,000 professional and occupational licenses, and over 400 State users. Over the next 24-36 months, the eLicensing system will be expanded to support most professional and occupation licenses in the State for the State's 120+ Agencies, Boards and Commissions.

Summary Scope of Pilot Agency	
Domain(s)	Summary Solution Elements

Citizen	State Worker	State Vendor	Ohio Business	Privileged State Worker	Proven Identity	Attribute Proofing	2 Factor Authentication	Logging and Real-Time Fraud Analysis	State Systems Integration Services
	✓		✓	✓	✓		✓	✓	✓
Priority Focus Shown in Black Text, all boxes indicated are in the summary scope of this Pilot Area.									

The eLicensing Pilot will require support for Identity Proofing for a subset of the professional and occupational licenses at application time (items with a light blue shading in the table below).

The eLicensing Pilot will require support for token based Two-Factor Authentication for any State Worker who has access to perform changes or updates to licenses, license payments, and for license renewals (items with a light red shading in the table below) as well as Privileged State Users.

The eLicensing Pilot will require support for Enterprise Logging, Audit and Fraud Detection for all access (user and State) as per the below sizing table.

Deliverable 008. Pilot 1 Requirements Scoping, Elaboration and Confirmation Document
Deliverable 009. Pilot 1 Design Document based on Requirements
Deliverable 010. Pilot 1 Functional and Technical Build Completion Acceptance
Deliverable 011. Pilot 1 System Test Completion Acceptance
Deliverable 012. Pilot 1 User Acceptance Testing Completion
Deliverable 013. Pilot 1 Deployment to Production
Deliverable 014. Pilot 1 Post-Production Completion Activities and Acceptance

6.1.1 eLicensing Platform Sizing Considerations

The State's Enterprise eLicensing platform had a successful go-live for three Agency Boards in the summer of 2015 and anticipates additional functionality and Agencies will be implemented in a variety of Agile phases that are generally organized as 90-120 sprints. As a sizing baseline and estimating guideline, the following table is offered to assist Offerors in the formulation of their responses to this RFP:

Release #	Pilot	R2	R3	R4	R5	R6
Approximate Go-Live Date	8/3/2015	12/14/2015	6/26/2016	12/12/2016	6/26/2016	12/11/2017
Incremental State SalesForce/BasicGov User Count associated with Release (State Workers)	93	42	99	86	36	43
Cumulative Total State SalesForce/BasicGov User Count (State Workers)	93	135	234	320	356	399
Privileged State Users of Salesforce/BasicGov Platform	10	10	10	10	10	10
Licensee Users in Release (Individuals)	147,789	200,553	325,477	130,483	69,584	76,271
Total Community Users **Cumulative**	147,789	348,342	673,819	804,302	873,886	950,157
Business Users (i.e., Businesses Licensing on Behalf of a group of Licensees) in Release	9,509	17,004	1,638	25,015	13,228	4,589
Business Users (i.e., Businesses Licensing on Behalf of a group of Licensees) **Cumulative**	9,509	26,513	28,151	53,166	66,394	70,983

6.2 Pilot Agency 2: Ohio Business Gateway 3.0 (Business Identities and 2FA)

The Ohio Business Gateway (OBG) Electronic Filing is a nationally recognized, collaborative initiative of state and local government agencies and an important part of Ohio's digital government strategy. References to OBG can

sometimes also include the state's broader business web portal at business.ohio.gov, which includes several resources as well as links to other business-related state sites. OBG electronic filing services offer Ohio's businesses a time- and money-saving online filing and payment system that helps simplify business' relationship with government agencies.

The Ohio Department of Administrative Services (DAS), in conjunction with the Office of Lt. Governor, has initiated a project to realize State's goal of defining a strategy, phasing plan and implementation for the modernization of the Ohio Business Gateway (OBG). In order to provide Ohio businesses with a system that simplifies business communications, registrations and interactions with the State, DAS is interested in engaging in a Project to modernize and expand the scope of the Ohio Business Gateway.

Ohio businesses use OBG to access various services and electronically submit transactions and payments with many state agencies. OBG Electronic Filing also partners with local governments to enable businesses to file and pay selected Ohio municipal income taxes.

The OBG Electronic Filling currently offers the following Service Areas:

- Business Enterprise Programs
- Commercial Activity Tax
- Deferred Compensation
- Development Services Agency Invoice Payments
- Employer Withholding Tax
- Equal Opportunity Certifications
- Financial Institutions Tax
- InvestOhio
- Municipal Income Taxes
- Petroleum Activity Tax
- Sales and Use Tax
- Severance Tax
- Taxation Department New Registrations
- Unclaimed Funds
- Unemployment Compensation Tax
- Wireless 911 Charges
- Workers' Compensation Payroll Report

The OBG offers services in collaboration with the following agencies:

- Bureau of Workers' Compensation
- Development Services Agency
- Department of Administrative Services
- Department of Commerce
- Department of Job & Family Services
- Department of Taxation
- Opportunities for Ohioans with Disabilities
- Public Employees Deferred Compensation
- 500+ Municipalities

As this capability is public, businesses facing, contains a variety of business and financial information considered sensitive and (in totality from a revenue perspective) very high monetary value, the State seeks to significantly improve the capabilities of the system through the implementation of Identity Proofing and Two Factor Authentication for the Agencies and Businesses in the State that utilize the OBG.

Offeror Notes: The Ohio Business Gateway 3.0 is the subject of an upcoming procurement opportunity. The services required under this procurement are **strictly limited to** the provision and integration of definitive Identity and Two-Factor Authentication services for the Ohio Business Gateway as contained herein. All other State requirements pertinent to the development and evolution of the Ohio Business Gateway are contained in the aforementioned procurement opportunity, which is separate and distinct from this RFP. The Contractor will cooperate with the State and the State selected Systems Integrator for the OBG project and support the State in ensuring that the Work contained in this RFP is delivered in such a matter as to not impede or delay the timely development of the OBG and in a manner in keeping with not adversely affecting the provision of ongoing services and other projects being performed on the OBG system concurrent with this project. As part of project initiation, the State will host meetings with the Contractor awarded this RFP and the Systems Integrator performing the OBG project and establish linkages between the respective project plans (i.e., this RFP and OBG), clearly identify roles, responsibilities, timing and dependencies and any other factors that are mutually required to ensure the success of this project as well as the degree this project (via this Pilot area) supports the evolution of the OBG. Will be determined by the State subsequent to the award of any contract arising from this RFP,

therefore the Offerors response must be designed with this in mind from a scope, timing and cooperation perspective.

Summary Scope of Pilot Agency									
Domain(s)					Summary Solution Elements				
Citizen	State Worker	State Vendor	Ohio Business	Privileged State Worker	Proven Identity	Attribute Proofing	2 Factor Authentication	Logging and Real-Time Fraud Analysis	State Systems Integration Services
	✓		✓	✓	✓		✓		✓
Priority Focus Shown in Black Text, all boxes indicated are in the summary scope of this Pilot Area.									

6.2.1 General OBG 3.0 Considerations

As mentioned, the scope and implementation specifics for the OBG 3.0 are the subject of an upcoming procurement and will be subject to Offeror proposed solutions as a result of the State's review, acceptance and award of the OBG 3.0 RFP. However, several general considerations related to OBG 3.0 that must be delivered as a result of this RFP include the following:

- The State has required the specification of an Enterprise Service Bus-based (ESB) approach in the OBG 3.0 RFP with similar compatibility and interoperability requirements as contained in this RFP. Therefore, as it relates to this RFP, Offerors are to assume a modern ESB that is contemporary to the needs of the OBG and compliant with State integration requirements contained herein (generally Oracle ESB or IBM/WebSphere or an interoperable alternative ESB).
- The actual ESB selected will be made known to the Contractor following the Project Start Date of this RFP and the State and Contractor will mutually determine impacts to scope, timing and other matters pertaining to the OBG 3.0 solution.
- The OBG interacts with a variety of State Agencies, and as part of the OBG project the ESB interoperability standard that is designed and developed for the OBG will be the prevailing service integration method for all OBG related transactions and systems activities.
- OBG 3.0 should be assumed by Offerors to be a consumer of the identity, 2FA and Fraud services arising as a result of the award of this RFP, therefore for convenience purposes a summary of the specific requirements of OBG on this RFP are contained below.

6.2.2 Specific OBG 3.0 Requirements on the Services/Solution in this RFP

Offeror Note: the term **"Offeror System"** in this section shall pertain to the Offeror Proposed System. Service or solution as applicable:

- The Offeror System will allow for the establishment and maintenance of an Identity Verified "Business Enterprise" inclusive of authorized users within that enterprise that are authorized to perform transactions within the OBG. The specific roles and functions permitted with respect to this enterprise and its users will be managed within the OBG;
- For all users. the Offeror System will perform 2 Factor Authentication based on tokens for State users and Devices for Business users;
- The Offeror System must provide all authorized users to define designates, who can operate on behalf of business owners. At the minimum, businesses can designate service provider companies, CPAs, and any

additional designates defined during design, to initiate, process, and submit specific transactions on their behalf;

- The Offeror System must allow all authorized users to activate/grant access, de-activate, and delete any type of user account that is associated with their organization and automatically send a notification (based on the user's preferred communication preferences) to the users impacted;
- The Offeror System must allow application users that complete transactions on behalf of a business to deactivate their access from accounts they no longer service and automatically send a notification (based on the user's preferred communication preferences) to both the application user requesting to be deactivated and the business application user of the deactivation;
- The Offeror System must support the enforcement Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) authentication when all users create an account and register as a user (to prevent against bots);
- The Offeror System must allow all users to create their own username;
- The Offeror System must allow all users to create a user profile and enforce business rules to ensure users are providing minimum required data;
- The Offeror System must prevent all users from creating a duplicate user based on defined business rules. At the minimum, use the email address associated to the user to perform duplicate user validation;
- The Offeror System must enforce all users to populate all mandatory information to complete their user profile upon registration and as required to establish a Definitive Proven Identity;
- The Offeror System must automatically send an email notification with basic user information to the application user upon successful user Identity Verification;
- The Offeror System must automatically validate that any email address entered is a good email address (at the minimum, structurally has all the components of an email address);
- The Offeror System must prevent duplicate accounts from being created by application users based on an existing account with the same FEIN, SSN, or any other attribute defined during design;
- The Offeror System must require all application users to provide either a Federal Identification (FEIN) or Social Security Number (SSN) upon registering for an account in the system;
- The Offeror System must enforce all application users to populate all mandatory information to complete their account profile and as required to validate Identity upon registering for an account in the system;
- The Offeror System must allow all users to maintain account administration information; and
- The Offeror System must allow authorized application users to change account information and login credentials.

Deliverable 015. Pilot 2 Requirements Scoping, Elaboration and Confirmation Document
Deliverable 016. Pilot 2 Design Document based on Requirements
Deliverable 017. Pilot 2 Functional and Technical Build Completion Acceptance
Deliverable 018. Pilot 2 System Test Completion Acceptance
Deliverable 019. Pilot 2 User Acceptance Testing Completion
Deliverable 020. Pilot 2 Deployment to Production
Deliverable 021. Pilot 2 Post-Production Completion Activities and Acceptance

6.3 Pilot Agency 3: Ohio Department of Taxation (Identity and Attribute Proofing)

The Ohio Department of Taxation is responsible for taxpayer registration, returns and remittance processing, taxpayer accounting and billing, non-filer discovery, selection and management of audits, processing

assessments, administering taxpayer appeals, revenue accounting and distribution of tax proceeds to local governments within the state.

The Ohio Department of Taxation (ODT) currently collects and administers Ohio State Personal Income and School District Income taxes using the State Income Tax Modernization System (IMOD). The IMOD system is a COBOL/CICS based State developed application with a DB2 backend. Personal Income Tax and School District Income Tax taxpayers can file and pay via electronic commerce channels developed and supported by The Ohio Department of Taxation. The vast majority of filings originate from commercial software packages; many of these are sent forward with the aid of tax preparers. These software packages are configured to send transactions to ODT through the IRS clearing house known as Modernized Electronic Filing (MeF.) Software companies and preparers send both federal and state returns through MeF. Other Ohio taxpayers make use of ODT's homegrown portal known as iFile. iFile is self-service, and there is no cost to the taxpayer.

The Ohio Department of Taxation is currently involved in a multi-year project to integrate all of their taxes into a single platform known as the State Taxation Accounting and Revenue System (STARS). The STARS system is based upon the Oracle Public Sector Revenue Management solution. This system is currently being used to collect and administer Ohio state taxes for twelve (12) business and excise taxes and will include eleven (11) additional taxes with Personal Income and School District Income implementation scheduled for January of 2018.

The pilot implementation will focus on Personal Income and School District Income Taxes currently administered through the IMOD system.

Summary Scope of Pilot Agency									
Domain(s)					Summary Solution Elements				
Citizen	State Worker	State Vendor	Ohio Business	Privileged State Worker	Proven Identity	Attribute Proofing	2 Factor Authentication	Logging and Real-Time Fraud Analysis	State Systems Integration Services
✓	✓		✓	✓		✓	✓	✓	✓
Priority Focus Shown in Black Text, all boxes indicated are in the summary scope of this Pilot Area.									

The Pilot implementation must be implemented to support Assurance Levels 1 through 3, for all identified user populations including State Workers, Privileged State Workers, Businesses, and Citizens. The pilot implementation must support multi-factor definitive identity proofing, attribute proofing, two factor authentication, and Authentication and Access Logging and Reporting.

The pilot implementation must be implemented support multi-factor definitive identity proofing in both batch and real-time modes. The pilot implementation will also need to support multi-factor definitive identity proofing for both identities for an overpayment joint return.

The pilot implementation will need to process the identities of approximately 10 million (10,000,000) refund requests, and detect those identities that require further proofing via the multi-factor identity quiz. It is expected that approximately 2 million (2,500,000) identities will need to be proofed. This includes dependents claimed on the tax returns.

Each business day the pilot implementation will send a batch file containing all tax refund requests for that day. The multi-factor identity proofing service will process this batch file within one business day and categorize each return into 1 of 3 categories. The three categories are:

- The return needs to be reviewed manually ("Manual Review");

- The return needs to be sent to the Multi-Factor identity quiz ("Quiz"), and/or any other viable alternative multi-factor identity validation solution; and
- The return does not need to be further proofed ("No Quiz").

Deliverable 022. Pilot 3 Requirements Scoping, Elaboration and Confirmation Document
Deliverable 023. Pilot 3 Design Document based on Requirements
Deliverable 024. Pilot 3 Functional and Technical Build Completion Acceptance
Deliverable 025. Pilot 3 System Test Completion Acceptance
Deliverable 026. Pilot 3 User Acceptance Testing Completion
Deliverable 027. Pilot 3 Deployment to Production
Deliverable 028. Pilot 3 Post-Production Completion Activities and Acceptance

6.4 Post Pilot Activities: Development of Extensible Enterprise Standards

As part of the conclusion of the pilot projects, the Contractor will develop a set of extensible Enterprise standards as a deliverable for the specification, use of and standards pertaining to the developed enterprise solution based on the successful completion of the Pilot Projects.

Deliverable 029. Extensible Enterprise Standards to include:

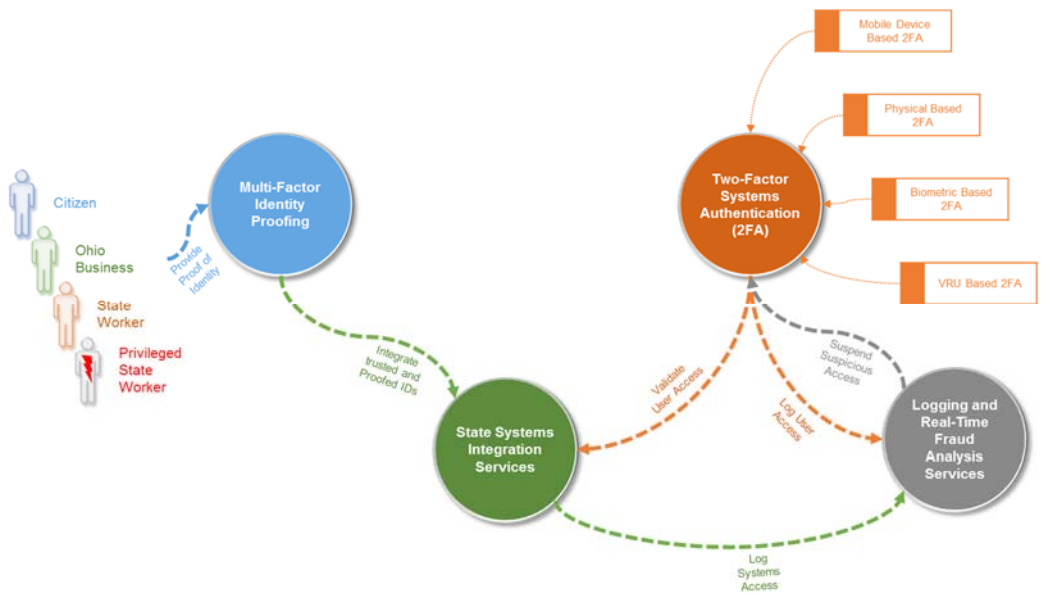
- The Identity Proofing Service Provider inclusive of integration, validation, technical, testing and other details pertinent to the State or a capable third party Contractor of the State's choosing to incorporate the features, functions and capabilities developed for the initial Pilot Agencies for other State Agencies who may wish to incorporate Identity Proofing capabilities in their systems or services.
- The Two-Factor Authentication and Token Management Service Provider inclusive of integration, validation, technical, testing and other details pertinent to the State or a capable third party Contractor of the State's choosing to incorporate the features, functions and capabilities developed for the initial Pilot Agencies for other State Agencies who may wish to incorporate Identity Proofing capabilities in their systems or services.
- Any and all Enterprise level integrations, configurations, extensions, workflows, conversions and other elements pertinent to the operation, maintenance or extension of Enterprise framework software associated with the aforementioned Services including operation manuals, release notes, test cases and results, technical contacts and documentation as provided or utilized in performing the Work for the initial Pilot Agencies.
- Any and all Enterprise level integrations, configurations, extensions, workflows, conversions and other elements pertinent to the operation, maintenance or extension of Fraud Detection software associated with the aforementioned Services including operation manuals, release notes, test cases and results, technical contacts and documentation as provided or utilized in performing the Work for the initial Pilot Agencies.
- During the Project, the Contractor will conduct informal information sharing and knowledge transfer services coincident with the delivery of the Services in this Statement of Work and on a formal basis at the conclusion of the project in such a manner as to ensure that State personnel assigned to support, develop, manage or operate the Enterprise Identity platform are apprised of the contents of each environment inclusive of features, functions, extensions, known defects and workarounds and other information as to manage and communicate to DAS/OIT leadership (in general) and users of the system (specifically) as to the most effective use of the then current services.
- These services shall be designed and delivered in a manner as to provide the State assistance, cooperation and information as is reasonably necessary to help enable a smooth

transition of the applicable services from participating Agencies (i.e., DAS/OIT, Department of Taxation, and the Lt. Governor's Office) and any Contractors associated with the development, operation or maintenance of the systems contained in the Pilots. As part of these services, Contractor will provide such information as the State may reasonably request relating to features, functions, extensions, configurations, release and programmer notes, FAQs and other delivery artifacts required to operate and maintain the system, and Contractor will make such information available to the State in a Microsoft SharePoint site provided by the State for this purpose.

