

REQUEST FOR PROPOSALS

RFP NUMBER: 0A1149
DATE ISSUED: January 21, 2015

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

Disaster Recovery and Storage Replication Services

INQUIRY PERIOD BEGINS: January 21, 2015
INQUIRY PERIOD ENDS: February 12, 2015
OPENING DATE: February 20, 2015
OPENING TIME: 1:00 P.M.
OPENING LOCATION: Department of Administrative Services
Office of Information Technology
IT Procurement Services
Bid Desk
4200 Surface Road
Columbus, Ohio 43228-1313

This RFP consists of five Parts and eleven Attachments, totaling 52 consecutively numbered pages. Supplements also are attached to this RFP. Please verify that you have a complete copy.

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 (DAS), Office of Information Technology (OIT) is soliciting competitive sealed proposals (“Proposals”) for the Provision and Operation of a 2nd Data Center Site and Disaster Recovery Services for the State (the “Work”), and this RFP to fulfill that request.

If a suitable offer is made in response to this RFP, the State of Ohio (the “State”), through the Office of Information Technology, 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 the 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, 2015 whichever is sooner. The State may renew this Contract for up to three additional two-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 OIT

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 maintains its primary computing operations at the State of Ohio Computer Center (SOCC) located at 1320 Arthur E. Adams Drive, Columbus Ohio. Recently, the State has made significant investments in the SOCC to increase the available power in the facility and to support the consolidation of more than 30 smaller data centers and computing concentrations currently located statewide into a consolidated operation located at the SOCC. As part of this initiative, the State has identified requirements for the provision and operation of a Disaster Recovery service for State critical computing functions as well as to locate specialized State equipment in an alternate location should the SOCC become unavailable as a result of a disaster condition impacting the SOCC.

Objectives. The State has the following objectives that it wants the Work to fulfill, and it will be the Contractor’s obligation to ensure that the Work meets these objectives:

Select offeror(s) to provide a geographically diverse site (Disaster Site) that is TIA942 or Uptime Institute Tier II (or higher) capable to support the following services:

1. Cloud Based Disaster Recovery as a Service (DRaaS) infrastructure;
2. Cloud Based Storage Replication as a Service (SRaaS) Infrastructure; and
3. Disaster Recovery Testing and Optimization Events

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.

While it is not a condition of award of the RFP, the offeror must use its best efforts to 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 Work's Scope. The scope of the Work is provided in Supplement One of this RFP. This section only gives a summary of the Work. If there is any inconsistency between this summary and the attachment's description of the Work, the attachment will govern.

The Scope of the Work contained in this RFP include:

- A secure TIA942 or Uptime Tier II facility that is geographically diverse to Columbus Ohio
- Provision and Operate a Cloud Based Disaster Recovery as a Service (DRaaS) Infrastructure
- Provision and Operate a Cloud Based Storage Replication as a Service (SRaaS) Infrastructure
- Coordinate with the State OIT Team to establish data, storage and systems replication services
- Participate in Disaster Recovery Testing and Optimization Events
- Provide computing elements that are highly available and reliable and able to support the State in the event of a disaster
- Accommodate the location of space, power and networking for certain specialized State computing and emergency services devices in the proposed facility
- Adhere to State data handling and security policies
- Accommodation of State use of the aforementioned elements in the event of a disaster that renders the State's primary computing sites unavailable or unusable

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:

Firm Dates

RFP Issued:	January 21, 2015
Inquiry Period Begins:	January 21, 2015
Inquiry Period Ends:	February 12, 2015, at 8:00 a.m.
Proposal Due Date:	February 20, 2015, at 1:00 p.m.

Estimated Dates

Award Date:	March 20, 2015
-------------	----------------

Estimated Work Dates

Work Begins:	March 30, 2015
--------------	----------------

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 10 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 | Work Requirements and 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 Mandatory Requirements |
| Attachment Eight | Offeror Requirements |
| Attachment Nine | Standard Affirmation and Disclosure Form (EO 2011-2012K) |
| Attachment Ten | Cost Proposal |
| Supplement One | Facility and Service Requirements |
| Supplement Two | State Security and Privacy Requirements |
| Exhibit 1 | OARnet POPS |

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:

Margaret Owens
OIT Procurement Analyst
Office of Information Technology
Acquisition Management Office
30 East Broad Street, 39th Floor
Columbus, Ohio 43215

During the performance of the Work, a State representative (the "Work Representative") will represent the Office of Information Technology and be the primary contact for the Work. The State will designate the Work Representative in writing 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 Navigation Bar on the left, select "**Find It Fast**";
- Select "Doc/Bid/Schedule #" as the Type;
- Enter the RFP number found on the first page of this RFP (the RFP number begins with zero followed by the letter "A");
- Click the "Find It Fast" button;
- On the document information page, click the "Submit Inquiry" button;
- On the document inquiry page, complete the required "Personal Information" section by providing:
 - First and last name of the 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
- 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 "Find It Fast" feature described above and by clicking the "View Q & A" button on the document information page.

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

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

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 “Find It Fast” 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 originally signed technical section and five (5) copies of the technical section, and the package with the cost section also must be sealed and contain one (1) complete copy of the cost section of the Proposal in a native Microsoft Excel (XLS) format. Further, the Offeror must mark the outside of each package with either “Second Data Center / Disaster Recovery Services RFP – Technical Proposal” or “Second Data Center / Disaster Recovery Services RFP – Cost Proposal,” as appropriate.

Included in each sealed package, the Offeror also must provide an electronic copy of everything contained within the package on CD-ROM or USB storage device in Microsoft Office, Microsoft Project, 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 not acceptable, and the State may reject them. Offerors must submit their Proposals to:

Department of Administrative Services
I.T. Procurement Services
Attn: Bid Room
4200 Surface Road
Columbus, Ohio 43228

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 Room 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 will have submitted a defective Proposal that the State may reject. Further, any Offeror that submits multiple Proposals may have all 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 in a manner as to demonstrate the Offeror's ability to 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. Offeror's that fail to achieve a technical evaluation point total in excess of seventy percent

(70%) of the maximum available points may not be evaluated in the next phase of the evaluation process. 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. 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 Offeror proposed for award. The Offeror must sign and return the two originals to the Procurement Representative. The Contract 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 state 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 Components

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 0A1149 - Disaster Recovery and Storage Replication Services Contract dated _____, 2015 which includes Attachment Four, Attachments, Supplements and the Cost Proposal Workbook dated _____, 20##.

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.

ATTACHMENT ONE

EVALUATION CRITERIA

Mandatory Requirements. The first table lists the RFP's Mandatory requirements. 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 described in the scored criteria table. Mandatory requirements are listed below in Table 1.

Mandatory Requirements	Accept	Reject	Supporting Documentation
The Offeror's data center facility must be located within the State of Ohio.			Publicly available information of the proposed facility including the address of the facility's location.
The Offerors data center must be compliant with either TIA 942 or Up Time Institute™ Tier II standards, or greater. (No certification is required)			A statement on the Offeror's company letterhead clearly stating that the company complies with this requirement. Describe the design attributes of the proposed data center that support Offeror's affirmation of TIA 942 or Up Time Institute™ Tier II capability.
The Offeror's data center facility must be capable of being served by OARnet or OARnet interconnectivity (costs to be included in Contractor proposal)			Publicly available information of the proposed facility including the address of the facility's location and the location of the OARnet pops.
The Offeror's data center facility must be served by an alternative power and telecom substation than that of the SOCC in Columbus Ohio for which AEP is the current provider at the SOCC. or AEP may be used at the proposed site provided there is sufficient diversity in transmission, control and substations			Provide statement on the letterhead of each of the providers of the power and telecom services confirming that the Offeror's proposed facility is on a separate substation from the State of Ohio's SOCC, or if using AEP, there is sufficient diversity in transmission, control and substations.
The Offeror must have provided hosted or cloud based managed server and storage solutions within the last five years for at least one customer. The Offeror must have supported for that customer at least 300 windows, Linux or Unix variants for a period of no less than one year. The Offeror must have supported for a customer at a total storage capacity of at least 100TB for a period of no less than one year.			At least one reference of an entity that meets this requirement. Offerors may not use services provided to themselves as a reference.

Table 1 – Mandatory Requirements

For the purpose of the evaluation, scoring and ranking, the technical requirements have been divided into the categories below. The following table, Table 2 – Scoring criteria, reflects the weights associated with each technical requirement category and the maximum number of points that may be awarded in each category.

Scored Criteria. In the technical evaluation phase, the State will rate the technical merits of the proposals based on the following requirements.

Scoring Criteria	Available Points
Mandatory Requirements - The ability to meet the mandatory requirements.	Accept/Reject
Offeror Organization Overview, Offeror Requirements and Staffing Capabilities - The ability of the Offeror to demonstrate its business experience, financial stability and staffing capabilities.	25 points

<p>Site Scope, Attributes and Connectivity-</p> <p>Site Scope - The ability of the Offeror to meet the space requirements for the data processing center and administrative elements of the facility. The ability of the Offeror to meet the requirements for connecting to various State and public data and voice network(s). (4 Requirements under Part 3 of Supplement 1).</p> <p>Site Attributes Requirements - The extent to which the Offeror can meet the access, use and egress to the building. (12 Requirements under Part 3 of Supplement 1)</p> <p>Site Connectivity Requirements – The extent to which the offeror can meet the connectivity requirements. (5 Requirements under Part 3 of Supplement 1)</p>	<p>50 points</p>
<p>Site Location Requirements- The ability of the Offeror to provide a suitable location and placement of the data center with the State. (9 Requirements under Part 3 of Supplement 1)</p>	<p>50 points</p>
<p>Facility Requirements</p> <p>Site Power Requirements - The ability of the Offeror to meet the power requirements based on the assumed usage and occupancy of the building by the State. (4 Requirements under Part 3 of Supplement 1)</p> <p>Site HVAC Requirements - The ability of the Offeror to meet the heating, cooling and air conditioning requirements for the building and the design targets. (3 Requirements under Part 3 of Supplement 1)</p>	<p>50 points</p>
<p>Site Physical Security including SSAE 16 Type 2 Reporting Requirements</p> <p>Site Physical Security – The ability of the Offeror to provide security of and control access to State equipment, networks, services and space. (7 Requirements under Part 3 of Supplement 1)</p> <p>SSAE 16 Type 2 Reporting Requirements – The ability and experience and commitment of the Offeror to support SSAE 16 Type 2 Audit/Reporting (5 Requirements under Part 3 of Supplement 1)</p>	<p>50 points</p>
<p>Facility IT Support Services Requirements including System Maintenance and HVAC Operation and Maintenance - The ability of the Offeror to provide facility elements that support State use of the Contractor provided services. (Part 3 of Supplement 1)</p>	<p>50 points</p>
<p>Contractor Provided Cloud Service for Disaster Recovery as a Service (DRaaS) – The extent to which the Contractor’s proposed service meets the State’s requirements for x86 (Linux and certain Unix variants) and Windows (Server) image provision, replication/synchronization, operation and Disaster Recovery requirements (Part 4 of Supplement 1)</p>	<p>100 points</p>
<p>Contractor Provided Cloud Storage Replication as a Service (SRaaS) – The extent to which the Contractor’s proposed service meets the State’s requirements for replication/synchronization of State critical data and storage for purposes of operation or recovery in the event of a disaster condition (Part 5 of Supplement 1)</p>	<p>100 points</p>
<p>Contractor Accommodation of Specialized State Computing and Emergency equipment – the extent to which the Contractor can provide space, continuous power and networking and security services in support of the location and operation of specialized State equipment (Part 6 of Supplement 1)</p>	<p>50 points</p>
<p>Adherence to State Service Level Agreements pertaining to the Contactor Provided Services – the extent to which the Contractor’s service, service reporting and operational capabilities adhere to State Service Level Agreement requirements (Part 7 of Supplement 1).</p>	<p>75 points</p>
<p>Maximum Total Score Possible (Available Points)</p>	<p>600 points</p>

Table 2- Scoring Criteria

Each proposal will be evaluated against the technical requirements using the evaluation criteria listed in Table 3 – Evaluation criteria. The requirements in each category will be assigned a value from 0 to 7 points based on the evaluation criteria guide.

Compliance			
Exceeds Requirement	Meets Requirement	Partially Meets Requirement	Does not Meet Requirement
7	5	1	0

Table 3 – Evaluation Criteria

After the Evaluation Proposal Team has completed the technical evaluation, the team will rank the Offerors based on the total points achieved.

Cost Proposal. Only the Offeror(s) who have ranked the highest number of points in the technical evaluation will be eligible for further participation in the procurement process.