7.0 Implementation of Two Factor Authentication (2FA)

Conceptually, these requirements can be viewed in the context of this overall Supplement as follows:

Conceptual Grouping of Two Factor Authentication (2FA) Services



7.1 User Authentication

System must support LDAP and Active Directory calls for username and password authentication, including passing an encrypted password string.

System must support integration with the proposed two factor authentication services/solutions and/or adaptive authentication services/solutions as required, including at least RSA SecurID tokens or stronger similar physical tokens.

System must support elevated (step-up) authentication, meaning that as a user requests more secure access, authentication requirements increase.

System must support location sensitive authentication, meaning authentication requirements increase as users attempt to access resources from less secure locations.

Solution must support Authentication and integration with the following technologies: Oracle DBMS, Microsoft SQL Server DBMS, DB2 for Z/OS DBMS, Windows Server, Linux, VMWare, Unix (generally AIX and HPUx) and to the extent possible support federated single-sign on or credential brokering of administrator authentication to an identity store, and the seamless logon to the technology where the administrator never knows the password.

Solution must support password synchronization with the following technologies: Oracle DBMS, SQL Server DBMS, DB2 for Z/OS DBMS, Windows Server, Linux, VMWare, Unix, others.

Solution must support temporary authorization of elevated privileges (such as granting domain admin to someone for a specific number hours to perform work, preferably from a known access location (e.g., IP address, VPN destination or PC/Mobile device) and then revoking the permission at the conclusion of the temporary period.

Solution must include a web services interface, to be callable by external applications for use with application service accounts.

The solution must be able to integrate with the State's PKI for certificate-based authentication (including support of revocation or suspension.)

System must provide mechanisms to prevent brute force attacks and other well-known attacks.

Authentication support must operate as an HTML form in a browser without plugins or additional software, regardless of browser (currently OEM supported versions of Internet Explorer, Microsoft Edge, Firefox, Safari, Chrome) or device type (desktop, tablet, mobile phone) or operating system (OEM supported versions of Windows, Linux, Unix: AIX, HPUX, Android, or IOS).

Supported User browsers must support HTTPS and session cookies.

Deliverable 030. 2FA Integration Enterprise Standards

Deliverable 031. Authentication Policy Draft

- Determine Appropriate 2FA parameters for Citizen, State Employee, State Vendor, Business and Privileged Users
- Establish Operating Norms and Exception Policies (for onward Fraud Detection, Auditing and Tracking)

Deliverable 032. Appropriate Mechanisms, Timing and Considerations for State Internal, State External and Privileged User Access

7.2 Standards Compliance

System must provide mechanisms for compliance with all State and Federal laws and mandates that the State is subject to including, but not limited to HIPAA, CJIS, IRS Pub.1075 Et.Seq., Homeland Security, and PCI for access to and use of secure data and applications.

System must support federated identity management, using National Institute of Standards Technology (NIST) best practices and equivalent industry standards for interoperability and integration with external public and private institutions. Including, but not limited to the following sub sections of 15.2:

- System must follow NIST 800-53 control standards for secure access to data and systems. Per NIST SP800-53: "Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet)."
- Must have an identity proofing service capable of implementing [remote and/or in-person] identity proofing processes at OMB-08-08 E-Authentication assurance levels (per NIST SP 80063-1).
- Solution must integrate with the State's existing advanced authentication system or provide NIST compliant advanced authentication per advanced authentication at level 3 or level 4 as defined in NIST SP800-63.

7.3 Technical, Operations, Change and Scalability

7.3.1 General Technical Requirements

The system must support and be implemented with a failover configuration to ensure high availability. System must not have a single point of failure.

The system must support full back up and restore capabilities so that the system can be restored from media with minimal additional intervention.

The batch and backup operations must not degrade the response times of the system in off hours, assuming a lower request load to be estimated and justified by the Service Provider.

The Offeror's hosted Primary Production and Disaster Recovery sites and all State data must be located in the United States and technically diverse from the primary production site. Technical diversity factors include at a minimum: alternative and redundant power providers or grids, telecommunications network providers to those servicing the primary and disaster recovery sites respectively.

Offeror must execute annual DR testing and provide the State with documented results and a remediation plan with committed resolution dates for any item identified as a weakness, material or otherwise from a technical, process, procedural or organizational perspective as provided to the State by the Service Provider or Contractor under this RFP.

7.3.2 Performance and Scalability Requirements

System must support a minimum of 99.99% uptime for 24 x 7 x 365 operations. (Offeror note: see Service Level Requirements Section 0 for additional specifics).

System must support a peak load of twice (2x) the expected maximum concurrency to ensure adequate spare capacity for growth and expansion without an unacceptable degradation of performance. The initial maximum concurrency is 20,000 users, but the Offeror is encouraged to adjust this number upward or downward with supporting data and estimation methods. (Offeror note: see Service Level Requirements Section 0 for additional specifics).

The Service Provider and the State will review actual peak load data no less frequently than twice yearly and mutually make sizing increase and deprecation decisions based on the actual load of the system. As this RFP affords, and the State anticipates, additional adoption of Agencies based on State priorities in the future, the Service Provider and State will review performance in advance of any such significant onboarding activity in the context of the then current performance and available capacity of the system and make adjustments as appropriate as to maintain a positive user experience from a performance and availability perspective and as to support ongoing attainment of Service Level Requirements. (Offeror note: see Service Level Requirements Section 0 for additional specifics).

Deliverable 033. System Performance Test Results

7.3.3 Operations, Maintenance and Change Management

Offeror must provide a regular patching mechanism, consistent with trust zone constraints (no internet access allowable in certain zones).

The State must be notified of any emergency maintenance activities that must be performed on internal or external components. A mutually approved procedure must be established by the State and Service Provider.

The solution must enable patch(s) or upgrade(s) to individual software or service components without shutting down access to the identity management system.

The solution must accommodate operating system and hardware maintenance on any individual hardware or network without shutting down access to the identity management system.

Offeror must comply with Ohio Request for Change (RFC) and change control management procedures which will be jointly developed to mutual satisfaction of the parties in the context of the proposed solution, but nonetheless

must include written State approval for any change to any element that could adversely impact users of the system (public, State or otherwise) or render a State system that utilizes the service unavailable to the systems user community (public, State or otherwise).

7.4 Authentication and Access Logging and Reporting

7.4.1 Authentication/Access Reporting and Logging

System must provide authentication and access reports based on any arbitrary attributes the State requires as provided by the underlying software or solution elements.

System must support report generation and logging to a State data store (see Section 8.0 for additional details) for administration tasks, including, but not limited to password resets, granting of privileges, account suspensions, and any other auditing event.

System must support report generation and alerting of State Security personnel both directly and via the State's SEIM for security incidents such as, but not limited to, hacking attempts and attempts to access secure resources above an individual's access levels.

The solution must support configuration of Standardized and Ad-hoc reports without requiring any customized programming using common reporting tools such as IBM/Cognos, which is the States standard reporting tool.

7.4.2 System Operational Reporting, Alerts and Notifications

System must include real time mechanisms for monitoring responsiveness, resource consumption, storage utilization, and overall system health.

System should include support for intrusion detection and other hacking attempts on identity stores.

System must provide real-time notification to administrators and State monitoring staff for performance issues and any security event. Notification must be configurable for email, mobile phone, text messaging, etc.

Alerts need to be configurable by administration staff, not requiring code changes.

Deliverable 034. Master Monitoring and Detection Event Model

- Catalog of All Suspicious and Fraudulent Behaviors
- Tracking and Alerting Framework
- Logging of Systems Access
- Archive / Purge of Systems Access Logs
- Privacy Considerations in Event Logging

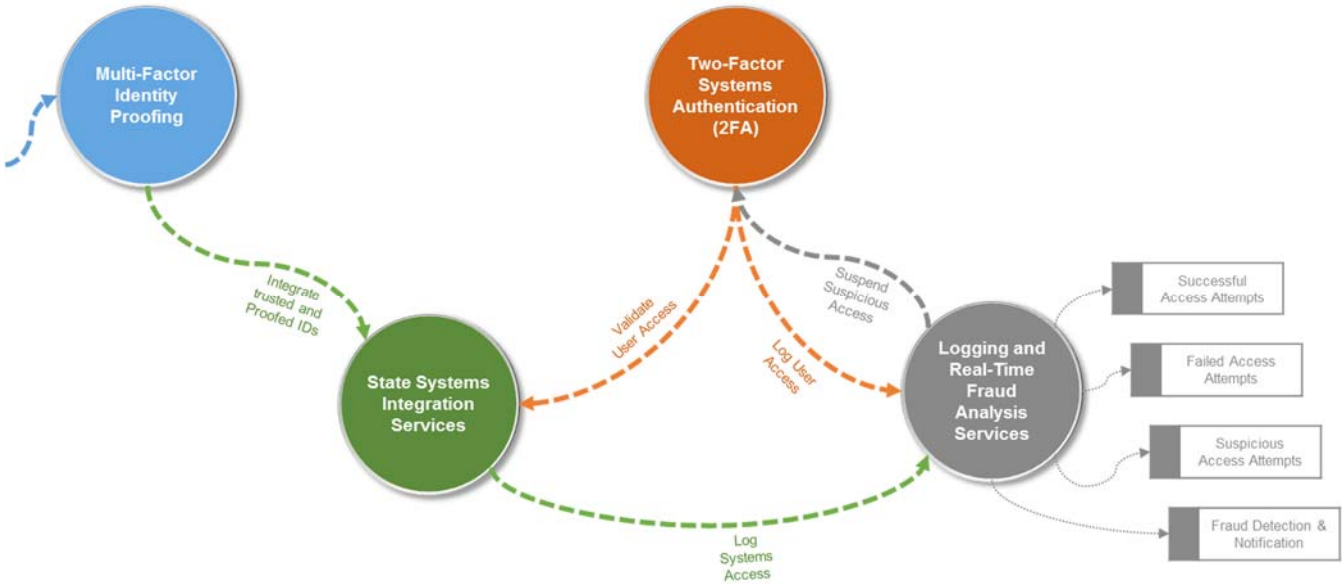
8.0 Implementation of Enterprise Logging, Audit and Fraud Detection

The State wishes to identify, design, implement and deploy an Enterprise Level fraud detection capability, initially focused on matters complimentary to the scope of this RFP (i.e., Identity Proofing and Multi-factor authentication), but extensible to other generalized uses in the State's IT applications and infrastructure portfolio. The proposed solution should be complimentary to existing State capabilities including but not limited to physical level security and protection of our computing assets and facilities as well as Infrastructure Level capabilities including but not limited to centralized intrusion detection, reporting, notifications as well as "operating system" level protections around state hardware, servers, networks, storage and the like.

Therefore Offerors are to propose a system (or framework of systems comprising an overall solution) that address all requirements in this Section, and as a result of the work in this Supplement, implement specific capabilities limited to support **both** of the Pilot Agency systems as defined and required in Section 5.0 of this Supplement.

Conceptually, these requirements can be viewed as follows:

Logging and Real-Time Fraud Analysis, Reporting and Analytics in the Context of the Overall Solution



8.1 Programmatic Fraud Detection and Fraud Analytics

The Offeror will specify, design, implement and deploy a system to programmatically identify Identity fraud, or suspected fraud that runs as a real-time background processes (transparent to users) that utilizes all available (both State and External Sources) contextual attributes and data points such as geolocation, device characteristics, user behavior, navigations and transaction activity to determine the likelihood of fraudulent transactions.

The system will compare this information to expected behavior using machine learning or statistical algorithms, or State defined or Offeror proposed “best practice” rules that define "abnormal" behavior and activities.

The system will verify legitimacy of a user's identity and system use using available internal and external information sources including the comparison of incoming identity information and contextual attributes (as described above), and comparing against available external and internal identity information (as required).

The system should be capable of utilizing (but not storing or otherwise making available outside of the system), personally identifiable Information (PII), such as name, Social Security number (SSN), passport number and date of birth; and non-PII information, such as email address, Internet Protocol (IP) address, and device and phone number and attributes.

Deliverable 035. Fraud Detection/Analytics Requirements Scoping, Elaboration and Confirmation Document
Deliverable 036. Fraud Detection/Analytics Design Document based on Requirements
Deliverable 037. Fraud Detection/Analytics Functional and Technical Build Completion Acceptance
Deliverable 038. Fraud Detection/Analytics System Test Completion Acceptance
Deliverable 039. Fraud Detection/Analytics User Acceptance Testing Completion
Deliverable 040. Fraud Detection/Analytics Deployment to Production
Deliverable 041. Fraud Detection/Analytics Post-Production Completion Activities and Acceptance

8.2 Identifying and Remanding Suspicious Identities to Proofing and Other Methods

The Offeror Proposed system will include, and be designed, implemented and deployed to leverage a combination of rule-based (State and Industry Best/Common Practice) methods as well as statistical or machine learning techniques to enable the linkage and relationships across users and other entities and their attributes using multivariate data stores to detect fraud.

The system will be designed, implemented and deployed to analyze and correlate user and other entity behavior across different access channels, modes and devices, and prioritize alerts and warnings using a combination of State and Best/Common practices, rules and statistical methods.

The system will include the capability to be extended to monitor and analyze user and entity behavior as well as to identify anomalous user or entity behavior using a combination of State and Best/Common practices, rules and statistical methods.

The system will be designed, implemented and deployed to:

- Detect account takeover, which can occur when user account credentials are stolen (for example, via malware-based attacks);
- Detect identity fraud (for example, when a fraudster sets up a new account or conducts an unauthorized transaction, using a stolen or fictitious identity);
- Detect the use of a stolen financial account (for example, a stolen credit card) by a fraudster when the individual makes a purchase or moves money from one account to another or seeks benefits (financial or otherwise) for which the identity is not entitled to;
- Identify and detect automated scripts targeting a limited number of accounts or an Agency system or infrastructure asset;
- Identify and detect automated scripts engaged in a massive attack against a large number (e.g., thousands) of accounts;
- Identify and detect an individual conducting a manual attack;
- Identify and detect a combination of human(s) and automated script(s) executing either targeted or mass attacks; and
- Identify and detect fraudulent or suspicious access via location based, network, device, browser or other methods that are inconsistent with authorized legitimate access.

The Proposed system should support user and entity profiling and behavioral analytics, such that a user's or entity's ongoing behavior is captured in a profile that can subsequently be used to compare against new activity to determine whether the activity is legitimate.

The Proposed system should include anomaly detection capabilities using statistical models, rules, or a combination of both. Ideally, one or more of each type of statistical model should be supported by the System for State use.

System modeling capabilities must include:

- Confirmed “bad” behavior and access methods that indicate illegitimate access;
- "Normal behavior," most of which is assumed to be "good.” Including common system uses, navigation transactions, transaction limits, historical transaction levels and values and other factors;
- The system should, as part of routine functions establish a history of confirmed fraud and bona-fide use, and include baselining various activities and entity behaviors;

- Detection of anomalies that deviate from established baselines but include controls to help the State to manage transactions holistically realizing that not all anomalies represent fraud;
- Continuous behavioral profiling of users, accounts and entities;
- Initiating workflow(s) to perform a real-time Identity verification on demand (using the Services included in Section 4.0 of this Supplement) for any State defined high-risk interaction — using internal and external identity information;
- Ingesting and integrating external threat intelligence into fraud detection analysis and operations, initially from the State's Enterprise SEIM;
- Using the above data sources and other State data to compare incoming transactions across online channels with existing profiles and norms of user or entity behavior in order to detect fraud; and
- Establish linkages and correlations between, fraud detection uses rules, statistical models or both and linkages across key attributes, such as device, name, IP, phone, address and email address and other factors, to find patterns of suspect activities.

Deliverable 042. Penetration Testing
Deliverable 043. SEIM Integration Testing

8.3 Integration with Enterprise Security, Notification and Tracking Services

8.3.1 General Identification and Integration Requirements

Should the system determine that one or more of: 1) a known fraudulent identity; 2) fraudulent activity; or 3) suspicious activity or transaction in progress, the system will:

- Suspend access to the system, if actual behavior is out of range with what's expected or if the user appears suspect;
- Remand attempted access to the system to the State to conduct further manual review and investigation of the transaction or user, as warranted;
- Trigger automated identity re-verification, stepped-up user authentication and/or transaction verification to automatically determine the legitimacy of the user or transaction as appropriate; and
- Be configurable to initiate State (or State Agency) specific workflows related to suspending or if necessary terminating compromised accounts inclusive of (at the State request) incorporating terminated account data into State Known Fraudulent Identity stores as required in Section 5.1 of this Supplement).

8.3.2 State Enterprise Security Event Management System Integration

As part of project initiation activities, the Contractor will conduct requirements and design sessions with DAS/OIT Security to establish a definitive set of **"security events"** that are available within the proposed solution elements by area including: Offeror Proposed Multi-Factor Identity Proofing platform or service; capabilities within the scope of Pilot Systems; the proposed Two-Factor Systems Authentication platform or service (physical, device and voice based) and the proposed logging and fraud detection solution.

Given this mutually agreed set of solution events, the Contractor will:

- implement integration between the proposed solution elements and services and the State's SEIM;
- support the State in the development of security alerts, warnings, programmatic system actions (e.g., suspend user access, require re-validation of IDs, alert Agency or State security staff) and other features as required to support the State in identifying fraudulent access to State systems; and

- ensure the State can take action as it requires within the context of State systems, networks, computing platforms and other means as to minimize the State's exposure to unapproved or inappropriate access.

The system must support real-time replication or integration of audit logs to the State's Security Information and Event Management (SIEM) solution: based upon an industry leading Security Intelligence Platform which will be disclosed by the State upon aware, for audit reporting, alerting and management by State Security and Privacy Personnel.