The State will conduct a detailed review of the cost proposals from the Offer(s) who have the highest scores in the technical review. In addition to considering overall Offeror costs by section and as a combined total, the State may at its sole discretion perform additional analysis on the Offeror provided cost data, including but not limited to:

- Comparison of proposed labor costs and rates in the Rate Card for facility services to existing industry rates in effect for similar job description and role responsibilities;
- Analysis of technical elements and element pricing as they pertain to delivery of the respective Statement(s) of Work, Service Levels and overall technical requirements;
- Assessment of the overall cost profile for the provision of business continuity, fault resilience and disaster recovery elements; and
- Assessment of overall adherence to budgetary and cash flow considerations as it pertains to Offeror proposed cost and timing elements.
- Additional analysis as deemed required by the State to assess the proposed costs and overall value in light of the Offeror’s proposal

Overall Evaluation

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

Criteria	Percentage
Technical Proposal	35%
Cost Proposal	55%
MBE Participation in Service Setup/Establishment Activities	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 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 Technical Proposal will receive 350 points. The remaining Offerors will receive a percentage of the maximum points available based upon the following formula:

$$\begin{array}{rcccl}
 \text{Technical Proposal} & & \text{Offeror's Technical Proposal Points in Each_Scored} & & \\
 \text{Points} & = & \text{Criteria Area} & & \\
 & \text{(equals)} & \text{-----} & \text{X} & \text{350} \\
 & & & \text{(times)} & \\
 & & \text{Highest Number of Technical Proposal Points} & & \\
 & & \text{Obtained in Each Scored Criteria Area} & &
 \end{array}$$

The Offeror proposing the best Cost Proposal Value (that is complete and inclusive of all project costs) according to the cost analysis will receive 550 points. The remaining Offerors will receive a percentage of the maximum cost points available based upon the following formula:

$$\begin{array}{rcccl}
 \text{Cost Proposal} & & \text{Best Cost Proposal Value} & & \\
 \text{Points} & = & \text{-----} & \text{X} & \text{550} \\
 & \text{(equals)} & & \text{(times)} & \\
 & & \text{Offeror's Cost Proposal Value} & &
 \end{array}$$

The Offeror proposing the highest utilization of MBE for as a percentage of Service/Setup Establishment Activity costs will receive 100 points. The remaining Offerors will receive a percentage of the maximum cost points available based upon the following formula:

$$\begin{array}{rcccl}
 \text{MBE Points} & & \text{Offeror MBE Percentage of Setup/Service} & & \\
 & = & \text{Establishment Activity Costs} & & \\
 & \text{(equals)} & \text{-----} & \text{X} & \text{100} \\
 & & & \text{(times)} & \\
 & & \text{Highest Offeror MBE Percentage of Setup/Service} & & \\
 & & \text{Establishment Activity Costs} & &
 \end{array}$$

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

$$\begin{array}{rcccl}
 \text{Total Points} & & \text{Technical} & & \text{MBE} \\
 \text{Score} & = & \text{Proposal} & + & \text{Points} \\
 & \text{(equals)} & \text{Points} & \text{(plus)} & \\
 & & & &
 \end{array}$$

ATTACHMENT TWO: WORK REQUIREMENTS AND SPECIAL PROVISIONS

PART ONE: WORK REQUIREMENTS

The scope of work and requirements are contained in Supplement 1 to this RFP.

PART TWO: SPECIAL PROVISIONS

Inconsistencies between Contract and Deliverables. 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 that are inconsistent or conflicts with the Contract, the Contract will prevail.

The Contractor's Fee Structure. The Contract award will be for a Not-To-Exceed Fixed Price, payable in accordance with the selected Contractor's Cost Summary, a Microsoft Excel® Workbook (Attachment 10) native format.

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 MBEs. The work set aside should equate to a minimum of 15% of the Offeror's cost proposal for those activities associated with Service Setup/Establishment Activities contained in this RFP. In seeking bids, the Offeror must:

- Utilize a competitive process to which only Ohio certified MBEs may respond;
- Issue the set aside competition to a minimum of three Ohio certified MBEs;
- Have established criteria by which prospective MBEs will be evaluated including business ability and specific experience related to the work requirements;
- Require the MBE to maintain their certification throughout the term of the Contract, including any renewals; and
- Propose the awarded MBE as a subcontractor under RFP 0A1149.

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. 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.

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 required 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 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.

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 must 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 Scope of Work (Supplement One) and required sections of the Proposal format (Attachment Three), 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 and Supplement Two 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.

Example of acceptable in-line section response (in italics below):

***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 reject the Proposal. No assumptions may be included regarding negotiation, terms and conditions, or requirements.*

Offeror Response: Offeror describes how it will address the Assumptions section within the Proposal.

Each Proposal must respond to every request for information in this attachment and Supplement 2, whether the request requires a simple "yes" or "no" or requires a detailed explanation. Simply repeating the RFP's requirement and agreeing to comply may be an unacceptable response and may cause the Proposal to be rejected.

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

- Cover Letter
- Vendor Information Form (OBM-5657)
- Subcontractor Letters
- Offeror Certification Form
- MBE Certification
- Mandatory Requirements
- Offeror Organization Overview and Requirements
- Staffing Capabilities
- Assumptions
- Project Plan
- Work Plan
- Support Requirements
- Proof of Insurance
- Payment Address
- Legal Notice Address
- W-9 Form
- Independent Contractor Acknowledgement Form

Standard Affirmation and Disclosure Form (EO 2011-2012K)
Acceptance of Attachment Four – General Terms and Conditions
Acceptance of Supplement Two – Security and Privacy, State IT Computing Policy and State Data Handling Requirements.
Cost Proposal (separate sealed package)

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

Vendor Information Form. The Offeror must submit a signed and completed Vendor Information Form (OBM-5657). The form is available at <http://ohiosharedservices.ohio.gov/VendorsForms.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 Six, Offeror Certification Form.

MBE Certification. Any offeror seeking to submit a proposal that is a certified MBE or includes a MBE subcontractor must provide a copy of their Ohio MBE Certification from the Department of Administrative Services pursuant to ORC 123.151 (MBE).

Mandatory Requirements. All Offerors must demonstrate experience to meet all of the mandatory requirements by completing the Mandatory Requirement pages provided in Attachment Seven that summarizes the relevant experience.

Offerors must identify the requirement at the top of each profile form. The Offeror must list each work experience separately and completely every time it is referenced. The form may be duplicated as necessary.

Offeror Organization Overview and Requirements. The offeror must provide an organizational overview. The description must 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. Each Proposal must include a description of the Offeror's capability, capacity, experience in the industry and any other background information that will help the State gauge the ability of the Offeror to fulfill the obligations of the Contract.

If the offeror has audited financial statements, it must provide them for the past three years. If the offeror's most recently completed fiscal year is not yet audited, the previous three years may be acceptable. If the offeror has no audited financial records, it may submit its financial statements for the last three years without an auditor's certification.

Offerors must use Attachment Eight in responding to the following offeror requirements. Offerors must provide information on their selected site and include the business and financial history, experience providing data center facilities and services with other clients via this site within the State of Ohio.

1. The Offeror must have provided data center facility services to at least three companies for the preceding two years using the proposed site or one large company that is using the site in excess of the State's requirements.
2. The Offeror must be the owner of the proposed data center facility and provide evidence of site ownership information using County Tax Records that demonstrate this ownership; or in the case of a leased premise, must have an unexpired lease period for seven (7) years from the RFP Response due date and provide an affirmation of this lease period from the lessor/landlord who owns the leased premise.
3. The Offeror (as an entity either within or outside of Ohio) must be operating for a minimum period of five years.

Staffing Capabilities.

- The offeror must provide a staffing plan that identifies the required key personnel by position that the offeror proposes to complete the Project.

The Offeror must identify a property manager ("Property Manager"), a building engineer ("Building Engineer"), a cabling designer ("Cabling Designer") and two building electricians ("Building Electricians"). The Offeror must identify any additional staff required for continuous 2nd Site/DR Data Center Site operations.

The staffing plan must show each individual's responsibilities on the Project. The State also requires a staffing plan that matches the skills and experience of the proposed Project Manager and Project Team to the activities and tasks that will be completed on the Project.

Resumes must be provided for the proposed key personnel to demonstrate proven experience on projects of similar scale and complexity. Representative resumes are not acceptable.

The resumes must include:

1. The person's name;
 2. The proposed role on this Project;
 3. Listings of completed projects 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 (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;
 4. Education;
 5. Professional licenses, certifications, and memberships; and
 6. Employment history.
- A contingency plan that shows the ability to add more staff if needed to ensure meeting the Project's due date(s); and
 - A statement that clearly indicates the time commitment of the proposed candidate. The Offeror also must include a statement indicating to what extent, if any, the proposed candidate may work on other projects during the term of the Contract. The State may reject any Proposal that commits the proposed candidate 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.

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 must 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 to. Offerors must not include assumptions elsewhere in their response.

Project Plan. The State encourages responses that demonstrate a thorough understanding of the nature of the Work and what the Contractor must do to get the Work done properly. To this end, the Offeror must submit a Project Plan that the Offeror will use to create a consistent and coherent management plan for the Work. The Project Plan must include detail sufficient to give the State an understanding of how the Offeror's knowledge and approach will:

- Manage the Project;
- Guide Project execution;
- Document planning assumptions and decisions;
- Facilitate communication among stakeholders;
- Define key management review as to content, scope, and schedule; and
- Provide a baseline for progress measurement and Project control.

At a minimum, the Offeror's Project Plan must include the following:

- Work breakdown structure;
- High Level Project schedule for all Project Deliverables and milestones;
- Who 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 and schedule;
- Major milestones and target date(s) for each milestone that are consistent with this RFP's dates;
- 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;
- Definition 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
- If the Offeror chooses to use Subcontractors, this part of the Offeror's Proposal must describe its approach to managing its subcontractors effectively.

Work Plan. The State encourages responses that demonstrate a thorough understanding of the nature of the Work and what the Contractor must do to get the Work done properly. To this end, the Offeror must submit a Work Plan that includes detail sufficient to give the State an understanding of how the Offeror's meet the requirements for project management and each Work Area defined in Supplement One. Offerors must complete an in-line response within Supplement One to fulfill the submission requirements for the work plan.

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.

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 will 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#zoom=80>

Standard Affirmation and Disclosure Form (EO 2011-2012K). The Offeror must complete and sign the Affirmation and Disclosure Form (Attachment Nine) 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.

Acceptance of Supplement 2 – Security and Privacy, State IT Computing Policy and State 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.

Cost Proposal. This RFP includes a Cost Proposal Form provided as an attachment. Offerors may not reformat this form. Each Offeror must complete the Cost Proposal Form in the exact format provided, since the State may reject any Proposal with a reformatted Cost Proposal Form or that is not separately sealed. (See: Part Three: General Instructions, Proposal Submittal.)

The Cost Proposal Form must not include exceptions, additional terms and conditions, or assumptions.

The Offeror's total cost for all the Work must be represented as the not-to-exceed fixed price.

Offerors may not alter to calculations of component, row or column totals contained in the Cost Proposal Form.

The State will not be liable for or pay any Work 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 (the "Proposal") and the State's Request for Proposals (the "RFP"), which are collectively referred to as the "RFP Documents", are a part of this contract (the "Contract") and describe the work (the "Work") the selected Offeror (the "Contractor") must do and any materials the Contractor must deliver (the "Deliverables") under this Contract. The Contractor must do the Work 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 Work.

The Contractor must consult with the appropriate State representatives and others necessary to ensure a thorough understanding of the Work and satisfactory performance. The State may give instructions to or make requests of the Contractor relating to the Work, 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 Work and will not amend or alter the scope of the Work.

Term. Unless this Contract is terminated or expires without renewal, it will remain in effect until the Work is completed to the satisfaction of the State and the Contractor is paid. But the current General Assembly cannot commit a future General Assembly to an expenditure. Therefore, this Contract will automatically expire at the end of each fiscal year or biennium, the first of which is June 30, 2015. The State may renew this Contract in the next fiscal year or 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 term during which the Work continues, subject to the State's approval. Termination or expiration of this Contract will not limit the Contractor's continuing obligations with respect to Deliverables that the State pays 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 Work 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 Work. The Contractor must make those deliveries, meet those milestones, and complete the Work 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 Suspension and Termination Section contained in Part II of this Attachment Four.

But the State also may have certain obligations to meet. Those obligations, if any, also are 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 Work. The Contractor must deliver any such notice to both the Work 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 Work. 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 solution to what the Work is intended to accomplish, and the Contractor must provide any incidental items omitted in the RFP Documents as part of the Contractor's not-to-exceed fixed price. All

required components and processes for the Work to be complete and useful to the State are included in the Work and the not-to-exceed fixed price, unless the RFP expressly provides otherwise.

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 "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 Work or, in the case of milestone payments or periodic payments of an hourly, daily, weekly, monthly, or annual rate, all relevant parts of the Work 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 Work Manager, the Contractor's executive responsible for the Work, the Work 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.

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 all the Work 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.

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 Work 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.

Reimbursable Expenses will not include expenses incurred by employees and consultants in connection with the services including but not limited to airfare, parking, car rental, hotel, meals and tips associated with travel, increased insurance premiums resulting from additional insurance coverage(s) requested by the State, printing,

plotting, and courier and overnight delivery expenses. Expenses of this nature are to be included in the Contractor's proposal as part of the proposed fee structure and (if applicable) hourly proposed rate of Contractor personnel.

Right of Offset. The State may set off the amount of any Ohio tax liability 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.

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#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

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 Work, such will be the sole and exclusive responsibility of the Contractor. And 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 Work under this Contract duplicates the work done or to be done under the other State contracts.

Other Contractors. The State may hold other contracts for additional or related work, including among others independent verification and validation (IV&V) efforts for the Work. 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 the Work. Such cooperation includes expeditiously providing the IV&V contractor with full and complete access to all 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 Work, the State will obligate the IV&V contractor to a confidentiality provision similar to the Confidentiality Section contained in this Contract. The Contractor must include the obligations of this provision in all its contracts with its subcontractors for the Work.