Deliverable 044. Compendium of Tracked System Events
Deliverable 045. State SEIM Integration Design
Deliverable 046. State SEIM System Test
Deliverable 047. Final State Acceptance Testing

8.3.3 Other Notification Capabilities

The proposed system will be designed, implemented and deployed to:

- Support electronic notification of high levels of fraud, programmatic fraud or other inappropriate access attempts that meet State defined parameters and utilize existing notification protocols and capabilities in the State such as text message, email and other common communications formats; and
- Be extensible for integration with State operational consoles utilized to protect State physical, logical, virtual, infrastructure and application level Agency users and State responsible parties. By way of an illustrative use case - alert an Agency system or security manager via email that his/her system is under attack or probing via fraudulent identities, credentials or other means.

8.4 Incorporating Fraudulent Identities and Entities in State Data Stores, Onward Sharing within the State

The proposed system will be designed, implemented and deployed to:

- Identify, for State review, all identities and entities that are determined via the methods, tools and techniques in this Supplement as well as any Contractor provided means, to be fraudulent, erroneous or suspicious;
- Ensure that no identifying details such as personal, financial or credential (e.g., password or token) information is included in any physical representations of data;
- Upon State concurrence or approval, provide automated programmatic mechanisms to include these identities and entities in State Enterprise data stores (as defined in Section 5.1 of this Supplement) for onward and subsequent State use;
- Upon State concurrence or approval, provide automated programmatic mechanisms to onward share these identities and Agencies in non-State (e.g., Federal or Cross-State) national fraud listings;
- Provide secure, audited manual entry capabilities to add, delete or modify any records that may have been inadvertently added to a fraudulent identity store as a result of any systemic, manual or other means; and
- Log all activities, programmatic, systemic or manual pertaining to any adds, changes, modifications or deletions of data in any State fraudulent identity store for State review and auditing purposes.

8.5 Auditing and Reporting Requirements

The Fraud Detection and Management solution shall:

- Be capable of producing audit reports via either Offeror provided web reporting tools or State access via State standard reporting tools (IBM/Cognos);

- Have the capability to generate ad-hoc business reports that can support internal State invoicing needs including Agency use/consumption, application level access and proration of the entire Service based on Agency actual use/consumption;
- Be capable of producing a web accessible report dashboard with the ability to export the report in CSV, PDF and Excel as appropriate to the content of the report;
- Not display or maintain sensitive personal or financial information in logs or administrative messages; and
- Be capable of generating a report for a specific customer pseudonymous identifier when the identifier is required to support other functionality.

9.0 State Project Delivery, Management, Methodology and Approach Requirements

The Contractor will provide the state its recommended methodology and approach to the Pilot projects and any projects that arise following the successful completion of the Pilots as a result of this RFP. The Contractor will provide knowledge and awareness transfer to State team members on use of the methodology so that State team members may complete their work in accordance with the responsibilities in this SOW.

The State maintains a project management and reporting methodology that is used at varying levels for complex, transformational Information Technology projects. This methodology is designed to provide a substantive and objective framework for the reporting and review of projects to impacted stakeholders and, should the need arise; identify the need for corrective action for one or many of the participants in a project (e.g., State, Contractor, Customer, Stakeholder).

The State acknowledges that various contractors that may do business with the State may maintain unique or proprietary project management methodologies, but seeks to ensure that the overall project is delivered to the State as contracted. Therefore a minimum standard project management reporting standard has been created to serve the State's project management and oversight needs while not adversely impacting or influencing Contractor provided delivery methodologies.

The Contractor must provide a summary Project Plan as requested by the State. For purposes of a summary project plan specific phase and gate dates, effort and costs are a sufficient minimum.

Following the award of this Contract, and during the project mobilization phase Contractors must include the following deliverables and milestones within their detailed project plans and methodologies at a minimum upon commencement of the project:

State Project Management Methodology, Minimum Standards

Phase	Milestone, Activity, Deliverable, Gate	
	Complete Gate 1 (G1)	G
Prioritization and Scheduling	Create Project Plan	D
	Identify / Secure Resources	A
	Create Detailed Cost/Time Analysis	A
	Create Phasing Strategy / Deliverables by Phase	D
	Conduct Policy Review	A
	Initiate Procurement Activities/Plan	A
	Complete Gate 2 (G2)	G
Requirements: Functional & Technical	Create/Maintain Refined Project Plan	A
	Establish Implementation Strategy	D
	Assess Internal/External Project Dependencies	A
	Assess Internal/External Risks	A
	Create Stakeholder/Customer Communications Plan	A
	Create Detailed Resource Plan	A
	Establish Level 0 System Design	D
	Establish/Manage End-User Goals	A
	Determine Existing Process Change Model	D
	Identify New/Enhanced Business Processes	D
	Finalize Implementation Strategy	M
	Analyze Impact to Enterprise Architecture/Data Model	A
	Develop Deployment Strategy	D

Phase	Milestone, Activity, Deliverable, Gate	
	--> Continued from prior column	
Component Test	Establish Component Test Expected Results	D
	Establish Test Plan & Procedures	A
	Create Test Procedures	A
	Execute Component Test	M
	Collect Performance Metrics	A
	Produce Test Analysis Report	D
	Create Component Technical Documentation	D
System Integration Test	Establish System Test Expected Results	A
	Establish UAT Expected Results	A
	Establish Test Plan & Procedures	D
	Collect Performance Metrics	A
	Produce System Test Report	M
	Create System Operational Documentation	D
	Publish Final Procedures	A
	Create System Technical Documentation	D
	Publish Version / Release Document	D
	Develop Training Scripts	A
	Develop Training Guide	A
	Complete Gate 5 (G5)	G

	Finalize Development Tools and Production Requirements	A
	Validate Customer Adoption Assumptions	A
	Complete Gate 3 (G3)	G
Design: Functional & Technical	Follow/Track Final Project Plan	A
	Compile Final Impact Analysis	A
	Compile Final Risk Assessment	A
	Create Detailed Design Documents - Functional	M
	Create Detailed Design Documents - Technical	M
	Establish Performance Requirements	D
	Establish Operational and Support Requirements	A
	Obtain System Application Software, Tools	A
	Create Process Flows with Key Inputs/Outputs	D
	Create Interface Control Documents	D
	Create Conversion/Migration Plan	D
	Create Integration Plan	D
	Develop Stakeholder Communications Materials	A
	Create Solution System Architecture Documents	D
	Update Enterprise Architecture Documents	A
	Create System(s) Sizing Requirements	A
	Establish Test Environment Plan	A
	Establish SDLC Environments	M
	Complete Gate 4 (G4)	G
Component Construction	Develop/Compile Overall Test Plan	A
	Establish Final Processes	D
	Develop Test Analysis Report	A
	Establish Q/A Metrics	A
	Create/Refine Development Plan	A
	Develop Code/Solution	D
	Gather and Report Q/A Metrics	A
	Develop UAT Plan, Scripts and Cases	D
	Establish Operational Performance Baseline	M
	Publish Committed Capacity Plan	A
	Prepare Component Test Analysis Report	D
	Develop Training Scripts	A
	Develop Training Guide	A
	continue to next column -->	

User Acceptance Testing	Perform User Acceptance Test	M
	Document/Publish Issue/Bug List	A
	Prioritize Issues/Bugs	D
	Create Remediation Effort/Schedule of Outstanding Issues/Bugs	A
	Perform Final Performance and Sizing Testing	M
	Create Operational Documents	D
	Create User Job Aids	A
	Complete Gate 6 (G6)	G
Deployment	Compile Release Checklist	D
	Update Business Contingency / Continuity Plan	A
	Transition Operational Procedures	M
	Publish Job/Control Schedule	A
	Establish SLA Parameters	A
	Assemble Audit Impact Statement (integrity, security, privacy)	A
	Create Release Verification Checklist	D
	Execute Operations Training	A
	Perform Release Verification	M
	Update Enterprise Architecture and Data Model	A
	Update Data Center Environments	M
	Perform User Training	M
	Disseminate Documentation and Procedures	A
	Complete Gate 7 (G7)	G

9.1 Project Management and Coordination Services

The Project will follow the Governance structure defined by the State. Project Management will include the activities to manage the Project including directing the Project Team according to the Project work plan, reporting status, managing issues, assessing quality, leading project meetings, and monitoring schedule and scope changes. The Project Team will produce project status reports on a weekly basis. The format of the status report will be mutually agreed to by the State and the Contractor during the first week of the Project.

The Contractor will, in conjunction with an authorized Statement of Work arising from this Supplement:

- Be responsible for the coordination and delivery of the overall Project;
- Ensure that an appropriate “Project Kickoff” occurs and that all integrated work plans are agreed to by the State from project commencement;
- Ensure that all efforts have an effective version control mechanism for all documents within the project document library that will be maintained on a State provided Microsoft SharePoint site;
- Work with the State leadership to ensure that the Project is staffed appropriately;
- Ensure that required testing activities across both technical and operational components are completed to minimize Project risk; and
- Collaborate with the task areas to ensure appropriate cross-team communication and delivery.

For purposes of the Project, “Perform” or “P” means, that the party assigned the task has the duty and ultimate responsibility to take all appropriate steps to complete or facilitate the identified task unless otherwise provided for between the parties, subject to the Supporting party completing its interdependent responsibilities. The term, “Support” or “S” means that the party has the duty and responsibility to provide ancillary support or assistance, which may be necessary to enable the party providing the “Perform” task to complete that task unless otherwise

provided for by the parties. The designation, "-" means that the party has no responsibility for the task, unless otherwise agreed by the parties.

Key Tasks	State	Contractor
Conduct Project kick-off meeting	Support	Perform
Create a Work Breakdown Structure (WBS)	Support	Perform
Create and Maintain a project work plan and any related deliverable sub plans	Support	Perform
Review Deliverables and manage the State's approvals	Perform	Support
Review Deliverables and manage the Contractor's approvals	Support	Perform
Prepare and conduct project meetings	Support	Perform
Prepare and conduct stakeholder meetings	Perform	Support
Create Project Status Reports adhering to the PMO policies	Support	Perform
Report and manage issues and risks	Support	Perform
Monitor and report schedule and scope changes	Support	Perform
Identify State stakeholders and manage expectations	Perform	Support
Assist with on-boarding for the Contractor resources	Support	Perform
Assist with on-boarding for the State resources	Perform	Support
Confirm State Project staffing	Perform	Support
Confirm Contractor Project staffing	Support	Perform
Confirm Project governance	Perform	Support
Initiate Production Acceptance Criteria ("PAC") process	Support	Perform
PAC – Provide planned checkpoint review dates	Support	Perform

9.2 Create and Maintain Project Plan

The Contractor must produce a detailed Project Plan, in electronic and paper form, to the State Project for approval within twenty business days after the State issues a purchase order or other written payment obligation under the Contract.

Deliverable 048. Master Project Plan

The Project Plan should include the following (at a minimum):

- Project Integration;
- Project Scope;
- Project Time;
- Project Quality;
- Project Staffing;
- Project Communications;
- Project Risks/Issues; and
- Project Procurement.

The Contractor must lead a planning session, which ensures the following:

- A common understanding of the work plan has been established;
- A common vision of all deliverables has been established;
- Contains a critical path that identifies all major milestones, dependences (both internal and external to the project), resources by name and resource assignments and is complete and inclusive of the entire work effort from commencement until conclusion of all contracted activities; and

- Clarity on scope of overall project and the responsibilities of the Contractor has been defined and agreed to by the State that includes a common understanding of the business, process, technical and other elements of the overall implementation as required.

Thereafter, the Contractor must:

- Formally update the Project Plan, including work breakdown structure and schedule, and provide the updated Project plan as part of its reporting requirements during the Project; and
- Ensure the Project Plan allows adequate time and process for the development for the State's review, commentary, and approval.

The State will determine the number of business days it needs for such reviews and provide that information to the Contractor after award and early in the development of the Project Plan. Should the State reject the plan or associated deliverables, the Contractor must correct all deficiencies and resubmit it for the State's review and approval until the State accepts the Deliverable at no additional cost to the State.

At minimum, the <u>Offeror must include a Proposed Project Plan(s)</u>, which will include the following:

- **A summary Work breakdown structure**; Scope statement that includes the Work objectives and the Work Deliverables and milestones associated with completion of all of the Work with specific provisions for the work contained and as required by Pilot projects;
- The Offeror must provide a **detailed Project Plan as a Microsoft Project Gantt chart (in native MS Project file ".mpp" format)**, showing all major Work tasks on a week-by-week schedule, with Proposed Team Members (by name for Key Personnel and by Role for other Project team members) and indications of State participation requirements in the Project(s) to serve as the basis for managing and delivering the Work. The schedule must clearly demonstrate how the project will become fully operational by the delivery date. Within this detailed plan, the Offeror must give dates for when all Deliverables and milestones will be completed and start and finish dates for tasks. The Offeror also must identify and describe all risk factors associated with the forecasted schedule;
- **The offeror will indicate who (State or Contractor) is assigned responsibility** for each Deliverable within the work breakdown structure to the level at which control will be exercised;
- Performance measurement baselines for technical scope, budget adherence, deliverable assembly, production and approvals in the context of the overall schedule;
- Description of the Offeror's proposed organization(s) and management structure responsible for fulfilling the Contract's requirements and supporting the Work, in terms of oversight and control;
- A summary Required State staff and their expected roles, participation and level of effort by project area (e.g., functional, technical, business) as well as role within each Project Phase (e.g., Requirements, Design, Construction, Testing, Deployment);
- Description of the review processes for each milestone and Deliverable (e.g. mandatory design review) and a description of how the parties will conduct communication and status review;
- Description of the Project issue resolution process including an escalation plan; and
- Description of the approach to manage subcontractors effectively, if the Offeror is proposing subcontractors.

9.3 Project Review Check Point.

Upon completion of the baselined Project Plan and on a quarterly basis throughout the Project, the Contractor, in conjunction with State Project team staff, must deliver a presentation to the State. At a minimum, the presentation must address any known State or Contractor issues or concerns, including but not limited to the following:

- Project scope, budget and schedule;
- Any changes to Key named resources assigned to the Project;
- Project readiness including key issues and risk from their current status;
- Project Status including variance from baseline for key milestones, tasks, deliverables (Significant work products) and project closure;
- Methodology, approach, and tools to achieve the Project goals (inventory and status of completeness and agreement for documented project management and implementation approaches, i.e., Project management plan, communication plan, requirements traceability, implementation approach and methodology); and
- Roles, responsibilities, and team expectations.

Upon completion of the presentation, the State will immediately assess the health of the project and determine next steps for moving forward with the Project, within one week of the meeting, which may include the following:

- Continue the Project;
- Terminate the Contract; or
- Suspend the Contract.

See Suspension and Termination language in Attachment Four for remedies for failure to deliver the proposed work.

Note: There may be additional Project Reviews conducted by the State on an as needed basis throughout the term of the Contract to assess Project health and ensure the Project is progressing successfully.

9.4 Meeting Attendance and Reporting Requirements.

The Contractor's project delivery approach must adhere to the following meeting and reporting requirements:

- Immediate Reporting - The Project Manager or a designee must immediately report any Project staffing changes to the State Project Representative;
- Attend Weekly Status Meetings - The State and Contractor Project Managers and other Project team members must attend weekly status meetings with the Project Representative and other members of the Project teams deemed necessary to discuss Project issues. These weekly meetings must follow an agreed upon agenda and allow the Contractor and the State to discuss any issues that concern them;
- Provide Weekly Status Reports - The Contractor must provide written status reports to the Project Representative at least one full business day before each weekly status meeting; and
- At a minimum, weekly status reports must contain the items identified below:
    - Updated GANTT chart, along with a copy of the corresponding Project Plan files (i.e. MS Project) on electronic media acceptable to the State;
    - Updated Critical Path analysis with the aforementioned GANTT chart and an accompanying PERT chart;
    - Status of currently planned tasks, specifically identifying tasks not on schedule and a resolution plan to return to the planned schedule;
    - Issues encountered, proposed resolutions, and actual resolutions;
    - The results of any tests;
    - A problem tracking report must be attached;
    - Anticipated tasks to be completed in the next week;
    - Task and Deliverable status, with percentage of completion and time ahead or behind schedule for tasks and milestones;

- Proposed changes to the Project work breakdown structure and Project schedule, if any;
- Planned absence of Contractor staff and the expected return date;
- System integration/interface activities; and
- The Contractor's proposed format and level of detail for the status report is subject to the State's approval.

9.5 Utilize OIT's Document Sharing/Collaboration Capability

In conjunction with the delivery of the Project, coincident with the start of the project through its conclusion, the Contractor must use the State provided and hosted document management and team collaboration capability (Microsoft® SharePoint™) to provide access through internal state networks and secure external connections to all project team members, approved project stakeholders and participants. In conjunction with the utilization of this tool, the Contractor must:

- Structure the document management and collaboration pages and data structures in such a manner as to support the overall requirements of the Project;
- Store all documents in machine readable, editable and native formats (e.g., XLSx, PPTx, VSD, DOCx) as opposed to proprietary, non-editable, image format or PDF based renderings;
- Be responsible for the maintenance and general upkeep of the designer configurations of the tool in keeping with commercially reasonable considerations and industry best practices as to not adversely impact the project delivery efforts performed by the Contractor and State; and
- At the conclusion of the project, or upon request of the State, ensure that the State is provided a machine readable and comprehensive backup of the SharePoint™ database(s) contained within the tool that is owned by the State and not proprietary to the Contractor or otherwise required by the State to maintain ongoing project documentation and artifacts (i.e., Contractor is to remove all Contractor proprietary or non-State owned or licensed materials from the tool).

9.6 Production/Version Control and Release Management

The Contractor will be responsible for working with the State and executing the production deployment and roll-out of any Release Package to the State's PaaS environment instance (if applicable). Production deployment includes software deployment to the production instance of the PaaS environment and (if applicable) interfaces to production tools and systems that orchestrate, manage, report or control those devices and services managed by the Service, identification of interfaces and any required conversions/migrations, installation of server software, and any required testing to achieve the proper roll-out of the Release Package software.