Subcontracting. The Contractor may not enter into subcontracts related to the Work after award without written approval from the State. But 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 Work. 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 Work 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. And 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. But 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 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. And the Contractor must keep all Work-related records and documents at its principal place of business or at its office where the work was performed. Should the Contractor deem for confidentiality obligations to other customers that these records be maintained separately from other customer records, the Contractor is permitted to maintain and keep these records separate.

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 Work provided by the Contractor to the State. This audit right also applies to the State's duly authorized representatives and any person or organization providing financial support for the Work. 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 Work will be done outside Ohio, the laws of the appropriate state(s) where any portion of the Work 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 will, 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 ten (10) day 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 who will do the Work, 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 Work 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 Work, if doing so is necessary for legal or disciplinary reasons. But 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 Work 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 Work. 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 Work. 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 Work, 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.

Suspension and Termination. The State may terminate this Contract 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 Work, 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.

Upon 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.

Moreover, the State may terminate this Contract for its convenience and without cause or if the Ohio General Assembly fails to appropriate funds for any part of the Work. If a third party is providing funding for the Work, the State also may terminate this Contract should that third party fail to release any funds for the Work. The RFP Documents normally identify any third party source of funds for the Work, 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 activity on the Work 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 Work's completion, any costs incurred in doing the Work 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. But if the State determines that delivery in that manner would not be in its interest, then the State may 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 termination is for the convenience of the State, the Contractor will be entitled to compensation for any Work that the Contractor has performed before the termination. Such compensation will be the Contractor's exclusive remedy in the case of termination for convenience and will be available to the Contractor only once the Contractor has submitted a proper invoice for such, with the invoice reflecting the amount that the State determines it owes to the Contractor. The State will make that determination based on the lesser of the percentage of the Work completed or the hours of work performed in relation to the estimated total hours required to perform all the Work.

The State will have the option of suspending rather than terminating the Work, 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

Work 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 Work 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 Work just as is required by this Section in the case of termination. After suspension of the Work, the Contractor may not perform any Work without the consent of the State and may resume the 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 Work. If the suspension is for the convenience of the State, then termination of the Contract will be a termination for convenience. If the suspension is with cause, the termination will also be for cause.

The State may not suspend the Work 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 Work 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 "Work Representative." The Work Representative will review all reports the Contractor makes in the performance of the Work, will conduct all liaison with the Contractor, and will accept or reject the Deliverables and the completed Work. The Work Representative may delegate his or her responsibilities for individual aspects of the Work to one or more managers, who may act as the Work Representative for those individual portions of the Work.

The Contractor's Work Manager under this Contract will be the person identified on the RFP Documents as the "Work Manager." The Work Manager will be the Contractor's liaison with the State under this Contract. Additionally, the Work Manager will conduct all Work meetings and prepare and submit to the Work 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 Work 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 Work.

Work 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 use 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 Work. The Contractor must coordinate the successful execution of the Work and direct all Work activities on a day-to-day basis, with the advice and consent of the Work Representative. The Contractor will be responsible for all

communications regarding the progress of the Work and will discuss with the Work Representative any issues, recommendations, and decisions related to the Work.

If any part of the Work 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 Work Representative certifying that installation is complete and the Work, 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 Work 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 Work and maintaining them throughout the duration of this Contract.

Changes. The State may make reasonable changes within the general scope of the Work. 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 Work, 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 Work, 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 Work 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 Work, 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 Office of Information Technology 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 Work or replacing one part of the Work with the change, the State will get a credit for the work no longer required under the original scope of the Work. 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 Work, 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.

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 Work. 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 Work. 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 of Information. The parties agree that they will not use any information, systems, or records made available to either party for any purpose other than to fulfill the obligations specified herein, and specifically agree to comply with state and federal confidentiality laws, rules, and regulations applicable to programs under which this Agreement is funded, specifically Title 7 of the Code of Federal Regulations, section 246.26 (d). The terms of this paragraph will be included in any subcontracts executed by either party for work under this Agreement.

The parties assure that they:

- will maintain applicant and participant confidentiality and not release or allow access to data and information in full or in part to any third person party or program;
- will not present or publish data and information in a manner in which any individual can be identified; and
- will not attempt to link or permit others to link data or information with individually identified records in another database, file, or other information source.

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.

Return of State Data. 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.

Ownership of Deliverables. The State owns all Deliverables that the Contractor produces under this Contract, 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.

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.

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.

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; (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 Work 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 Work. 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.

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 or [\[\\$\(2 x Annual Contract Value\)\]](#), whichever is greater. 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

Acceptance. There will be no formal acceptance procedure unless the RFP Documents expressly provide otherwise. If the RFP Documents do not provide otherwise, the acceptance procedure will be an informal review by the Work Representative to ensure that each Deliverable and the Work as a whole comply with the requirements of this Contract. The Work Representative will have up to 30 calendar days to do this. No formal letter of acceptance will be issued, and passage of the 30 calendar days will imply acceptance, though the State will issue a notice of noncompliance if a Deliverable or the Work as a whole does not meet the requirements of this Contract. If the Work Representative issues a letter of noncompliance, then the Contractor will have 30 calendar days to correct the problems listed in the noncompliance letter. If the Contractor fails to do so, the Contractor will be in default without a cure period. If the Work Representative has issued a noncompliance letter, the Deliverables or the Work as a whole will not be accepted until the Work Representative 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 Work Representative will issue the acceptance letter within 15 calendar days.

If the Work fails to meet the standard of performance after 90 calendar days from the start of 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 Work.

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.

PART SIX: CONSTRUCTION

Entire Document. This Contract is the entire agreement between the parties with respect to its subject matter and supersedes any previous statements or 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 Work 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.

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. 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 Work 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. And the Contractor must 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 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.

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

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

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.

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, but not limited to 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 DAS 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 Equal Opportunity Departments web site: <http://www.das.ohio.gov/Eod/AEEO.htm>

USE OF MBE AND EDGE VENDORS. The State encourages Contractor to purchase goods and services from Minority Business Enterprises (MBE) and Encouraging Diversity, Growth, and Equity (EDGE) vendors.

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.

**ATTACHMENT FIVE
SAMPLE CONTRACT**

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

AND

(CONTRACTOR)

THIS CONTRACT, which results from RFP 0A1134, entitled <RFP Title> , is between the State of Ohio, through the Department of Administrative Services, on behalf of the Ohio Department of Administrative Services and _____ (the "Contractor").

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.

This Contract consists of:

1. The one-page Contract (Attachment Five) in its final form;
2. The Disaster Recovery and Storage Replication Services Negotiated Contract dated _____, 2015 which includes Attachment Four, Attachments, Supplements, the Cost Workbook and additional Contract Appendices dated _____, 20##;
3. The applicable Purchase Order.

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 _____, 20##, 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.

CONTRACTOR

STATE OF OHIO
OFFICE OF INFORMATION TECHNOLOGY

SAMPLE – DO NOT FILL OUT

By: _____

By: [Robert Blair](#)

Title: _____

Title: [Director](#)

Date: _____

Date: _____

ATTACHMENT SIX

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 and Supplement One or take data that belongs to the State of Ohio outside the geographic limitations contained in Attachment Two and Supplement One 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 its 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.

Please 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: MANDATORY REQUIREMENTS

MANDATORY REQUIREMENT: The Offeror's data center facility must be located within the state of Ohio.

Identify the address of the proposed data center facility:

ATTACHMENT SEVEN: MANDATORY REQUIREMENTS

MANDATORY REQUIREMENT: The Offerors data center must be capable of either TIA 942 or Up Time Institute™ Tier II standards, or greater capable. No certification is required.

Provide a statement on the Offeror's company letterhead clearly stating that the company complies with this requirement. Describe the design attributes of the proposed data center that support Offeror's affirmation of TIA 942 or Up Time Institute™ Tier II capability.

ATTACHMENT SEVEN: MANDATORY REQUIREMENTS

MANDATORY REQUIREMENT: The Offeror's data center facility must be capable of being served by OARnet or OARnet interconnectivity (costs to be included in Contractor proposal).

Provide statement referencing publically available information affirming that the address of the Offeror's proposed data center facility location in relation to the location of the OARnet pops.

ATTACHMENT SEVEN: MANDATORY REQUIREMENTS

MANDATORY REQUIREMENT: The Offeror's data center facility must be served by an alternative power and telecom substation than that of the SOCC in Columbus Ohio for which AEP is the current provider at the SOCC. or AEP may be used at the proposed site provided there is sufficient diversity in transmission, control and substations.

Provide statement on the letterhead of each of the providers of the power and telecom services confirming that the Offeror's proposed facility is on a separate substation from the State of Ohio's SOCC, or if using AEP, there is sufficient diversity in transmission, control and substations.

ATTACHMENT SEVEN: MANDATORY REQUIREMENTS

MANDATORY REQUIREMENT: The Offeror must have provided hosted or cloud based managed server and storage solutions within the last five years for at least one customer. The Offeror must have supported for that customer at least 300 Windows, Linux or Unix variants for a period of no less than one year. The Offeror must have supported for a customer at a total storage capacity of at least 100TB for a period of no less than one year.

Customer Name:		Contact Name: (Indicate Primary or Alternate)	
		Contact Title:	
Customer Address:		Contact Phone Number:	
		Contact Email Address:	
Site Name:	Site Address:	Beginning Date of Experience: Month/Year	Ending Date of Experience: Month/Year
Provide a detailed description of services provided to meet the requirement, including the number of Windows, Linux or Unix variants and the total storage capacity:			

ATTACHMENT EIGHT: OFFEROR REQUIREMENTS

Requirement: The Offeror must have provided data center facility services to at least three companies for the preceding two years using the proposed site or one large company that is using the site in excess of the State's requirements. (Duplicate form as necessary)

Customer Name:		Contact Name:	
		Contact Title:	
Customer Address:		Contact Phone Number:	
		Contact Email Address:	
Site Name:	Site Address:	Beginning Date of Experience: Month/Year	Ending Date of Experience: Month/Year
Provide a detailed description of services provided to meet the requirement:			

**ATTACHMENT NINE:
STANDARD AFFIRMATION AND DISCLOSURE FORM
EXECUTIVE ORDER 2011-2012K**

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 will perform no services requested under this Contract outside of the United States.

The Bidder/Offeror will 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 NINE - CONTINUED

**STANDARD AFFIRMATION AND DISCLOSURE FORM
EXECUTIVE ORDER 2011-12K**

Governing the Expenditure of Public Funds on Offshore Services

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)

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)

ATTACHMENT TEN OFFEROR COST PROPOSAL

Offerors must use the electronic Cost Proposal form attached to this RFP. The embedded Cost Proposal form is for reference purposes only. No changes may be made to the cost proposal formulas. Submission must be in excel format and not as a PDF.

SUPPLEMENT 1

FACILITY AND SERVICE REQUIREMENTS

This Supplement is organized as follows:

Page No.

Part 1:	Business Overview and Summary Objectives	1
Part 2:	Key Date Requirements	1
Part 3:	Offeror Facility Requirements	3
Part 4:	Disaster Recovery as a Service (DRaaS) Requirements	9
Part 5:	Storage Replication as a Service (SRaaS) Requirements	13
Part 6:	Location of State Specialized Equipment (SSE) Requirements	18
Part 7:	Service Level Requirements for DRaaS, SRaaS and SSE	19
Part 8:	Services Responsibility Matrix (State and Contractor) Requirements	26

Each will be presented in turn. Offerors are to respond to each section in this Supplement.

Part 1: BUSINESS OVERVIEW AND OBJECTIVES

Business Overview and Summary Objectives

The State of Ohio Office of Information Technology (OIT) has identified the need for the provision of secondary data processing sites, Disaster Recovery as a Service (DRaaS), Storage Replication as a Service (SRaaS) and provision for Specialized State computing equipment to support certain disaster recovery functions for systems maintained and operated in the State's primary data centers. While the preponderance of data processing for the State is performed at the State of Ohio Computer Center (SOCC), the State also processes data in other centers located in and around the greater Columbus Ohio Area.

Following the State's review of its data processing facility assets and capabilities, a strategy has been identified that is designed to consolidate greater Columbus area data processing facilities in such a manner as to potentially reduce costs, increase service levels to users of these computing assets, better provide for the protection and privacy of State computing assets and related data. Based on this strategy, the need for a geographically and technically diverse data processing facility (second site) to support DRaaS and SRaaS functions for State critical systems and data has been identified and is included in Statewide Agency IT plans for critical systems. The end goal of the State is to acquire a set of services to support the business continuity of State critical computing (collectively DRaaS and SRaaS as well as location of State specialized equipment) that meets the State's requirements with regard to: location, capabilities, services, features, service levels and other technical considerations.

Based on a review of the current IT facility portfolio, due to geographic and technical diversity considerations, the State does not currently maintain a suitable capability to support these business continuity functions and related services and is interested in current market offerings for same. In addition, and as part of this review, the State has determined that recent technology advances in server, storage and network virtualization, dense computing, as well as a general migration from mainframe processing to distributed computing has allowed the State to formulate a strategy to consolidate systems maintained within Agencies in the greater Columbus area to the SOCC, and in addition within the SOCC to a more significantly more efficient use of the capabilities of the facility than contemplated when it was designed in the late 1980s.

In short, the State requires geographically and technically diverse facilities and services to compliment and support those offered via the SOCC for State critical computing functions.