Contractor will establish and comply with the State required implementation and deployment procedures. This may include laboratory testing, migration procedures, the use of any pre-production or pseudo-production environment prior to production migration. Contractor will submit to the State, for the State's approval, a written deployment plan describing Contractor's plan to manage each such implementation. The tasks and activities to be performed by Contractor as part of the deployment services also include the following:

- Establish procedures and automated software versioning mechanism(s) to ensure that the entire contents of a release, following State acceptance or authorization to implement to a production environment, are complete and maintain all elements that comprise the defined Release Package and the then current production version of the software prior to deployment of the Release Package to same;
- Develop, prepare and test emergency back out or roll back procedures to return the production system to its pre-deployment State as it pertains to correcting an errant, erroneous or defective deployment of a Release Package to the production environment inclusive of all code, data, middleware, infrastructure, tables and parameters;

- If, in the opinion of the State, the deployment of a Release package to the production environment is errant, erroneous or otherwise defective, implement back-out or rollback procedures in their entirety upon the written authorization or direction of the State;
- If required, convert electronic data into a format to be used by the new solution using a data conversion program as well as perform any data cleansing of legacy data, with the State's assistance, prior to loading data to the new solution;
- Conduct production pilot(s) (including "day in the life" simulations) and fine tune solution as mutually agreed with the State as appropriate;
- Compile and maintain solution issue lists;
- Conduct post Production Deployment quality and progress reviews with appropriate State personnel;
- Develop, and thereafter maintain and make available to the State, a knowledge base of documentation gathered throughout the Release Package's life and allow for re-use of such documentation for future Projects; and
- Establish a performance baseline for the impacted business systems, and where appropriate document requirements for future enhancement of the business systems implemented as part of a future Project or Authorized Work.

9.7 Maintaining Solution and Operations Documentation

For all nonproprietary portions of the solution, the Contractor will:

- Document the solutions developed or modified by the Contractor in accordance with established methods, processes, and procedures such that, at a minimum the State or a competent 3rd Party vendor can subsequently provide a similar scope of Services;
- Develop and maintain, as agreed appropriate, the documentation on system environments. Where it is determined that documentation is inaccurate (for example, due to demonstrated errors or obsolescence), and such inaccuracy may negatively affect the Services, Contractor will correct such documentation as part of normal day-to-day operational support;
- Update programmer, End User and operational reference materials; and
- Maintain all documentation on the State's SharePoint site.

9.8 Project Delivery, Role and Responsibility Requirements

The State has organized our requirements for responsibilities of the State and Contractor based on the anticipated Activity Areas required to analyze, design, implement and deploy the solution as well as those requirements and activities required to support the deployment of the overall solution. Should an Offeror, as a result of the review of these requirements in light of their proposed approach require additional roles or clarity, the Offeror must indicate the additional requirements of the State and provide a high level rational for the same as part of their response.

The responsibility matrices included throughout the remainder of this section identify Key Tasks to be performed as part of this project. Each Key Task has been assigned to a party and the level of responsibility for each party is designated as either a "P" for Perform, "S" for Support or designated "-" for no responsibility.

Note: If the Offeror's recommended methodology does not align with the responsibility matrices below, the offeror will propose and subsequently as the Contractor adhere to matrices that do align with the Contractor's methodology. The offeror must also demonstrate that the recommended methodology and the responsibility matrices comply with the State's need to know that:

- the offeror has a complete understanding of the State's requirements;
- the offeror's design and development efforts are in line with the State's requirement for the solution;
- the offeror's progress during the project;
- the project risk is acceptable and is managed effectively by the offeror;
- the accurate and complete technical documentation regarding the solution (as designed and as delivered), and;
- the solution delivered and deployed by the offeror has been adequately tested and meets the State's requirements.

9.9 System/Environment Administration Support of the Project

The Contractor will coordinate with the State, but be responsible for all environments (production, non-production, demo/training/CRP, development and testing) as required to support the overall effort and will:

- Perform technical activities including but not limited to: version control, PS-Admin, PeopleTools development, system code/object migrations, patch implementations, log administration, data copies and exports, interface and scheduled reporting/ETLs, and responsibility for incident resolution such that migrations into production will be executed at agreed periodic intervals and other production changes will be scheduled during the maintenance window.
- Support multiple release levels of System software/hardware elements for in-scope Services, provided that such support does not impair the Contractor's ability to meet Contractor development and project commitments until such time as all environments can be upgraded to the same version/release level.

9.10 Establish and Manage a Program Management & Master Release Calendar

The Contractor will coordinate with the State in the development, and maintenance on a monthly basis a Master Release Calendar that includes a schedule (with dates) of:

- Major/Minor and Scheduled Releases, Upgrades, Updates and Enhancements;
- Implementation of Projects, Minor Enhancements or Discretionary Work;
- Scheduled Maintenance Windows and Planned Outages;
- Major and Minor Project Key Dates (i.e., Start, SDLC Gate Completion, Production Release, Completion) whether Contractor delivered or otherwise; and
- Other pertinent dates that require end-user notification or coordination.

9.11 Cooperation with State and State Contractors

Contractor will cooperate with the State in its attempts at transferring, replacing or augmenting the services responsibilities to another provider in a manner in keeping with not adversely affecting the provision of ongoing services and other projects being performed concurrent with this project.

9.12 Requirements Confirmation and Analysis (for each Pilot Agency)

The expectation for this project phase is the Contractor will thoroughly document the desired Identity Management business requirements, and elaborate on and confirm all State business, operational, functional and technical requirements and recommend changes which will improve the State's business processes and requirements.

9.13 Analyze Phase Requirements (for each Pilot Agency)

The Contractor Team will review, analyze and update the State's Requirements and system(s) documentation. The Contractor team will conduct workshops to confirm with SMEs the results of their business requirements analysis.

The Contractor Team will also analyze impacts to the integration points with external systems. In addition, the Contractor team will analyze external systems and data and recommend data for migration to the solution as applicable.

The Contractor team will deliver the resulting business requirements (expected to be a modified version of the State's current functional requirements), a Requirements Traceability Matrix (RTM), the accompanying business processes modified as required and a list of customizations if applicable. All changes to the State's original functional requirements and business processes are to be clearly indicated.

Key Tasks	State	Contractor
Review and update Business Requirements.	Support	Perform
Document analysis of integration points with external systems.	Perform	Support
Provide functional impacts within external systems.	Support	Perform
Create Requirements Traceability Matrix.	Support	Perform
Create Customization Tracking Database (if applicable).	Support	Perform
Define Technical Requirements.	Support	Perform
Define the solution architecture.	Support	Perform
Document possible solution options for identified gaps, as applicable	Support	Perform
Document plan for integration points.	Support	Perform
Define technical environment requirements for the project from design through deployment and run. This includes any components or tools required to support development, test, configuration management, etc.	Support	Perform
Updated RTM with functional requirements and technical requirements cross-referenced.	Support	Perform

9.14 Design Phase Requirements (for each Pilot Agency)

The Analyze Checkpoint must be successfully completed prior to beginning the Design phase. This includes the State's acceptance of all deliverables due to date per the project schedule. A validation of the scope and schedule for the remainder of the Project will also be completed at the Analyze Checkpoint.

The Contractor Team will create and maintain Functional Designs for the solution. Functional Designs contain data, business and security impacts and includes integration points to external systems.

Key Tasks	State	Contractor
Create Functional Designs according to the requirements.	Support	Perform
Update Requirements Traceability Matrix with design and configuration cross references	Support	Perform
Create System Test, UAT, and ORT strategies	Support	Perform
Create and update the Technical Designs for solution, including any interfaces to external systems.	Support	Perform
Create and update the Security Designs for the solution.	Support	Perform
Update environment plans for the Project	Support	Perform
Build technology environments required for Build & Test	Support	Perform
Support technical environments, including patches and fixes	Support	Perform
Create Deployment Plan	Support	Perform

9.15 Build Phase Requirements (for each Pilot Agency)

The Design Checkpoint must be successfully completed prior to beginning the Build phase. This includes the State's acceptance of all deliverables due to date per the project schedule. A validation of the scope and schedule for the remainder of the Project will also be completed at the Design Checkpoint.

The Contractor Team will build the solution and prepare for testing. The State will provide one (1) knowledgeable SME per functional area in test preparation and as mutually agreed to with the Contractor to support test preparation.

Key Tasks	State	Contractor
Provide test conditions and scripts.	Support	Perform
Build and Unit Test configuration and security to support the business processes	Support	Perform
Create System Test, UAT, and ORT conditions, scripts, and scenarios	Support	Perform
Prepare testing schedule and participation for System Test, UAT, and ORT	Support	Perform
Create Master Test Plan	Support	Perform
Build and Unit Test the solution as applicable	Support	Perform
Build and Unit Test customizations as applicable	Support	Perform
Build and Unit Test updates to Execution Environment (i.e. interfaces, print, security services, and network infrastructure)	Support	Perform
Build Test Environment(s)	Support	Perform
Build Training environment	Support	Perform
Build Operations Environment (i.e. production)	Support	Perform
Create Assembly Test and Performance Test conditions, scripts, and scenarios	Support	Perform
Support technical environments, including patches and fixes	Support	Perform
Create Deployment and Stabilization Plan and tools (readiness criteria, critical path, and cutover activity list).	Support	Perform

9.16 Test Phase Requirements (for each Pilot Agency)

The Test Readiness Review Checkpoint must be successfully completed prior to beginning the Test phase. This includes the State's acceptance of all deliverables due to date per the project schedule. A validation of the scope and schedule for the remainder of the Project will also be completed at the Test Readiness Review Checkpoint.

For avoidance of doubt with respect to testing activities, the Contractor is accountable for all activities associated with System Test while the State will participate in these activities. The State is accountable for UAT Test execution while Contractor will be responsible for test preparation, management and tracking of UAT activities.

The Contractor Team will execute System Test, User Acceptance Test ("UAT"), and Operational Readiness Test ("ORT"). The State will provide SMEs knowledgeable in test execution and as mutually agreed to with the Contractor to support test execution.

System Test focuses on the customizations, configurations, workflow and integrations. Test conditions and test scenarios to be included in the System Test will be mutually agreed upon by the Contractor and the State. These scenarios will be based on an analysis of the requirements, changes, and modifications that are approved for implementation.

UAT verifies the usability of the new processes and ensures that the system meets the needs of the organization and the end user. UAT leverages System Test Scripts and is executed by Agency resources. A key objective of UAT is to facilitate an understanding of the technology and the business change being implemented.

ORT includes end-to-end testing of processes and technologies and will be executed by State members of the Project team. ORT will be conducted during a specific time period before Go-Live.

The State will conduct a Security Test that includes an application scan, manual testing of the system using client-side code analysis, and loading maliciously formatted inbound interface files.

The Contractor Team will develop and prepare weekly status reports to monitor the progress of each test phase. The status reports will contain sections for condition creation, script creation, script execution, issue identification and resolution, and defect identification and resolution.

Key Tasks	State	Contractor
Develop and maintain test data repositories as agreed appropriate	Support	Perform
Manage and track System /Regression Test, UAT, and ORT	Support	Perform
Execute System / Regression Test and document results	Support	Perform
Execute UAT	Perform	Support
Document UAT results	Support	Perform
Execute ORT	Perform	Support
Document ORT results	Support	Perform
Prepare for and execute Security Test	Perform	Support

Key Tasks	State	Contractor
Prepare for and execute Assembly Test	Support	Perform
Prepare for and execute Performance Test	Support	Perform
Support Functional Team Testing	Support	Perform
Conduct Test Moves to Production	Support	Perform
Create the Deployment and Stabilization Plan	Support	Perform
Develop, update and maintain a migration checklist	Support	Perform
Prepare for final Move to Production	Support	Perform

The Contractor team will execute Assembly Test and Performance Test.

Assembly Test verifies that the technical architecture works together as planned and tests that all modules were migrated appropriately. The objective of the Assembly Test is to verify that related components function properly when assembled into an overall system.

Performance Test establishes a baseline of acceptable performance for a sample of online transactions. The tests are conducted under a practical proportion of expected transaction and user volumes to mimic real-world usability. The sample is based upon mocked up data entered into the solution. The approach taken will ensure testing against empty databases. The number, frequency, and concurrency of online user transaction load will be defined using the most recent Contractor team estimates of activity available at the time of test preparation. The estimates will be based on enterprise-wide usage (as opposed to usage of only the Initial Release Agencies).

The Contractor will recommend a Test Moves to Production strategy as appropriate for their solution's environment(s). The contractor will demonstrate to the State that the strategy allows for the development and testing of a migration process and checklist, as well as an assessment of timing and any mitigation or resolution of any issues related to timing.

Throughout the Project duration, if a testing or production incident is due to errors, omissions, documentation inconsistencies, or bugs in an "in-scope" environment, supported server, or "in-scope" software element licensed by a Third Party to the State, the Contractor will assist the State by referring such incident to the appropriate Third Party entity for resolution and coordinating with the Third Party contractor, as appropriate, to help minimize the State role in problem management.

The Contractor will, to the extent possible, implement measures to help avoid unnecessary recurrence of incidents, by performing root cause analysis and event correlation for items discovered during testing/validation activities.

9.17 Deploy Phase Requirements (for each Pilot Agency)

A Test Completion Checkpoint must be successfully completed prior to beginning the Deploy phase. This includes the State's acceptance of all deliverables due to date per the project schedule.

The Contractor Team will support the deployment activities and will conduct a deployment readiness assessment to determine the readiness of the organization and the solution for go-live. Part of the readiness review will be to determine that the State has reviewed and accepted all functional, technical, and user documentation. Upon completion of the readiness assessment, the State will make a final go-live decision. The go-live date will be scheduled and resources, roles, and responsibilities will be confirmed.

Key Tasks	State	Contractor
Identify deployment readiness criteria, critical path, and contingency plan	Support	Perform
Assess deployment readiness	Support	Perform
Define stabilization approach and plan	Support	Perform
Perform deployment activities	Support	Perform
Define end user security mapping and assignments for new or altered functionality	Perform	Support
Create production deployment plan	Support	Perform
Create detailed task lists and work plans for deployment	Support	Perform
Create production deployment staffing schedule	Support	Perform

Create production deployment roles and responsibilities	Support	Perform
Perform cutover activities	Support	Perform
Support technical environments, including patches and fixes	Support	Perform
Coordinate PAC items for Deployment	Perform	Support
Deploy the Solution	Support	Perform
System Turnover	Support	Perform

The Contractor Team will drive the planning and execution for the system deployment activities. Deployment includes coordination of software deployment to the file server elements, identification of interfaces and any required conversions/migrations, installation and testing of any required middleware products, installation of server software, and any required testing to achieve the proper roll-out of the application software.

The Contractor Team will execute the deployment plan, which will describe the plan to manage the go-live. The tasks and activities to be performed include the following:

- Execute required data conversions or migrations as applicable;
- Perform required data matching activities and error reporting as applicable;
- Document data issues and provide to the State for resolution as applicable;
- Compile and maintain solution issue lists;
- Produce an end-to-end final validation of the operational architecture and corresponding operational documentation for the upgraded and implemented modules;
- Conduct quality and progress reviews with appropriate State personnel;
- Develop, and thereafter maintain and make available to the State, a knowledge base of documentation gathered throughout the Project's life and allow for re-use of such within the State for future Project Phases or upgrades; and
- Transition solution support responsibility according to the Deployment & Stabilization Plan.

The production deployment schedule will be agreed upon mutually by the State and the Contractor.

Production migration activities will adhere to the State Production Acceptance Criteria (PAC) and will not be considered for production migration until all such criteria are met or otherwise accepted by the State. Any deviation, partial acceptance or waiver of requirements in the Production Acceptance Criteria must be agreed to in writing by the State in advance of presentation of any deliverables associated with, or determined to be part of these Production Acceptance Criteria.

Throughout the Project, Application and Tools patches and fixes will be reviewed. Patches will be applied until the QA environment is established. After the QA environment is established and prior to Go-Live, any Application or Tools related patches and fixes will be evaluated for implementation based on the criticality of the patch or fix.

9.18 Knowledge Transfer and Production Handoff

The Contractor will perform knowledge transfer support to the State in keeping with State Production Acceptance Checklist (PAC) process, which will be made available to the Contractor at the commencement of the project to support knowledge transfer to the State. In general, the PAC will include, at a minimum the following work products as a deliverable:

Deliverable 049. Production Acceptance Checklist

The PAC Deliverable will include, at a minimum:

- Final Requirements Traceability Matrix for the Project as Implemented;
- A list of all customizations and objects as implemented;

- Detailed System Test Cases and Demonstration of Successful Completion of Same;
- Detailed Performance Testing Results showing at least one high volume process (e.g., a Fiscal Quarter or Year or Seasonal Processing as mutually agreed);
- Completion of State User Acceptance Testing and an affirmation of same by State;
- Operational Readiness Testing Results and an affirmation of same by State;
- Complete User and System Administration Documentation that represent the system as implemented; and
- Complete operational documentation sufficient for the State or the State's managed service vendor to operate and maintain the system in the State's environments inclusive of Production, DR, Demo/Train and at least one non-Production replica of the system as delivered.

9.19 Project Completion Activities, Final Documentation and System Acceptance Support Obligations

Following ninety (90) calendar days of successful execution (defined as no Priority 1 or 2 issues) by the Contractor to the State production environment, the Contractor shall submit the system for acceptance. During the 90-day period immediately following the introduction of the Contractor provided enhancements, configurations or extensions to the State's production environment the Contractor must:

- Ensure adequate staffing from the Contractor Project Team is on hand (or available remotely) to ensure that during this 90-day period all defects identified by the State and mutually committed to resolve by the Contractor in this RFP or any approved changes to the Contract are adhered to.
- This responsibility shall specifically include:
  - Prompt isolation, triage and repair of any Priority 1 or 2 issues;
  - Performance Monitoring of the System to ensure that there are no statistically significant (i.e., +5%) deviations from actual production performance as compared to the system performance prior to the implementation of Contractor developed elements;
  - All interfaces, and system functions perform and function as specified;
  - Compile all final versions of the upgrade documentation, work products and delivery materials and locate / organize them as 'FINAL' on the State provided SharePoint site; and
  - Obtain a final system acceptance document from the State confirming that all of the above has been delivered and accepted as final.

If, during the 90-day period immediately following the introduction to Production, a Priority 1 or 2 issue occurs that can be directly attributable to the efforts of the Contractor, and not the State or other non-Project parties. The 90-day period will, at the sole discretion of the State, be reset for additional 90-day periods, until such time as the system can perform without Priority1 and 2 issues.

Deliverable 050. Project Completion Certification

9.20 Future Project Services Pricing Response and Rate Card

Offerors must provide a Rate Card, by project personnel role and experience level as well as Technical role and experience level that is binding over the Contract term. The Contractor may not propose rates (blended or otherwise) in any Project SOW that differ from this rate card as allowed under any contract arising from this RFP.

10.0 Schedule of Deliverables and Work Products

To support the execution of the Project and provide supporting follow-on documentation, the Contractor will create and deliver to the State the following set of Deliverables and Work Products. The State Project Lead will serve as

the representative for coordinating respective internal reviews of the subject Deliverable(s) and Work Products for sign off by the State. The Offeror may recommend modifications or propose other deliverables based on their solution or methodology characteristics. Any differences proposed to the ones listed below must include an explanation in the Offeror's response.

10.1 Delivery and Deliverable Standards

- The Contractor will define, document and submit all standards they intend to utilize in the performance of this project. Once the State approves these standards, variances to the standards must be approved by the State prior to implementation of other than standard practices.
- The Contractor's work and deliverables will be in accordance with the contractor's standards (e.g., SDLC, project management, etc.).

10.2 Schedule of Key Project Management Deliverables and Work Products

Name	Key Project Management Deliverable / Work Product Descriptions	Phase
Kickoff Meeting Presentation	Documents the governance for the Project, roles, approach, timeline, and deliverables in a presentation format and presents to the Project team.	Analyze
Project Execution Methodology	This is a detailed description of their project management approach as well as the requirements gathering and analysis, design, build, test, deploy and run methodologies the contractor follows, standards the contractor intends to apply to this project, and any applicable tool sets. Contractor must address topics such as: • Financial Controls • Risk and Issue Management • Resource Management • Change Control • Configuration Management • Development Methodology • Test Methodology	Analyze
Work Breakdown Structure (WBS)	This document is a hierarchical decomposition of the project into phases, deliverables and work packages. In the work breakdown structure supplied, sufficient detail needs to be presented and maintained over the course of the project to track the earned value against the proposed costs and work efforts. This WBS will be reflected in the Project Work Plan.	Analyze
Resource Plan	The resource plan must specify resources required, by type, over the duration of the project. Contractor must identify all required resources (Contractor, State or otherwise) to complete the project, except where otherwise specified in this document, and include all costs for those resources that are to be provided by the Contractor. Sample roles should be inclusive of Developers, Business Analyst, Administrator, Security Analyst, Database Administrator, or any other roles deemed necessary by the Contractor. The contractor will specify the percent of time the each resource will perform their role on State premises.	Analyze
Organization Structure	This is an org structure reflecting a high-level org structure that incorporates both Contractor and State resources. Roles to address may include any of the following: • Sponsors and Stakeholders • Project Management • Quality Assurance • Team Structure and Leads	Analyze
Project Workplan	Documents the tasks required to complete the Project, the responsible party for the task, task dependencies, and the resources, duration and work hours required. This plan should include key milestones and phases. The project work plan should be in an acceptable format for the State (e.g., MS Project). The contractor's project manager will work with the State's project manager to ensure an acceptable Project Work Plan is completed and accepted as baseline within 20 business days after the Kickoff Meeting.	Analyze
Change Control Approach	This document must explain the approach for performing change control. This must also include the required communications and coordination points for properly obtaining sign-offs and authorizations.	Analyze

Name	Key Project Management Deliverable / Work Product Descriptions	Phase
Requirements and Process Analysis	Documents the results of the requirement and business process analysis and workshop sessions in spreadsheet format, specifically: • All recommended changes to the State's original functional requirements and State processes and rationale for the changes. • For each business process gap analyzed, list the functional requirement, standard functionality of the appropriate component of the solution, options to meet the requirement and recommendation	Analyze
Gap Analysis	Report documenting gaps between propose solution and requirements, as well as potential solution options to resolve the gaps.	Analyze
Business Processes & Requirements	The State's identity management business processes modified as applicable. The State's functional requirements modified as applicable. In addition, include analysis identifying data migration needs from external systems during deployment	Analyze
Requirements Traceability Matrix	Lists the requirements for the processes, which will be designed and/or built and subsequently tested and deployed. This deliverable will be revised and updated and will be due at each phase check point or as defined in the agreed upon project work plan.	Analyze
Integration Points Analysis	Defined integration points with external systems to include data analysis, potential for data migration required for deployment and any impacts within the external system.	Analyze
Customization Tracking Database	This database will track customizations to any commercially developed component of the solution. It will include assessment of the impact to the lifecycle ownership of the component as a result of the customization (e.g., voided warranties, impacts with respect to future commercially available upgrades, patches, etc.).	Analyze
Solution Architecture	This document defines the application architecture that is to be used during the project and contains the solution architecture (logical and physical). This architecture must show all components and how various systems interrelate, including the external technical environment the solution will operate within.	Analyze
Capacity Plan	This plan includes the results of the process of determining the operational capacity the solution needs to achieve in order to satisfy the business process demands of the system. It should include planning through the accomplishment of the State's long-term goal of the solution supporting all identity Management within the State, including sub recipient management, sub recipient needs, etc. This document(s) specifies by phase and system the sizing, CPU, and memory requirements.	Analyze
Technical Requirements	All recommended changes to the State's original technical requirements and rationale for the changes. These requirements should be elaborated upon as required to support the development of the technical specification and design.	Analyze
Technical Environments Requirements	The identification of all technical environments and the associated requirements, inclusive of all technical environments to be used for the project from the Build Phase through Test, Deploy and Run.	Analyze
Communicatio n Plan	This specifies typical project stakeholders, communication frequency, and communications vehicles. It must also include the approval process for communications, and how the approval process may differ based on target audience.	Analyze
Training Needs Analysis	Identifies the training needs that the target audiences affected by the Project require. Primarily highlights the following: • Areas that are changing • Who is affected by the change • Desired level of knowledge and skills expected after the training • Importance or priority of each of the identified processes to the business	Analyze
Readiness Plan	Agency/Stakeholder Readiness Plan: Outlines the approach that will be taken to track end user adoption and readiness for the proposed solution, including business process change.	Analyze
Knowledge Transfer Plan	A plan defining the activities and roles required to perform knowledge transfer of the operations and support of the solution.	Analyze
Checkpoint Report – Analyze	Documents any difference in the Project scope, schedule, and/or resources at or before the end of the Analyze Phase. The focus of this deliverable will be on the scope of the solution. Also indicates any deliverables, which have not been accepted by the State per the Work Plan.	Analyze

Name	Key Project Management Deliverable / Work Product Descriptions	Phase
Functional Design	Functional design of the solution. Includes the Systems Requirements Document: systems specifications and functional requirements including reliability, performance, operations, usability, maintainability and functional specifications for any interfaces to external systems.	Design
Security Design	Documents the details of the approach that will be followed to meet the identified security requirements of the Sate.	Design
Technical Design	Documents the technical specifications for the solution to include: • Data definitions, identifying any new data elements and classifying new data to be added to the list of confidential and sensitive data. • Unit Test scripts – including both normal and exception processing • Changes to technical architecture • Interfaces to external systems • Any customizations if applicable. • Data Migration from external systems at deployment, if applicable.	Design
Test Strategy	This is the overall test strategy which includes: • Tests to be completed • Test environments • Test tools • Defect tracking • Test approach	Design
Deployment Plan	Documents the solution deployment approach.	Design
Technology Environments – Build Test	Establish the Technology Environments for Build and Test.	Design
Checkpoint Report – Design	Documents any difference in the Project scope, schedule, and/or resources at or before the end of the Design Phase. The focus of this deliverable will be on the scope of the solution. Also indicates any deliverables which have not been accepted by the State per the Work Plan.	Design
Master Test Plan	This document the plan, scripts (including expected results) and schedule required to execute the various tests phases, including but not limited to System Test, User Acceptance Test, and Performance Test.	Build
Technology Environments	Establish all remaining Technology Environments as defined in the Technical Environments Requirements.	Build
Build and Unit Test Results	Provide build documentation (i.e., changes to code) as a result of unit tests conducted during the Build phase.	Build
Deployment Plan	The plan for deployment of the solution, including tools, readiness criteria and cutover activity list (as applicable).	Build
Training Materials	This includes all training materials and all mediums.	Build
Training Deployment Plan	Documents the plan for rolling out the training to end-users. The Training Deployment Plan lists all the tactical activities that need to occur as training gets rolled out to end-users.	Build
Checkpoint – Test Readiness Review	Documents any difference in the Project scope, schedule, and/or resources at or before the end of the Design Phase. This checkpoint report will focus on the readiness for entering the test phase. Also indicates any deliverables, which have not been accepted by the State per the Work Plan.	Build
Deployment Approach	Detailed approach and plan for cutover activities for transitioning the in-scope processes into production. Includes: • Deployment preparation • Cutover planning • Stabilization planning for Post Go-Live support.	Test

Name	Key Project Management Deliverable / Work Product Descriptions	Phase
Deployment & Stabilization Plan	The plan will cover the timeframe forty-five (45) calendar days before Go-Live and thirty (30) calendar days after Go-Live. This document must identify the series of tasks to be performed in the appropriate sequence to ensure production readiness. This plan must also explain the approach for business continuity during and after cutover. The plans will detail the following for each task: • Task name • Owner • Target date for completion • Critical path indicator • The type of tasks will include: • Knowledge transfer/training tasks • Operational cutover tasks (i.e., converting data, etc.) • Publish revised policies and procedures • Technical Architecture tasks including readiness, mock deployments and production cutover • Post Go-Live support tasks • Approach for the project team to hand-over long term support to the run support team	Test
Data Migration Checklist	Create a data migration checklist.	Test
Data Migration	Test the migration of data from external systems and use the data during testing as applicable.	Test
System Test Results	These documents are the presentation of the results from a particular testing Phase inclusive of substantiation of Contractor testing of all elements as required by the State and contained in the requirements traceability matrix.	Test
Performance Test Results	Documents the results of Performance Test and establishes new performance baselines.	Test
User Acceptance Test Results	These documents are the presentation of the results based on the State's completion of acceptance testing of the Contractor developed upgrade elements. The Contractor will facilitate this deliverable and include identification, classification (i.e., Priority 1-3), and the prioritization of fixing all defects based on State UAT efforts.	Test
Operational Readiness Test Results	Documents the results of the Operational Readiness Test.	Test
Trainer Training	Delivery of training to State's Trainers or Technical Staff as appropriate.	Test
Checkpoint – Test Completion Report	This checkpoint report will focus on the readiness for exiting the test phase and entering the Deploy Phase. Also indicates any deliverables, which have not been accepted by the State per the Work Plan.	Test
Training Delivery	Completion of the delivery of training per the Training Deployment Plan.	Deploy
System Deployed	This is the acceptance of the State deployment checklist for Production and Non-Production environments.	Deploy
System Turnover	Transition solution support responsibility per the Deployment & Stabilization Plan. This includes Knowledge Transfer Activities per the Knowledge Transfer Plan.	Deploy

11.0 Assumptions

The Offeror must list all the assumptions the Offeror made in preparing the Proposal. If any assumption is unacceptable to the State, the State may at its sole discretion request that the Offeror 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 Offeror response as a stand-alone response section that is inclusive of all assumptions with reference(s) to the section(s) of the RFP that the assumption is applicable too. **Offerors should not include assumptions elsewhere in their response.**

11.1 Support Requirements

The Offeror must describe the support it wants from the State other than what the State has offered in this RFP. Specifically, the Offeror must address the following:

- Nature and extent of State support required in terms of staff roles, percentage of time available, and so on;
- Assistance from State staff and the experience and qualification levels required; and
- Other support requirements.

The State may not be able or willing to provide the additional support the Offeror lists in this part of its Proposal. The Offeror therefore must indicate whether its request for additional support is a requirement for its performance. If any part of the list is a requirement, the State may reject the Offeror's Proposal, if the State is unable or unwilling to meet the requirements.

11.2 Pre-Existing Materials

The Offeror must list any Pre-Existing Materials it owns that will be included in a Deliverable if the Offeror wants a proprietary notice on copies that the State distributes. For example, the Offeror may have standard user interfaces or standard shells that it incorporates in what is otherwise custom software. (See the Ownership of Deliverables section of the General Terms and Conditions.) The State may reject any Proposal that includes existing materials for a custom solution, if the State believes that such is not appropriate or desirable for the Project.

11.3 Commercial Materials

The Offeror must list any commercial and proprietary materials that the Offeror will deliver that are easily copied, such as Commercial Software, and in which the State will have less than full ownership ("Commercial Materials"). Generally, these will be from third parties and readily available in the open market. The Offeror need not list patented parts of equipment, since they are not readily copied. If the Offeror expects the State to sign a license for the Commercial Material, the Offeror must include the license agreement as an attachment. If the State finds any provisions of the license agreement objectionable and cannot or does not negotiate an acceptable solution with the licensor, regardless of the reason and in the State's sole discretion, then the Offeror's Proposal may be rejected. If the State is not going to sign a license, but there will be limits on the State's use of the Commercial Materials different from the standard license in the General Terms and Conditions, then the Offeror must detail the unique scope of license here. Unless otherwise provided in this RFP, proposing to use Commercial Materials in a custom solution may be a basis for rejection of the Offeror's Proposal, if the State, in its sole discretion, believes that such is not appropriate or desirable for the Project. Any deviation from the standard license, warranty, and other terms in Attachment Four also may result in a rejection of the Offeror's Proposal.

If the Offeror proposes a Deliverable that contains Commercial Software or other Commercial Materials with terms that differ from the terms in Attachment Four for Commercial Software and Materials, then those terms must be detailed here, and any proposed separate agreement covering those items must be included in the Offeror's Proposal. This is required even if the State will not be expected to sign the agreement. Any deviation from the standard terms in Attachment Four may result in a rejection of the Offeror's Proposal.

12.0 State Staffing Requirements

The State will provide oversight for the Project, but the Contractor must provide overall Project management for the tasks under this Contract, including the day-to-day management of its staff. The Contractor also must assist the State with coordinating assignments for State staff, if any, involved in the Project. Additionally, the Contractor must provide all administrative support for its staff and activities. Throughout the Project effort, the Contractor must employ ongoing management techniques to ensure a comprehensive Project Plan is developed, executed, monitored, reported on, and maintained.

The Contractor must provide a Project Manager for the Work. The Contractor must employ the proposed Project Manager as a regular, fulltime employee on the Proposal submission date and throughout the term of the Contract, including all renewals. Additionally, the Contractor's full-time regular employees must perform at least 30% of the effort required to complete the Project. The Contractor may use its personnel or subcontractor personnel to meet the remaining 70% of the effort.

As this project is an Enterprise offering supported by DAS/OIT and includes Agency participation in the Pilot Projects identified herein, the following table represents the State's minimum commitments to this Project. Should, based on the experience of the Offeror additional roles be required of the State, the Offeror will identify these roles, provide rationale and include a summary description of the skills and competencies required for each position. Note all roles (State minimum or otherwise) must be included in the Offeror Staffing Plan as required in this section of the Supplement. For all State roles marked "as required" Offerors are to include (within their proposal) the staffing level required of the State to ensure that the Contractor project is supported adequately.

The State will provide a dedicated State Project Lead (Project Representative) to serve as the Contractor's day-to-day point of contact for the Project. This role will be staffed throughout the duration of the Project. The State Project Lead will facilitate process and policy decisions in support of the Project schedule. State personnel assigned to the Analyze Phase will maintain consistent involvement throughout the duration of the Project. These individuals will be accessible and available to participate as agreed upon in the approved Project Plan.

Project Area	State Identity Core Team (DAS/OIT)	Pilot Projects		
		Enterprise eLicensing Platform	Ohio Business Gateway	Department of Taxation
Overall Project Management	1 FTE	-	-	-
State Standards Lead: State Policy and IT Standards	1 PTE as required (advisory)	-	-	-
Security Advisor (State CISO Office)	1 FTE (design phases), part-time advisory thereafter	-	-	-
Privacy Advisor (State CIPO Office)	1 FTE (design phases), part-time advisory thereafter	-	-	-
Security/Privacy SME	Up to 1 FTE As required	-	-	-
Functional Lead	-	1 PTE As Required	1 PTE As Required	1 PTE As Required
Technical Lead	-	1 PTE As Required	1 PTE As Required	1 PTE As Required
Integration Lead	-	1 PTE As Required	1 PTE As Required	1 PTE As Required
State SEIM Integration and Reporting	Up to 1 FTE As required	-	-	-
System Test Lead	As required	As Required	As Required	As Required
System Test Participants	As required	As Required	As Required	As Required
State Infrastructure Liaisons	Up to 4 PTE (Network, Server, Storage, Directory) as required	-	-	-

12.1 Contract Staffing and Key Activities

The offeror is to consider the roles provided by the State as well as those proposed that are required for the Pilot Phase of the Project based upon the details, the key activities, proposed time commitments required for each role, and the percent of the proposed time the role will be on the State's premises performing work. The offeror, as part of their response will identify all roles that are required to be performed (by phase), the work location(s) for the team and identify requirements for performing these roles off-site at a Contractor location or on State's Premises (e.g., Project Manager, business analysis, technical lead, functional lead, etc.). Offerors are to propose a combined team organization (i.e., State and Contractor) designed to deliver the project to the State as per the requirements in this Supplement.

Offeror Team Organization, Key Personnel and Work Location(s) – Pilot Phase (Overall and Per Pilot)

Role #	Contractor Role	Role Activity	FT/PT	% Time On Site
Analyze Phase				
		[insert rows as required]		
Design Phase				
		[insert rows as required]		
Build Phase				
		[insert rows as required]		
Test Phase				
		[insert rows as required]		
Deploy Phase				
		[insert rows as required]		
Post Implementation Support				
		[insert rows as required]		

12.2 Staffing Plan and Time Commitment

The offerors Staffing Plan and Time Commitment response must include the following information:

- An organizational chart including any subcontractors and key management and administrative personnel assigned to this project.
- A contingency plan that shows the ability to add more staff if needed to ensure meeting the Project's due date(s).
- The number of people onsite at State location(s) at any given time to allow the State to plan for the appropriate workspace. **Offeror Note:** The following table is provided as an ***example*** of what the State expects the offeror to provide in the proposal response for this requirement.

Illustrative Offeror Staffing Plan

Project Month	1	2	3	4	5	6	7	8	9	10	11
Phase	Startup / Analyze		Design Phase		Build Phase		Test Phase		Deployment		Operate
Project Management											
State	3	3	3	3	3	3	3	3	3	3	3
Contractor	2	2	2	2	2	2	2	2	2	2	2
Functional FTEs											
State	4	4	4	4	4	4	4	4	4	4	4
Contractor	8	8	8	8	8	8	8	8	8	8	8
Technical FTEs											
State Infrastructure	2	2	2	2	2	2	2	2	2	2	2
State Security	1	1	1	1	1	1	1	1	1	1	1
Contractor	6	6	6	6	6	6	6	6	6	6	6
Business / Agency FTEs											
State	4	4	4	4	4	4	4	4	4	4	4
Contractor	2	2	2	2	2	2	2	2	2	2	2
Summary Total											
State	14	14	14	14	14	14	14	14	14	14	14
Contractor	18	18	18	18	18	18	18	18	18	18	18

Offerors are encouraged to add additional roles and responsibilities as appropriate based on their proposed Project Staffing Plan as to highlight the involvement of their Proposed Team and inclusion of State resources in the project to help ensure its success. The number of FTEs depicted in the above table is provided as an **illustrative example** and in no way connotes State expectations as to the level or involvement of the State or Contractor in this project.