Part 2: KEY DATE AND SERVICE SETUP/ESTABLISHMENT REQUIREMENTS

As part of their response, Offerors are to provide an indication of the following dates pertaining to the State's occupancy and use of the Site. Offerors are to note that the State's current requirement to begin detailed design

and provisioning of “in facility” features such as racks, cages, floor space, layout and the like is currently April 1, 2015 with a phased move in and bringing the contracted services fully operational over the course of April 1, 2015 through July 1, 2015. Offerors are encouraged to provide additional dates that they believe are important to the State in decision making, as Offerors deem necessary. Key Dates include:

Site Available for Facility Survey, Design and Planning	April 1, 2015
Site Available for State computing space installations	May 1, 2015
Site Available for network/connectivity planning/assessment	April 1, 2015
Site Available for Operation at scale for intended purpose	July 1, 2015
DRaaS Services Available for Design	June 1, 2015
SRaaS Services Available for Design	June 1, 2015
DRaaS/SRaaS Service Live for Initial State Use	July 1, 2015

Service Setup/Establishment Activities and State MBEs

As this RFP has provisions to use State MBEs, evaluation components and elements of cost associated with MBEs, the State has created two categories of work associated with the service: Service Setup/Establishment Activities and Service Operation Activities. The State believes that there are opportunities to leverage the MBE community with regard to Service Setup/Establishment as follows:

Service Setup/Establishment (MBE Community Involvement Opportunity)	Service Operation Activities (Not Subject to MBE Involvement)
<ul style="list-style-type: none"> ▪ Site Preparation Activities (e.g., Space, HVAC, Conditioning etc) ▪ Purchase Server Hardware and Ongoing Maintenance Services ▪ Purchase Storage Hardware and Ongoing Maintenance Services ▪ Purchase Network Hardware and Ongoing Maintenance Services ▪ Installation, Provisioning and Certification/Testing of purchased equipment ▪ Liaising with State technical teams in the setup of the DRaaS, SRaaS and SSE (as applicable) 	<ul style="list-style-type: none"> ▪ Operations and Maintenance of DRaaS, SRaaS and State SSE ▪ Participation in Audit and Security Functions (Supplement 2) ▪ Other Work Areas not mentioned above

This RFP’s cost collection workbook includes a tab dedicated for Offerors to report the nature, extent and value of the MBE involvement in the Offeror’s solution, Offerors must report as required in the cost proposal workbook.

Part 3: OFFEROR FACILITY REQUIREMENTS

This section contains the facility requirements for the Offeror Proposed facility. It is the goal of the State to identify and secure a data center facility that is sufficient to perform both as an alternate data processing facility to the State of Ohio Computer Center (SOCC), and support the State’s disaster recovery planning and implementation processes as required by Agencies.

These requirements are specific to the facility and that the actual design of building IT services in support of the State’s data processing and disaster recovery requirements are contained in subsequent parts of this Supplement, but are heavily reliant on the achievement of the facility requirements described herein. The State will retain responsibility regarding State provided computing, storage and network equipment located at the Contractor provided facility for State computing inclusive of assets, data and related business processes and documentation.

This section contains the following requirement areas, each with a brief description of requirements and assumptions:

Requirement Area	Contents
Site Scope Requirements	a high level outline aggregate space calculation for anticipated data processing center elements of the facility;
Site Attributes Requirements	other elements that may assist the State in access, use and egress to the building with additional considerations regarding local “street level” attributes
Site Connectivity Requirements	requirements for connecting to various State and public data and voice network(s)
Site Location Requirements	attributes that may allow the State to determine the suitability of the location and placement of the data center within the State and key considerations regarding determining the suitability of the site from a geographic perspective;
Site Power Requirements	a calculation of the power requirements in light of the assumed usage and occupancy of the facility
Site HVAC Requirements	requirements for providing adequate heating, ventilation and cooling for State computing equipment, Contractor equipment providing services to the State, and for personnel
Site Physical Security Requirements	requirements for the security and control of access to State space and equipment (DRaaS and SRaaS security requirements are contained later in this Supplement)
Facility IT Support Services Requirements	IT services requirements based on facility driven elements that support State use of the Contractor provided services.
DRaaS	IT services requirements based on facility driven elements that support State use of the Contractor provided services.
SRaaS	IT services requirements based on facility driven elements that support State use of the Contractor provided services.
Accommodation of Specialized State Equipment (SSE) Requirements	IT services requirements based on facility driven elements that support State use of the Contractor provided services.

For purposes of conveying industry standard definitions and requirements, the State requires that all data center space meet or exceed the conventions established by either TIA 942 or Up Time Institute™ in classifying data center Tier Standards (<http://www.uptimeinstitute.org/>) As a matter of convenience, and given the general similarity of these standards, TIA 942 and Uptime Institute™ Tier II capabilities are used interchangeably and

without preference by the State for purposes of this RFP, given the lower tier preference of the State in consideration of the site's use (e.g., DR) and in light of anticipated cost considerations (e.g., non-active processing). All Site capabilities pertaining to this RFP in support of computing, networking and related activities will be classified as Tier II space, which in general must provide multiple power and cooling distribution paths, but only one path active at any given time; maintain fully redundant components; and be concurrently maintainable without interruption to operations for maintenance activities.

Site Scope Requirements:

The State requires that the Offeror facility be capable of supporting critical computing functions during the period in which a disaster or emergency condition is declared at a State primary computing site. The Offeror's response must accommodate a Tier II raised floor data center space ranging from 1,320 sq. ft. up to 7,000 sq. ft. as indicated in the Offeror Cost Proposal Form inclusive of: Offeror provided DRaaS, SRaaS and State specialized equipment requirements.

In addition, and at the discretion of the State, the Site could be utilized in the future as an alternate data processing facility for primary production purposes or to support non-production systems development activities. Therefore, the processing model for the building must be able to support: active processing, passive processing and data replication, alternate primary processing, alternate secondary processing and these models have been contemplated in assembling the facility requirements. The detailed design and implementation of the processing capabilities of the services within the building and the connectivity to the building will be developed over the course of Fiscal Year 2015 in collaboration with State Agencies that will leverage the contracted services.

From a size stand point these options are unlikely to materially change the overall size of the facility but may influence the future configuration of the data center, as well as the power distribution and HVAC considerations for a completely active back up of State servers, storage, applications, configuration, data, working files and interfaces (that serves as a basis for a more active/expedient restoration of service in the event of a disaster).

To provide some degree of insight into the State's rationale and assumptions related to these requirements, the following is the State's current requirement set for the calculation of Tier II raised floor data center space:

1. Distributed Computing space to accommodate the State's DRaaS, SRaaS, Contractor and State network devices and other Specialized State Equipment that support virtual server hosts in modern 42U racks: 1,320 sq. ft.
2. Provision for up to 500 square feet for E911 infrastructure, backup check printers, scanners or other specialized State equipment to operate in an emergency or disaster situation.