The offeror must include:

- A statement and a chart that clearly indicate the time commitment of the proposed Project Manager, the offeror's Key Project Personnel, and the offeror's proposed team members for this Work during each phase of the Project, the System Development Life Cycle associated with Project, and the commencement and ongoing operations.

- A statement indicating to what extent, if any, the candidates may work on other projects or assignments that are **not** State related during the term of the Contract. The State may reject any Proposal that commits the proposed Project Manager or any proposed Key Project Personnel to other projects during the term of the Project, if the State believes that any such commitment may be detrimental to the offeror's performance.

In addition, the offeror's proposal must identify all Key Project Personnel who will provide services as part of the resulting Contract. The Key Project Personnel are identified in each applicable Supplement. The State expects that the proposed named Key Project Personnel will be available as proposed to work on the Project. Resumes for the proposed candidates must be provided for all Key Project Personnel. Representative resumes are **not** acceptable. The resumes will be used to supplement the descriptive narrative provided by the offeror regarding their proposed project team.

The resume (2-page limit per resume) of the proposed Key Project Personnel must include:

- Proposed Candidate's Name
- Proposed role on this Project
- Listings of competed projects (a minimum of two references for each named Key Project Personnel) that are comparable to this Project or required similar skills based on the person's assigned role/responsibility on this Project. Each project listed should include at a minimum the beginning and ending dates, client/company name for which the work was performed, client contact information for sponsoring Directors, Managers or equivalent level position (name, phone number, email address, company name, etc.), project title, project description, and a detailed description of the person's role/responsibility on the project.
- Education
- Professional Licenses/Certifications/Memberships
- Employment History

12.3 Background Checks

All Contractor and subcontractor personnel assigned to the Identity Validation, Authentication and Fraud Services Project who have access to sensitive or confidential information or to sensitive State systems must have a current fingerprint search and background check performed by the Federal Bureau of Investigation or other Federal investigative authority. The fingerprint search and background checks must be completed before any such Contractor or subcontractor personnel gain access to State facilities, sensitive and/or confidential information or systems. All costs associated with this requirement will be at the Contractor's expense. At its discretion, the State may reject any Contractor or subcontractor personnel based on the information provided in the completed background check.

The offeror must confirm in their Proposal that all Contractor and subcontractor personnel assigned to the Project will have Background Checks completed before Project Start or before reporting to State designated Project facilities.

13.0 Service Level Requirements: Identity Proofing & 2FA Service Providers

The following Service Levels shall apply to Service Providers providing either or any of Identity Proofing services (as described in Section 4.0 of this Supplement); Two Factor Authentication Services (as described in Section 7.0); and Fraud Detection Solutions (as described in Section 8.0).

13.1 Service Availability

Service Availability for each in-scope element provided by the Service Provider that the State utilizes in Production to support State system operations, as well as the ongoing development and maintenance of the system inclusing training and demonstration or supporting non-non production usage shall be subject to these Service Levels.

Standard: 99.5% available, 24 hours per day, 365 days per year less mutually agreed to scheduled maintenance windows not to exceed one hour per month.

13.2 Priority 1 Outage Resolution Time

Priority 1 Outage means that there is a Critical Function outage causing severe impact on service delivery and no alternative or bypass is available. The Service Provider will provide notice of Priority 1 incidents along with a preliminary diagnosis and estimated resolution time within 15 minutes of detecting the Incident or being informed by the State of such outage.

A severe impact means: the Incident renders a business critical function, System, Service, Software, Equipment or network component un-Available, substantially un-Available or seriously impacts normal State operations, in each case prohibiting the execution of productive work.

Standard: Detection of Outage and Reporting to State estimated time of resolution: 15 Minutes, resolution of outage and return to contracted standards within 60 minutes.

13.3 System Performance and Timeliness

System performance shall be measured by the Service Provider and be subject to demonstration to the State for auditing and verification purposes upon the request of the State. System performance shall meet the following standards:

Standard: Online Identity Verification Services shall be returned (allowing for network transit time) from origination by the State to the return of a properly formatted system response message within five (5) seconds for at least 99% of all properly formatted State transactions during available hours.

Standard: Offline Identity or Attributed Verification Services shall be returned (allowing for network transit time) from origination by the State to the return of a properly formatted system response message within sixty (60) minutes for at least 99% of all properly formatted State transactions provided to the Service Provider.

Standard: Online Two Factor Authentication Services shall be returned (allowing for network transit time) from origination by the State to the return of a properly formatted system response message within five (5) seconds for at least 99% of all properly formatted State transactions during available hours.

Standard: Online Fraud Detection Service alerts shall be remanded to the State (allowing for network transit time) from identification of actual or suspected fraudulent access within fifteen (15) seconds of detection for at least 99% of all fraudulent accesses detected.

13.4 Service Level Specific Performance Credits

Failure to meet any Service level contained in this Section in a given month shall result in a 5% fee credit of the total monthly charges to the State for the Service reporting month following the observation of an **incident** identified by the State or Service Provider failure to meet the contracted Standard(s).

14.0 Service Level Requirements: State Systems Integration Projects

This section sets forth the performance specifications for the Service Level Agreements (SLA) and Service Level Objectives (SLO) to be established between the Contractor and the State that are applicable to any work associated with the development, configuration, extension or implementation of any software (asset or cloud-based) associated with this Supplement in general, and under Section 5.0 specifically as the work pertains to any Agency Pilots or subsequent or Additional Work for State Agencies.

The section contains the tables and descriptions that provide the State framework, requirements relating to service level commitments, and the implications of meeting versus failing to meet the requirements and objectives, as applicable. This document defines the State's detailed performance, management, and reporting requirements for the Project Implementation and to all subsequent Project related services and phases that are contracted under future Statements of Work between the State and the Contractor related to this RFP.

The mechanism set out herein will be implemented to manage the Contractor's performance against each Service Level, in order to monitor the overall performance of the Contractor.

The Contractor will be required to comply with the following performance management and reporting mechanisms for all Services within the scope of this RFP and will provide these reports to the State on no less than a monthly basis:

- **Service Level Specific Performance** – Agreed upon specific Service Levels to measure the performance of specific Services or Service Elements. Most individual Service Levels are linked to financial credits due to the State ("Performance Credits") to incent Contractor performance.
- **Overall Contract Performance** – An overall performance score of the Contractor across all Service Levels. The overall performance score is linked to governance and escalation processes as-needed to initiate corrective actions and remedial processes.

14.1 Service Level Specific Performance Credits

Each Service Level (SL) will be measured using a "Green-Yellow-Red" traffic light mechanism (the "Individual SL GYR State"), with "Green" representing the highest level of performance and "Red" representing the lowest level of performance. A Performance Credit will be due to the State in the event a specific Individual SLA GYR State falls in the "Yellow "or "Red" state. The amount of the Performance Credit for each SLA will be based on the Individual SLA GYR State. Further, the amounts of the Performance Credits will, in certain cases, increase where they are imposed in consecutive months. No Service Level Performance Credit will be payable for the Contractor's failure to meet a Service Level Objective.

Set forth below is a table summarizing the monthly Performance Credits for each SLA. All amounts set forth below that are contained in a row pertaining to the "Yellow" or "Red" GYR State, represent Performance Credit amounts.

Consecutive (SLA Performance Credits)												
Individual SL GYR State	1st Month	2nd Month	3rd Month	4th Month	5th Month	6th Month	7th Month	8th Month	9th Month	10th Month	11th Month	12th Month
Red	A =1.71% of MPC	A + 50% of A	A + 100% of A	A + 150% of A	A + 200% of A	A + 250% of A	A + 300% of A	A + 350% of A	A + 400% of A	A + 450% of A	A + 500% of A	A + 550% of A
Yellow	B = 0.855% of MPC	B + 50% of B	B + 100% of B	B + 150% of B	B + 200% of B	B + 250% of B	B + 300% of B	B + 350% of B	B + 400% of B	B + 450% of B	B + 500% of B	B + 550% of B
Green	None	None	None	None	None	None	None	None	None	None	None	None

The Contractor agrees that in each month of the Contract, 12% of the monthly project charges (MPC) associated with the Project Implementation portion of this RFP will be at risk. MPCs are the charges for the deliverables accepted during a given month. The MPC for the Project Implementation will be at risk for failure to meet the Service Levels set forth in the Contract. The Contractor will not be required to provide Performance Credits for multiple Performance Specifications for the same event; the highest Performance Credit available to the State for that particular event will apply.

On a quarterly basis, there will be a “true-up” at which time the total amount of the Performance Credits will be calculated (the “Net Amount”), and such Net Amount will be set off against any fees owed by the State to the Contractor.

Moreover, in the event of consecutive failures to meet the Service Levels, the Contractor will be required to credit the State the maximum Performance Credit under the terms of the Contract.

The Contractor will not be liable for any failed Service Level 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 immediately 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 possible.

For example, if an Individual SL GYR State is Yellow in the first Measurement Period, Red in the second Measurement Period and back to Yellow in the third Measurement Period for an SLA then the Performance Credit due to the State will be the sum of Yellow Month 1 (B) for the first Measurement Period, Red Month 2 (A + 50% of A) for the second Measurement period, and Yellow Month 3 (B + 100% of B) for the third Measurement period, provided (1) such Performance Credit does not exceed 12% of the MPC (the At-Risk Amount); and, (2) no single Service Level Credit will exceed 20% of the total At-Risk Amount, as stated below:

SLA Calculation EXAMPLE						
Monthly Project Charge (MPC) = $290,000.00						
Monthly At Risk Amount = 12% of MPC = $34,800						
Maximum for any one SLA = 20% of At Risk Amount = $6,960						
GYR State	1st Month		2nd Month		3rd Month	
Red	0	$	0	$7,438.50	0	
Yellow	1	$2,479.50	1		1	$4,959.00
Green	6	$	6		6	
Totals	7	$2,479.50	7	$7,438.50	7	$4,959.00
Adjusted Totals by At Risk Amount and 20% per individual SLA Limitations	(Is monthly total of all Service Level Credits equal to or less than $34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than $ 6,960?) - Yes $2,479.50		(Is monthly total of all Service Level Credits equal to or less than $34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than $ 6,960?) - No $6,960.00		(Is monthly total of all Service Level Credits equal to or less than $34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than $ 6,960?) - Yes $4,959.00	
Total Quarterly Credit:	$ 2,479.50 +		$ 6,960.00 +		$ 4,959.00	
Total Quarterly Credit: $ 14,398.50						

Service Level Performance Credit payable to the State = (B) + (A + 50% A) + (B + 100% B), based on an illustrative MPC of $290,000;

The total of any weighting factors may not exceed 100% of the total At-Risk Amount. 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. Service Levels will commence with Project initiation for any Implementation Project.

14.2 Overall Contract Performance

In addition to the service specific performance credits, on a monthly basis, an overall SL score (the "Overall SL Score") will be determined, by assigning points to each SL based on its Individual SL GYR State. The matrix set forth below describes the methodology for computing the Overall SL Score:

Individual SLAs and SLOs GYR State	Performance Multiple
Green	0
Yellow	1
Red	4

The Overall SL score is calculated by multiplying the number of SLAs and SLOs in each GYR State by the Performance Multiples above. For example, if all SLAs and SLOs are Green except for two SLAs in a Red GYR State, the Overall SL Score would be the equivalent of 8 (4 x 2 Red SLAs).

Based on the Overall SL Score thresholds value exceeding a threshold of fifteen (15), mandatory Executive escalation procedures outlined in this RFP will be initiated to restore acceptable Service Levels.

If a successful resolution is not reached, then **the State may terminate the Contract for cause if:**

The overall SL score reaches a threshold over a period of 3 consecutive months with the equivalent of 50% of the service levels in a red state; and the Contractor fails to cure the affected Service Levels within 60 calendar days of receipt of the State's written notice of intent to terminate; **OR**

The State exercises its right to terminate for exceeding the threshold level of 75% of Service levels in total over a six (6) month period.

The Overall Contract Performance will not constitute the State's exclusive remedy to resolving issues related to the Contractor's performance. The State retains the right to terminate for Overall Contract Performance under the terms of this Contract.

14.3 Monthly Service Level Report

On a State accounting monthly basis, the Contractor will provide a written report (the "Monthly Service Level Report")to the State which includes the following information: (i)the Contractor's quantitative performance for each Service Level; (ii) each Individual SL GYR State and the Overall SL Score; (iii) the amount of any monthly Performance Credit for each Service Level (iv) the year-to-date total Performance Credit balance for each Service Level and all the Service Levels; (v) a "Root-Cause Analysis" and corrective action plan with respect to any Service Levels where the Individual SL GYR State was not "Green" during the preceding month; and (vi) trend or statistical analysis with respect to each Service Level as requested by the State . The Monthly Service Level Report will be due no later than the tenth (10th) accounting day of the following month.

Failure to report any SLA, SLA performance in a given month or for any non-Green (i.e., performing to Standard) SLA a detailed root cause analysis that substantiates cause will result in the State considering the performance of the Contractor for that period as performing in a Red State.

14.4 Service Level Commitments – Project Implementation Services

The Contractor will meet the Service Level Commitment for each Service Level set forth in the tables and descriptions below:

Service Level	State Requirements			
	SLA or SLO	Support Hours	Required	
			Response	Resolution
Defect Resolution – Priority 1 Items	**SLA**	7x24	Every 4 hours until resolution	<= 24 hours
Defect Resolution – Priority 2 Items	**SLA**	7x16	Every 8 hours until resolution	<=72 hours
Defect Resolution – Priority 3 Items	**SLO**	5x9	Every 24 hours until resolution	<= 7 calendar days
System Test Execution Exit Quality Rate	**SLA**	-	See specification below	-

Service Level	State Requirements			
	SLA or SLO	Support Hours	Required	
			Response	Resolution
Blocking Issues Identification and Removal	**SLA**	7x24	Every 2 hours until resolution or agreeable workaround is implemented	<=10%%
Regression Testing Performance Issue Find/Fix Rate	**SLA**	-	See specification below	-
Code Coverage – Automated Test Beds	**SLO**	-	See specification below	-
Milestone Date Delivery	**SLA**	-	See specification below	-
Issue Reporting	**SLO**	-	See specification below	-
Deliverable Acceptance	**SLO**	-	See specification below	-
UAT Process and Environment Support	**SLO**	7x9	Every 2 hours until completion of testing effort	-
Development Methodology Compliance– % SDLC Compliance	**SLA**	-	See specification below	-
Development Methodology Compliance – % Build and Testing Activities	**SLO**	-	See specification below	-
Development Methodology Compliance - Issues Detected and Resolved in Production	**SLO**	-	See specification below	-

14.5 Service Level Specifications

14.5.1 Defect Resolution – Mean Time to Repair/Resolve (Priority 1 Items)

Specification: Defect Resolution – Mean Time to Repair/Resolve (Priority 1 Items)

Definition: Mean Time to Repair (Priority 1 Items) will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all Priority 1 Defects for in-scope deliverables in the Contract Month. "Time to Repair" is measured from time and Issue is received at the Contractor Issue/Defect tracking system to point in time when the Defect is resolved or workaround is in place and the Contractor submits the repair to the State for confirmation of resolution.
"Priority 1 Defect Service Request" means an incident where the State's use of a solution service element has stopped or is so severely impacted that the State personnel cannot reasonably continue to work.
This Service Level begins upon Contractor presentation of a deliverable (generally code based) to the State for conducting Acceptance Testing and when this deliverable is initially migrated or otherwise used in a production environment.

Formula:

$$\text{Mean Time to Repair (Priority 1 Outages)} = \frac{\text{(Total elapsed time it takes to repair Priority 1 Defect Service Requests)}}{\text{(Total Priority 1 Defect Service Requests)}}$$

Measurement Period: Month

Data Source: Monthly Project Report

Frequency of Collection: Per Incident

Service Level Measures

Individual SL GYR State	Incident Resolution – Mean Time to Repair (Priority 1 Defects).
Green	**<=24 hours**
Yellow	**>2 4 hours and <= 48 hours**
Red	**>48 hours**

14.5.2 Defect Resolution – Mean Time to Repair/Resolve (Priority 2 Items)

Specification: Defect Resolution – Mean Time to Repair/Resolve (Priority 2 Items)

Definition: Mean Time to Repair (Priority 2 Items) will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all Priority 2 Defects for in-scope deliverables in the Contract Month. "Time to Repair" is measured from time and Issue is received at the Contractor Issue/Defect tracking system to point in time when the Defect is resolved or workaround is in place and the Contractor submits the repair to the State for confirmation of resolution.
"Priority 2 Defect Service Request" means an incident where the State's Software or Processing Error that results in a partial or intermittent system outage or unavailability, performance Items that result in undue delay of processing business cycle data and creation of a processing backlog, System performance and availability levels not adhering to agreed-upon SLAs, the State's traditional performance levels, and generally accepted and customary industry standards for similar functions or capabilities, a temporary workaround identified but due to processing, hardware, labor or other considerations is deemed unreasonable by the State, or may be a recurring issue with identified or indeterminate cause.
This Service Level begins upon Contractor presentation of a deliverable (generally code based) to the State for conducting Acceptance Testing and when this deliverable is initially migrated or otherwise used in a production environment.

Formula:

$$\text{Mean Time to Repair (Priority 2 Outages)} = \frac{\text{(Total elapsed time it takes to repair Priority 2 Defect Service Requests)}}{\text{(Total Priority 2 Defect Service Requests)}}$$

Measurement Period: Accounting Month

Data Source: Monthly Project Report

Frequency of Collection: Per Incident

Service Level Measures

Individual SL GYR State	Incident Resolution – Mean Time to Repair (Priority 2 Defects).
Green	**<= 72 hours**
Yellow	**> 72 hours and <= 90 hours**
Red	**> 90 hours**

14.5.3 Defect Resolution – Mean Time to Repair/Resolve (Priority 3 Items)

Specification: Defect Resolution – Mean Time to Repair/Resolve (Priority 3 Items)

Definition: Mean Time to Repair (Priority 3 Items) will be calculated by determining time (stated in hours and minutes) representing the statistical mean for all Priority 3 Defects for in-scope deliverables in the Contract Month. "Time to Repair" is measured from time and Issue is received at the Contractor Issue/Defect tracking system to point in time when the Defect is resolved or workaround is in place and the Contractor submits the repair to the State for confirmation of resolution.
"Priority 3 Defect Service Request" means an incident where the State's Software or Processing Error that results in a partial or intermittent system outage or unavailability, performance items that result in periodic, but not otherwise undue delay of processing business cycle data and creation without the creation of a processing backlog that spans a business cycle, system performance and availability levels not adhering to agreed-upon performance parameters, the State's traditional performance levels, and generally accepted and customary industry standards for similar functions or capabilities, errors or omissions in the software, related software elements, operational processes or software integration suite for which a workaround exists, but have been reported to and accepted by the Contractor, an acceptable State agreed workaround has been identified and implemented, temporary workaround identified with State acceptable processing, hardware, labor or other considerations, may be a recurring issue with identified or indeterminate cause, and items otherwise not classified as a Priority 1 or Priority 2 Defect.
This Service Level begins upon Contractor presentation of a deliverable (generally code based) to the State for conducting Acceptance Testing and when this deliverable is initially migrated or otherwise used in a production environment.

Formula:

$$\text{Mean Time to Repair (Priority 3 Outages)} = \frac{\text{(Total elapsed time it takes to repair Priority 3 Defect Service Requests)}}{\text{(Total Priority 3 Defect Service Requests)}}$$

Measurement Period: Accounting Month

Data Source: Monthly Project Report

Frequency of Collection: Per Incident

Service Level Measures

Individual SL GYR State	Incident Resolution – Mean Time to Repair (Priority 3 Defects).
Green	**<= 7 calendar days**
Yellow	**> 7 calendar days and <= 10 calendar days**
Red	**> 10 calendar days**

14.5.4 Service Levels – Testing Performance

Specification: System Test Execution Exit Quality Rate

Definition: System Test Execution Exit Quality Rate will 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.
"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".
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 Priority 1 issues (which must be resolved prior to presentation to the State)and will be validated during an initial measurement period. Following the initial measurement period, and for all releases, updates, enhancements or patches and as a result of any production or commercial use the initial Service Level will be 95%. The initial measurement period will be as mutually agreed by the Parties, not to exceed three months and only pertain to the first production release.

Formula

$$\text{Test Quality Exit Rate} = \frac{\text{(Total \# of Test Scripts Passed during Final Pass of System Test)}}{\text{(Total \# of Test Scripts Executed during Final Pass of System Test)}} \times 100$$

Measurement Period: Accounting Month

Data Source: Monthly Project Report

Frequency of Collection: At end of System Test

Service Level Measures

Individual SL GYR State	System Testing Test Execution Exit Quality Rate
Green	**>= 90%**
Yellow	**>= 85%, <90%**
Red	**< 85%**

14.5.5 Blocking Issues – Identification and Removal

Specification: Testing of Blocking Issues – Identification and Removal Rate

Definition: A "blocking issue" is an item that is non-compliant, or otherwise fails to meet the overall quality standard agreed for work comprising a release or otherwise described in an approved statement of work between the Contractor and the State, that without remediation causes testing or production efforts to be halted, delayed or blocked for a delivery element, a logical system function or set of functions up to and including the overall work product contracted by the State.
If a blocking issue is identified, and meets the standard of prohibiting the State to reasonably conclude testing and accepting a release or SOW in part or in full, meaning no more testing (or promotion to a production environment in a reliable or timely manner) can be completed prior to resolution of the blocking issue, the Contractor will remedy the issue or deliver suitable working and commercially viable alternatives to the State as to resume testing activities and meet the business requirement as requested by the State.
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 10.0% and will be validated during an initial measurement period. Following the initial measurement period, and as a result of any production or commercial use the initial Service Level will be adjusted to 5%. The initial measurement period will be as mutually agreed by the Parties, not to exceed three months.

Formula:

$$\text{\% of time lost to blocking issues} = \frac{\text{(Total Test Time Lost to Blocking Issues)}}{\text{(Total Scheduled Test Time)}} \times 100$$

Measurement Period: Accounting Month

Data Source: Monthly Project Report

Frequency of Collection: Per Incident

Service Level Measures

Individual SL GYR State	Blocking Issue Identification and Removal
Green	**<= 10%**
Yellow	**>10%, <= 12%**
Red	**<= 15%**

14.5.6 Regression Testing Performance – Issue Find/Fix Rate

Specification: Issue Find/Fix Rate

Definition: Regression Testing Issue find fix rate is the time the Contractor spends resolving issues identified during UAT testing as a percentage of the time required to develop the code content associated with a release, enhancement, maintenance fix or otherwise identified for production execution.
The State would like to ensure the Contractor has a prompt response to addressing issues detected during testing and ensure that the Contractor is well aligned with removal of issues detected during testing efforts and that there is a prompt return of the fix to be included in the regression testing process.
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 10.0% and will be validated during an initial measurement period. Following the initial measurement period, and as a result of any production or commercial use the initial Service Level will be adjusted to 5%. The initial measurement period will be as mutually agreed by the Parties, not to exceed three months.
"Time spent in Regression Fix" is the development time required for fixing UAT defects which cause UAT testing to stop or be delayed past the scheduled test completion date. The sum of this time is then rounded (using standard rounding) to result in the number of days.
"Time spent in Regression Test" is measured as the number of days that are added to the original UAT Test schedule due to test defect or issue resolution and additional testing having to occur due to regression testing of identified UAT defects.
"Total Development Time for Release in Days" is measured as the total time for the Release prior to the UAT phase for development and systems testing activities performed by the Contractor.
Should issues be identified and resolved within the planned UAT period, this SLA will not apply.

Formula:

$$\text{\% of Time Repairing Issues} = \frac{\text{Time spent in Regression Fix + Time Spent in Regression Test (Days)}}{\text{(Total Development Time for Release in Days)}} \times 100$$

Measurement Period: Accounting Month

Data Source: Monthly Project Report

Frequency of Collection: At end of UAT phase for each release to Production

Service Level Measures

Individual SL GYR State	Issue Find/Fix Rate
Green	**<= 10%**
Yellow	**>10%, <= 12%**
Red	**<= 15%**

14.5.7 Code Coverage – Automated Test Beds

Specification: % Automated Code Coverage – Regression, Release and Performance Testing

Definition: Amount of Code that is covered using automated testing tools for performance, functionality or scenario testing pertaining to (re)testing items or releases that had been previously tested under prior releases OR performance testing of the system or release element and relationships between a release item and its relationships to production code.
The Contractor is to provide best practices in conjunction with the overall testing effort. To facilitate rapid and quality testing, with a high degree of code coverage, the Contractor will employ automated testing tools and techniques where possible to test core scenarios, scenario variations, regression testing and performance testing
This SL will commence upon the delivery of a function set to the Contractor System testing environment and be in effect during the overall testing effort including Contractor efforts, joint efforts or in support of the State activities as agreed and apply to initial testing elements, regression/fix elements, performance and integration testing prior to production use.

Formula:

$$\text{\% of Code covered by Automated tools} = \frac{\text{Number of Test Cases covered by Automated Testing Tool within a Testing Period + Total Number of Performance Test Cases covered by Automated Performance Test Tool}}{\text{Number of total Test Cases within a Testing Period + Total Number of Performance Test Cases within a Testing Period}} \times 100$$

Measurement Period: Weekly, During Testing

Data Source: Weekly Project Report

Frequency of Collection: Mutually Agreed Testing Periods

Service Level Measures

Individual SL GYR State	% Automated Code Coverage
Green	**>75%%**
Yellow	**>50%, <= 75%**
Red	**<= 50%**

14.5.8 Service Levels – Project Performance

Specification: % Compliance Milestone Dates

Definition: Amount of committed and accepted Project Milestones achieved on time as per the Project plans. The Contractor is to produce an overall Project plan inclusive of the milestones, activities and deliverables at the commencement of the Project. Due to the overlapping nature of phases, tasks and activities, a measurement period of 1 calendar month will be established to serve as the basis for the measurement window. Vendor will count all milestones, activities and deliverables to be completed during that measurement window and their corresponding committed delivery dates. Any date variations (positive or negative) will be recorded upon the State's acceptance of the deliverable and used in the calculation of this SL.
This SL will commence upon Project initiation and will prevail until Project completion.

Formula:

$$\text{\% Compliance, Milestone Dates} = \frac{\text{Total Number of Contractor Milestones met within the measurement month}}{\text{Total Number of Contractor Milestones planned to be met during the measurement month per the agreed upon list of milestones}} \times 100$$

Measurement Period: Monthly, During Project

Data Source: Weekly Project Report

Frequency of Collection: Weekly

Service Level Measures

Individual SL GYR State	% Compliance Milestone Dates
Green	**> 90%**
Yellow	**>85%, <=90%**
Red	**<= 85%**

14.5.9 Issue Reporting

Specification: % Compliance Issue Reporting

Definition: The reporting of any issues impacting the Project to the State for prompt resolution and possible solutions to the State. The Contractor is to promptly report all issues to the Project management and sponsorship personnel within the State upon detection of an issue that will impact overall Project delivery, Project quality, or overall effectiveness of the Project in its intended production operation mode.
Wherever possible, the Contractor must include recommendations as to work-arounds, remedial actions, impact assessment and potential mitigation strategies the State may employ.
This SL will commence upon Project initiation and will prevail until Project completion.

Formula:

$$\text{\% Compliance, Issue Reporting} = \frac{\text{\# Project Issues Identified during reporting period – Issues not reported during period Status Reports - \# issues – Other unreported Issues that arise or are discovered subsequent to reporting dates}}{\text{\# Project Issues Identified during reporting period}} \times 100$$

Measurement Period: Monthly, During Project

Data Source: Weekly Project Report

Frequency of Collection: Weekly

Individual SL GYR State	% Compliance Issue Reporting
Green	**>90%**
Yellow	**>85%, <=90%**
Red	**<= 85%**

14.5.10 Deliverable Acceptance

Specification: % Deliverable Acceptance

Definition: The State's ability to accept Contractor deliverables based on submitted quality and in keeping with initially defined standards and content for Contractor deliverables.

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. For the avoidance of doubt, the deliverables contained in this RFP as they pertain to the Shared Services Implementation Project and general Ongoing Project Services delivery concepts associated with structured software development will represent the minimum set of expected deliverables.

Notwithstanding the State review and approval cycles, this SL will commence upon the delivery of a final deliverable for acceptance to the State, and any work/re-work to the final deliverable as a result of any State questions, required clarifications/amplifications, and conclude upon due completion of the required amendments.

This SL will commence upon Project initiation and will prevail until Project completion.

Formula:

$$\text{\% Deliverable Acceptance} = \frac{\text{\# Deliverables Accepted During Period (less the State review Time)}}{\text{\# Deliverables Presented during Period}} \times 100$$

Measurement Period: Monthly, During Project

Data Source: Weekly Project Report

Frequency of Collection: Weekly

Service Level Measures

Individual SL GYR State	% Deliverable Acceptance
Green	**>85%**
Yellow	**>80%, <=85%**
Red	**<= 80%**

14.5.11 Support of State User Acceptance Testing Activities

Specification: Support of the State User Acceptance Testing (UAT) activities

Definition: The Contractor must support the State UAT activities based on their knowledge of the overall system, responsibility to maintain environments, regression test beds, automated tools and retained developers on the Project to affect prompt and quality resolutions to issues detected by the State during a UAT phase.
Testing environments are to be functional and available to the State to conduct UAT activities, configured with all required base configuration and test data, application code and other elements as required to support the overall State testing effort.
The Contractor must provide a system(s) to accept and track any issues, defects or questions arising from the State during the performance of UAT functions, and acknowledge all issues with an estimate to resolve these issues within 2 business hours of receipt of the issue.
This SL will commence upon the delivery of a function set to the State to perform any User Acceptance or Validation and be in effect during the overall State testing effort including Contractor efforts, joint efforts or in support of the State activities as agreed and apply to initial testing elements, regression/fix elements, performance and integration testing prior to production use.
NOTE: All issues, defects, or questions will be recorded in a mutually agreeable tool and will be acknowledged with an estimate to resolve within 2 business hours.

Formula:

$$\text{\% UAT Support} = \frac{\text{\# Business Hours, Seven Days Per Week During UAT Period – (minus) (\# hours testing environments unavailable or unusable to perform testing + number business hours beyond standard State inquiries are not acknowledged and estimated)}}{\text{\# Business Hours, Seven Days Per Week During UAT Period}} \times 100$$

Measurement Period: Monthly, During Project

Data Source: Weekly Project Report

Frequency of Collection: Monthly

Service Level Measures

Individual SL GYR State	% UAT Support
Green	**>85%**
Yellow	**>80%, <=85%**
Red	**<= 80%**

14.5.12 Service Levels – Development Methodology Compliance

Specification: %SDLC Compliance.

Definition: The Contractor will present and adapt as required a Software Development Lifecycle (SDLC) Methodology to manage the end-to-end software delivery process. This process will be followed. The Contractor must provide as part of overall Project delivery a proven and tested SDLC to drive and govern the overall software development process and adapt wherever possible to accommodate State considerations and processes. Based on this SDLC and the prescribed development stages (e.g., requirements, design, build, test, deployment) and phase exit documentation, reviews and signoff, this process will be followed for the duration of all development or code based Projects contracted by the State.
Notwithstanding State review and approval cycles, this SL will commence upon Project initiation and will prevail until Project completion.

Formula:

$$\text{\% SDLC Compliance} - \frac{\text{\# Deliverables, Milestones, Activities, Reviews and Signoffs Made Per Phase/SDLC Gate}}{\text{\# Deliverables, Milestones, Activities, Reviews and Signoffs Required Per Phase/SDLC Gate}} \text{ X } 100$$

Measurement Period: Monthly, During Project

Data Source: Weekly Project Report

Frequency of Collection: Weekly

Service Level Measures

Individual SL GYR State	% SDLC Compliance
Green	**>95%**
Yellow	**>90%, <=95%**
Red	<= 90%

14.5.13 Service Levels–Project Delivery–Build/Test Activities as a Percentage of Overall Activities

Specification: % build and testing activities

Definition: The Contractor will perform (subject to other SLAs in effect) and prioritize deliverable construction efforts in keeping with overall Project plans and focus effort on deliverable creation and completion associated with the successful delivery of a working Project delivered with quality to a production environment.
The Contractor must report the overall date and quality considerations of the Project delivery for the SOW governing this SL, the amount of time doing constructive efforts in building software elements, deliverables, and associated documentation; and conducting testing (system, integration, interface and performance) as a percentage of overall activities during the measurement period.
This SL will commence upon Project initiation and will prevail until Project completion.
Prior to the Start of the Build and Test Phases, the State and Contractor will forecast the number of development objects and test scripts in a schedule (**planned** number submitted by month) for the phase. Each Team Lead will track the **actual** number of completed development objects and test scripts and report progress during status meetings with project leadership.

Formula:

$$\text{\% Estimating Accuracy} = \frac{\text{\% Time Spent in Build and Testing Activities Actual Number of Work Units Submitted in a Month (cumulative for phase or release) Actual Number of Work Units Submitted in a Month (cumulative)}}{\text{100\% Planned Number to be Submitted at Month End (cumulative for phase or release)}} \times 100$$

Measurement Period: Monthly, During Project

Data Source: Weekly Project Report

Frequency of Collection: Weekly

Service Level Measures

Individual SL GYR State	**% Build and Testing Activities**
Green	**>75%**
Yellow	**>70%, <=75%**
Red	**<= 70%**

14.5.14 Service Levels – Project Completion – Issues Detected and Resolved In Production

Specification: Issues Detected and Resolved in Production

Definition: During post-implementation the Contractor must continue to support and promptly resolve any issues emerging as a result of the implementation in a production environment for a period of 90 days or otherwise mutually agreed upon, or until such time as a Managed Services SL is in effect for the element in question.
The Contractor must measure all production exceptions, issues, or problems associated or in conjunction with the initial 90 day period associated with a move of a software release to a production environment regardless of the priority level unless otherwise agreed with the State. Function points from system and user acceptance testing will serve as the basis for counting the total number of elements associated with a release.
This SL will commence upon promotion of code associated with the Project to a production or commercial environment and will prevail until all issues are resolved to the State's satisfaction or 90 days, whichever is longer.

Formula:

$$\text{Issues Identified and Resolved in Production} = \frac{\text{Total Time Required to Resolve Issues Identified During initial 90 day production Period}}{\text{Total Hours included in a Production Release}} \times 100$$

Measurement Period: Monthly, During Project

Data Source: Weekly Project Report

Frequency of Collection: Weekly

Service Level Measures

Individual SL GYR State	Issues Detected and Resolved in Production
Green	**<= 2%**
Yellow	**>2%, <=3%**
Red	**>3%**

Supplement 2

State Architecture and Computing Standards Requirements

State Security and Privacy Requirements

State IT Computing Policy Requirements

State Data Handling Requirements

Contents

1. Overview and Scope 4
2. State Architecture and Computing Standards Requirements 4
2.1. Requirements Overview 4
2.1.1. State of Ohio Standards 4
2.1.2. Offeror Responsibilities 4
2.1.3. State Infrastructure Services 5
2.2. Compute Requirements 6
2.2.1. Client Computing 6
2.2.2. Server / OS 6
2.2.3. Ohio Cloud: Hypervisor Environment 6
2.3. Storage and Backup Requirements 6
2.3.1. Storage Pools 6
2.3.2. Backup 7
2.4. Networking Requirements: Local Area Network (LAN) / Wide Area Network (WAN) 7
2.5. Application Requirements 8
2.5.1. Application Platforms 8
2.5.2. Open API's 8
2.5.3. SOA (Service Oriented Architecture) 8
2.6. Database Platforms 8
2.7. Enterprise Application Services 8
2.7.1. Health and Human Services: Integrated Eligibility 8
2.7.2. The Ohio Business Gateway (OBG) 9
2.7.3. Ohio Administrative Knowledge System (OAKS) 9
2.7.4. Enterprise Business Intelligence 10
2.7.5. Enterprise Content Management 10
2.7.6. SharePoint 11
2.7.7. IT Service Management 11
2.7.8. Customer/Citizen Relationship Management (CRM) 11
2.7.9. Enterprise Geocoding Services 11
2.7.10. GIS Hosting 11
2.8. Productivity, Administrative and Communication Requirements 11
2.8.1. Communication Services 11
3. General State Security and Information Privacy Standards and Requirements 12
3.1. State Provided Elements: Contractor Responsibility Considerations 13
3.2. Periodic Security and Privacy Audits 14
3.3. Annual Security Plan: State and Contractor Obligations 14
3.4. State Network Access (VPN) 15
3.5. Security and Data Protection 15
3.6. State Information Technology Policies 15
4. State and Federal Data Privacy Requirements 16
4.1. Protection of State Data 17
4.2. Handling the State's Data 18
4.3. Contractor Access to State Networks Systems and Data 18
4.4. Portable Devices, Data Transfer and Media 19
4.5. Limited Use; Survival of Obligations 20
4.6. Disposal of PI/SSI. 20
4.7. Remedies 20
4.8. Prohibition on Off-Shore and Unapproved Access 20
4.9. Background Check of Contractor Personnel 21
4.10. Federal Tax Information 21
5. Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues 23

5.1. General 23
5.2. Actual or Attempted Access or Disclosure 23
5.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities 23
5.4. Security Breach Reporting and Indemnification Requirements 24
6. Security Review Services 24
6.1. Hardware and Software Assets 24
6.2. Security Standards by Device and Access Type 25
6.3. Boundary Defenses 25
6.4. Audit Log Reviews 25
6.5. Application Software Security 25
6.6. System Administrator Access 25
6.7. Account Access Privileges 26
6.8. Additional Controls and Responsibilities 26

1. 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.

2. State Architecture and Computing Standards Requirements

2.1. Requirements Overview

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

2.1.1. State of Ohio Standards

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

2.1.2. Offeror Responsibilities

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

Hardware and storage (memory, speeds, cpu and other configuration details) should be proposed to adhere to established State standards (generally VMware based system images for x86 environments) and or virtualized Oracle Exadata/Exalogic frames and components unless otherwise specified in the SOW Request.

In addition, Offerors are required to take advantage of all published IT Application Services where possible, i.e. Enterprise Service Bus, Content Management, Enterprise Document Management, Data Warehousing, Data

Analytics and Reporting and Business Intelligence. When dedicated Application components are required, i.e. Application Servers, Databases, etc., they should comply with the Core Technology standards.

2.1.3. State Infrastructure Services

The State of Ohio's Office of Information Technology Infrastructure Services Division (OIT/ISD) will be responsible for providing the technical infrastructure platform as a service to the Contractor and will host the Contractor developed software and operating solution following the conclusion of the project for on-premise solutions. In general, this service includes the following:

- Primary Computing Facility: State of Ohio Computing Center (secure Tier III capable facility)
- Alternate/Disaster Recovery Center: Ohio Based Secure Tier II facility
- Redundant Networking between State facilities and Data Centers (Metro-E to 10Gb/s OARnet)
- Physical and Infrastructure Security Services
- Redundant Power, Cooling, Fire Suppression and onsite Redundant UPS/Power Generation
- Servers, Storage, Networking Devices, Firewalls, Security Appliances, Vulnerability and Virus Scanning to the operating system prompt
- Binding SLAs regarding performance, availability, reliability, provisioning and systems administrative access

The State of Ohio will provide ITIL based services in support of the Contractor as follows:

Table 1 – State Infrastructure Responsibility Matrix

State Infrastructure Responsibility Matrix	
Asset Management ▪ Hardware Asset Tracking ▪ Software Asset Tracking ▪ Logistics Support ▪ Inventory Capture and Maintenance **Service Desk** ▪ Help Desk Operations ▪ Help Desk Tools ▪ Service Desk Processes	**Enterprise Security Management** ▪ Emergency Response Service ▪ Threat Analysis ▪ Managed Intrusion/Detection/Prevention ▪ System Security Checking ▪ Security Advisory and Integrity ▪ Malware Defense Management ▪ Vulnerability Management ▪ ID Management ▪ Security Policy Management ▪ Security Compliance Support ▪ Security Audit
Server Management ▪ Platform Support (Tools/Processes Procedures) ▪ Unix/Intel Servers ▪ Incident Management ▪ Server Operations ▪ High Availability ▪ File Management **Storage Planning** ▪ Capacity Management ▪ Storage Performance Management	**Data Center and Wide Area LAN/WAN Management** ▪ Enterprise Internet Services ▪ Regulatory/Change Management ▪ Network Engineering ▪ Standards ▪ LAN/WAN Management ▪ Network Operations and Management ▪ Network Capacity/Availability Management ▪ Network HW/SW Management ▪ Network Security ▪ Network M/A/C/D
Data Center Architecture Planning ▪ Hardware/Facilities Planning ▪ Unix/Intel Servers ▪ Platform Configuration Management ▪ Performance Management ▪ Capacity Management ▪ Batch Operations/Scheduling ▪ Storage Management ▪ Backup/Restore ▪ Media Management, Media Operations, Offsite Storage	**Data Center Facilities Management** ▪ Site Maintenance and Operations ▪ Site Availability Management ▪ Routine Maintenance and Upgrades ▪ Non-Technical Services (parking lot, landscaping, snow removal etc.)

2.2. Compute Requirements

2.2.1. Client Computing

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

2.2.2. Server / OS

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

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

Table 21 – Supported Server/OS versions

Operating Systen	Version	Edition
Microsoft Windows Server	2012, 2012 R2	Standard, Enterprise, & Datacenter
RedHat Linux	7	Enterprise
SUSE Linux	11	Enterprise
IBM AIX	7.1	
Oracle Enterprise Linux		Enterprise

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

The State hosts and manages the Virtual Server hardware and Virtualization layer. The State is also responsible for managing the server's Operating System (OS). This service includes 1 virtual CPU (vCPU), 1 GB of RAM and 50 GB of Capacity Disk Storage. Customers can request up to 8 vCPUs and 24GB of RAM.

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

2.2.3. Ohio Cloud: Hypervisor Environment

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

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

2.3. Storage and Backup Requirements

2.3.1. Storage Pools

The State provides three pools (tiers) of storage with the ability to use and allocate the appropriate storage type based on predetermined business criticality and requirements. Storage pools are designed to support different I/O workloads.

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

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

The pools and their standard use cases are below:

Table 3 – State Supported Storage Pools

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

2.3.2. Backup

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

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

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

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

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

The State of Ohio's One Network is a unified solution that brings together Design, Engineering, Operations, Service Delivery, Security, Mobility, Management, and Network Infrastructure to target and solve key Government challenges by focusing on processes, procedures, consistency and accountability across all aspects of State and Local Government.

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

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

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

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

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

2.5. Application Requirements

2.5.1. Application Platforms

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

2.5.2. Open API's

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

2.5.3. SOA (Service Oriented Architecture)

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

2.6. Database Platforms

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

- DB2 Version 10
- SQL 2012 or higher
- ORACLE 11g and 12C
- Exadata Version 11.2.3.2.1

2.7. Enterprise Application Services

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

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

2.7.1. Health and Human Services: Integrated Eligibility

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

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

2.7.2. The Ohio Business Gateway (OBG)

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

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

2.7.3. Ohio Administrative Knowledge System (OAKS)

OAKS is the State's Enterprise Resource Planning (ERP) system, which provides central administrative business services such as Financial Management, Human Capital Management, Content Management via myOhio.gov, Enterprise Learning Management, and Customer Relationship Management. Core System Capabilities include (but are not limited to):

Content Management (myohio.gov)

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

Enterprise Business Intelligence

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

Financial Management (FIN)

- Accounts Payable
- Accounts Receivable
- Asset Management
- Billing
- eBid
- eCatalog (Ohio Marketplace)
- eInvoicing (coming Fall 2015)
- eSupplier/Offeror Maintenance
- Financial Reporting
- General Ledger

- Planning and Budgeting
- Procurement
- Travel & Expense

Enterprise Learning Management (ELM)

- Training Curriculum Development
- Training Content Delivery

Human Capital Management (HCM)

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

2.7.4. Enterprise Business Intelligence

- Health and Human Services Information
    - Eligibility
        - Operational Metrics
        - County Caseworker Workload
    - Claims [Q1, 2015]
    - Long Term Care [Q2, 2015]
- Financial Information
    - General Ledger (Spend, Disbursement, Actual/Forecast)
    - Travel and Expense
    - Procure to Pay (AP/PO/Offeror/Spend)
    - Capital Improvements
    - Accounts Receivable
    - Asset Management
- Workforce and Human Resources
    - Workforce Profile
    - Compensation
    - MBE/EDGE

2.7.5. Enterprise Content Management

Hyland OnBase is the State's Enterprise Content Management system for Document Imaging and Document and Records Management. The service is designed to provision, operate and maintain the State's Enterprise Content Management solution.

2.7.6. SharePoint

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

2.7.7. IT Service Management

ServiceNow, a cloud-based IT Service Management Tool that provides internal and external support through an automated service desk workflow based application which provides flexibility and ease of use. The IT Service Management Tool provides workflows aligning with ITIL processes such as Incident Management, Request Fulfillment, Problem Management, Change Management and Service Catalog.

2.7.8. Customer/Citizen Relationship Management (CRM)

Salesforce, is the State's cloud-based Customer Relationship Management tool that helps agencies build stronger connections between citizens, employees, governments, services, and the information they need.

2.7.9. Enterprise Geocoding Services

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

2.7.10. GIS Hosting

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

2.8. Productivity, Administrative and Communication Requirements

2.8.1. Communication Services

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

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

Exchange

- Exchange Mail
- Office 365
- Skype for Business Instant Messaging & Presence
- Enterprise Vault
- Clearwell eDiscovery
- Exchange Web Services
- Bulk Mailing

- External Mail Encryption
- Outbound Fax
- Mobile devices

EDI/Application Integration/Medicaid EDI

Lyris Listserv

On-premise application based FAX: eFAX

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

Voice over Internet Protocol (VoIP)

The CBTS VoIP service, which is open to all agencies, boards, commissions, local governments and state supported education institutions, as well as State of Ohio Cooperative Purchasing Program members, provides core telephony, voice mail, collaboration, video, audio, and auto attendant functions to eligible customers. Optional services including ACR, IVR, Call Center Solutions and SIP Trunking are also available.

3. 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.
- Manage and administer access to the systems, networks, System software, systems files and State data, excluding end-users.
- Provide support in implementation of programs to educate State and Contractor end-users and staff on security policies and compliance.
- Install and update Systems software security, assign and reset passwords per established procedures, provide the State access to create User ID's, suspend and delete inactive logon IDs, research system security problems, maintain network access authority, assist in processing State security requests, perform security reviews to confirm that adequate security procedures are in place on an ongoing basis, and provide incident investigation support (jointly with the State), and provide environment and server security support and technical advice.
- Develop, implement, and maintain a set of automated and manual processes to ensure that data access rules are not compromised.
- Perform physical security functions (e.g., identification badge controls, alarm responses) at the facilities under the Contractor's control.
- Prepare an Information Security Controls Document. This document is the security document that is used to capture the security policies and technical controls that the Contractor will implement, as requested by the State, on Contractor managed systems, supported servers and the LAN within the scope of this agreement. The Contractor will submit a draft document for State review and approval during the transition period.

The State will:

- Develop, maintain and update the State IT Security Policies, including applicable State information risk policies, standards and procedures.
- Provide a State Single Point of Contact with responsibility for account security audits;
- Support intrusion detection and prevention and vulnerability scanning pursuant to State IT Security Policies;
- Provide the State security audit findings material for the Services based upon the security policies, standards and practices in effect as of the Effective Date and any subsequent updates.
- Assist the Contractor in performing a baseline inventory of access IDs for the systems for which the Contractor has security responsibility;
- Authorize User IDs and passwords for the State personnel for the Systems software, software tools and network infrastructure systems and devices under Contractor management;
- Approve non-expiring passwords and policy exception requests, as appropriate.

3.1. State Provided Elements: Contractor Responsibility Considerations

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

To the extent that Contractor's access or utilize State provided networks, the Contractor is responsible for adhering to State policies and use procedures and do so in a manner as to not diminish established State capabilities and standards.

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

The Contractor's responsibilities with respect to security services must also include the following:

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

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

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

3.2. Periodic Security and Privacy Audits

The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue or finding be discovered the following resolution path shall apply:

- If a security or privacy issue is determined to be pre-existing to this agreement, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

3.3. 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
- Logical security controls (privacy, user access and authentication, user permissions, etc.)
- Technical security controls and security architecture (communications, hardware, data, physical access, software, operating system, encryption, etc.)
- Security processes (security assessments, risk assessments, incident response, etc.)
- Detail the technical specifics to satisfy the following:
- Network segmentation
- Perimeter security
- Application security and data sensitivity classification
- PHI and PII data elements
- Intrusion management
- Monitoring and reporting
- Host hardening
- Remote access
- Encryption
- State-wide active directory services for authentication
- Interface security
- Security test procedures
- Managing network security devices
- Security patch management

- Detailed diagrams depicting all security-related devices and subsystems and their relationships with other systems for which they provide controls
- Secure communications over the Internet

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

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

3.4. State Network Access (VPN)

Any remote access to State systems and networks, Contractor or otherwise, must employ secure data transmission protocols, including the secure sockets layer (SSL) protocol and public key authentication, signing and encryption. In addition, any remote access solution must use Secure Multipurpose Internet Mail Extensions (S/MIME) to provide encryption and non-repudiation services through digital certificates and the provided PKI. Multi-factor authentication is to be employed for users with privileged network access by leveraging the State of Ohio RSA solution.

3.5. Security and Data Protection.

All Services must also operate at the [moderate level baseline] as defined in the National Institute of Standards and Technology ("NIST") 800-53 Rev. 3 [moderate baseline requirements], be consistent with Federal Information Security Management Act ("FISMA") requirements, and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications. Additionally, they must provide the State's systems administrators with 24x7 visibility into the services through a real-time, web-based "dashboard" capability that enables them to monitor, in real or near real time, the Services' performance against the established SLAs and promised operational parameters.

3.6. 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:

- Support intrusion detection & prevention including prompt agency notification of such events, reporting, monitoring and assessing security events.

- Support the State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency's review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Managing and administering access to the Operating Software, systems files and the State Data.
- Installing and updating State provided or approved system security Software, assigning and resetting administrative passwords per established procedures, providing the agency access to create administrative user ID's, suspending and deleting inactive logon IDs, researching system security problems, maintaining network access authority, assist processing of the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the agency's assistance providing incident investigation support, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State data access rules are not compromised.
- Where the Contractor identifies a potential issue in maintaining an "as provided" State infrastructure element with the more stringent requirement of an agency security policy (which may be federally mandated or otherwise required by law), identifying to agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.
- The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue be discovered the following resolution path shall apply:
- If a security or privacy issue is determined to be pre-existing to this agreement, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
- If over the course of delivering services to the State under this Statement of Work for in-scope environments the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Contractor is to notify the State within two (2) hours. This notification shall not minimize the more stringent Service Level 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.
- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

The Contractor will comply with State Security and Privacy policies and standards. For purposes of convenience, a compendium of links to this information is provided in the Table below.

Table 4 - State of Ohio Security and Privacy Policies

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

4. 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 SOW request including but not limited to:

- United States Code 42 USC 1320d through 1320d-8 (HIPAA);
- IRS 1075 pertaining to FTI data;
- Code of Federal Regulations, 42 CFR 431.300, 431.302, 431.305, 431.306, 435.945,45 CFR164.502 (e) and 164.504 (e);
- Ohio Revised Code, ORC 173.20, 173.22, 1347.01 through 1347.99, 2305.24, 2305.251, 3701.243, 3701.028, 4123.27, 5101.26, 5101.27, 5101.572, 5112.21, and 5111.61; and
- Corresponding Ohio Administrative Code Rules and Updates.
- Systems and Services must support and comply with the State’s security operational support model which is aligned to NIST 800-53 Revision 3.

4.1. 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 (“PI”) 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 PI/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 PI/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 PI/SSI received from the State and (b) establish and maintain physical, technical and administrative safeguards to prevent unauthorized access by third parties to PI/SSI received by Contractor from the State;
- Give access to PI/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 PI/SSI received from the State;
- Cooperate with any attempt by the State to monitor Contractor’s compliance with the foregoing obligations as reasonably requested by the State from time to time. The State shall be responsible for all costs incurred by Contractor for compliance with this provision of this subsection;
- Establish and maintain data security policies and procedures designed to ensure the following:
  a) Security and confidentiality of PI/SSI;
  b) Protection against anticipated threats or hazards to the security or integrity of PI/SSI; and
  c) Protection against the unauthorized access or use of PI/SSI.

4.1.1. 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 PI/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; or
- To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

4.2. 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.

4.3. 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.

4.4. 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.

4.5. Limited Use; Survival of Obligations.

Contractor may use PI/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 PI/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.

4.6. Disposal of PI/SSI.

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

4.7. 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 PI/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.

4.8. 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.

4.9. 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.

4.10. Federal Tax Information

Contract Language for General Services

In order to protect risk of loss, breach, or misuse of Federal Tax Information (“FTI”) held by government agencies, the Internal Revenue Service issued Publication 1075 which includes specific language to include in any State contract in which FTI may be disclosed.

4.10.1. Performance

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

1. All work will be done under the supervision of the Contractor or the Contractor's employees.
2. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract.
   Disclosure to anyone other than an officer or employee of the Contractor will be prohibited.
3. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

4. The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
5. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
6. All computer systems receiving, processing, storing, or transmitting Federal Tax Information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operations, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
7. No work involving Federal Tax Information furnished under this Contract will be subcontracted without prior written approval of the IRS.
8. The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
9. The agency will have the right to void the Contract if the Contractor fails to provide the safeguards described above.

4.10.2. Criminal/Civil Sanctions

1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of the officer or employee (United States for Federal employees) in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.
3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
4. Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their

authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (See Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

4.10.3. Criminal/Civil Sanctions

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

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

5.1. 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; and

5.2. 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 PI/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.

5.3. 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 PI/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.

5.4. 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.

6. Security Review Services

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

6.1. Hardware and Software Assets

The Contractor will support the State in defining and producing specific reports for both hardware and software assets. At a minimum this should include:

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

6.2. Security Standards by Device and Access Type

The Contractor will:

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

6.3. Boundary Defenses

The Contractor will:

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

6.4. Audit Log Reviews

The Contractor will:

- Work with the State to review and validate audit log settings for hardware and software
- Ensure that all OAKS systems and environments have adequate space to store logs
- Work with the State to devise and implement profiles of common events from given systems to both reduce false positives and rapidly identify active access
- Provide requirements to the State to configure operating systems to log access control events
- Design and execute bi-weekly reports to identify anomalies in system logs
- Ensure logs are written to write-only devices for all servers or a dedicated server managed by another group.

6.5. Application Software Security

The Contractor will:

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

6.6. System Administrator Access

The Contractor will

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

- Configure systems to log entry and alert when administrative accounts are modified
- Segregate administrator accounts based on defined roles

6.7. Account Access Privileges

The Contractor will:

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

6.8. Additional Controls and Responsibilities

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

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