For the DR Site: Total = 1,320 sq. ft. of required raised floor rack space for distributed computing servers up to 1,820 sq. ft. of raised floor space in the event that the State requires the location of check printers or other specialized devices.

3. In addition, the State would like to maintain a modest degree of additional space for future growth, which has been calculated at 25% of the baseline requirements, described above.

Estimated Total = up to 455 sq. ft. of raised floor rack space for future growth and service expansion

Administrative, Personnel and Common Space

4. Site must support initial service establishment projects, periodic work locations for common, administrative and personnel up to 20 staff during a declared emergency or disaster testing period to operate the equipment in light of the disaster condition. In addition, ad hoc meeting rooms that support 10-20 people are also required.

Estimated Periodic Administrative, Personnel and Common Space = 1,000 Sq. Ft.

Offerors are to note that there are a variety of State requirements and configurations that may be implemented at the Contractor site. As such, Offerors are instructed to complete the provided Offeror Cost Proposal Form based on the square footage requirements contained therein. The State's use of the space may vary over time based on the State's needs at any point in time.

Site Attributes Requirements:

The Offeror's Site must be accessible from a vehicle from major airports, shipping locations to speed the delivery of personnel, equipment, running supplies such as diesel replenishment, and shipping/delivery of media stored in off-site secure locations.

1. Clearances, inclines ramps, double doors and similar capabilities must facilitate the ease of moving equipment and devices to the building and within the building (while not sacrificing security, fire, power and cooling distribution considerations)
2. Use of containerized, or self-contained/dedicated data center provisions (within the Contractor's Tier II facility) is an acceptable means of delivering State required space, so long as other access/egress for equipment delivery and location purposes, heating, cooling power and networking and security requirements are met as specified herein.
3. Space above the drop ceiling (or beneath the floor) where ducting is routed must be sufficient to support the power density and waste heat removal commensurate with power densities mentioned elsewhere in this RFP.
4. An unobstructed pathway must exist among the Data Center, its corresponding storage room, and the exterior of the building, for transporting equipment.
5. The structural capacity of floors, hallways and loading areas that equipment will traverse must support contemporary use and standards as a data center.
6. The loading dock must be placed in such a manner as to ensure that servers, cabinets, networking devices, or backup storage units are not exposed to damage (due to collisions or prevailing weather conditions) during transport to and within the Data Center.
7. The loading dock must allow equipment to be rolled a short distance across level ground, either directly into the server environment or an associated storage room, rather than having to be offloaded from an elevated truck bed and shuttled a longer distance.
8. Should a freight elevator be required within the Site to access the computing facility, the freight elevator must be at least 8 feet (2.4 meters) high and at least 4 feet (1.2 meters) wide so as to accommodate everything from tall server cabinets to wide pallets of equipment.
9. The freight elevator must also have enough weight-bearing capability to carry a fully loaded server cabinet up to 1,500 pounds per server cabinet location.
10. The Site's water pipes (supply and distribution) must be routed around or away from the data processing area or utilize containment techniques as to not pose a leakage threat to the computer processing equipment in the Site.
11. The Site's non-data processing, administrative and common areas must not be situated as to cause a fire hazard to the data processing, mechanical, control and telecommunications areas that support the data processing areas of the Site.
12. During a declared emergency condition affecting the State's primary site, and the State's operation of systems at the Contractor provided facility, the Contractor will allow the State to temporarily activate a wireless local area network to serve the State emergency response team in operating systems until such time as the emergency condition is resolved. Following this resolution, this network will be deactivated and not used.
13. The State does not have a preference for either raised floor or overhead wiring, Offerors are to specify which wiring routing (e.g., under floor tray or overhead race) is the standard for their proposed facility. Notwithstanding wiring considerations, all other Tier II/TIA.942 conventions must be adhered to as well as

HVAC, fire suppression and other attributes required by the State or defined in the aforementioned Standards.

Site Connectivity Requirements:

1. Building connectivity must be logically divided into non-State connectivity and State data connectivity.
2. The site must offer connectivity to OARnet's backbone (via a point-of-presence or an OARnet tail circuit), a minimum of 10Gbit/sec. Most OARnet POPs are serviced by 100Gb/s links.
3. All connectivity from the SOCC to any OARnet pop will be provided by the State, any onwards connectivity from the OARnet POP to the Contactor site will be the responsibility of the Offeror. Any intra or inter data center connectivity within the proposed sites to devices that will provide the State's service (collectively DR, DR and SSE) is the responsibility of the Offeror and should be included in the Cost Proposal.
4. This connectivity must provide alternate paths that do not share common physical cabling or conduits to OARnet for redundancy and diversity.
5. The cost to connect and operate the Contractor's facility connection to OARnet will be incurred by the Offeror and included in this RFP Cost Proposal Form.
6. Should OARnet not be directly serving the Offeror's facility, the State will view existing service (or service that can be provisioned) to the site by one or more of: the State's existing providers to the SOCC including Time Warner Telecommunications, AT&T, Qwest, Verizon or Time Warner Cable as a positive as this may allow for more efficient network configuration. (e.g., a VPN, Metro-E or direct connect will take fewer hops across a single carrier's circuit).
7. The Contractor will work with the State to ensure that this connection is operational no later than ninety (90) days following the execution date of any agreement that arises from this RFP.

Site Location Requirements:

As part of the evaluation and award and this RFP, the State is seeking to identify a site to perform these services: consisting of a primary Disaster Recovery site for performance of DRaaS, SRaaS services and the location of State Specialized Equipment (SSE) called "Primary DR Site".

The Offeror proposed facility must be sufficient distance from the primary site, in this case the SOCC (in order to provide geographic, telecommunications and power diversity). In order to be a Tier II site, the location must allow for alternate power substations, and alternate connectivity distribution paths

1. The Site will be less than one-hour distance commute from a major Airport, Train/Rail Facility or Public Transportation
2. Connectivity and network devices may be located in other States than Ohio (but within the United States), but all servers and storage associated with the site and Service must be located within the State of Ohio.
3. Power uptime 99.741% (or higher) as measured at the rack and verified through inspection of the site elements that power the rack (e.g., cabling, PDU, riser(s), UPS, Diesel, commercial power, switching and the like).
4. The Site will include provisions for truck access for equipment delivery
5. The Site must be accessible via common vehicle in all weather conditions
6. The Site must be handicap/disabled/ADA accessible with provisions for handicap/disabled parking places building access, restrooms and other accommodations as to support this type of access.
7. The Site must be served by a local Police and Fire department. Average response time of that local department must be provided.
8. The Site must show how there are multiple access/exit routes to and from the location.

Site Power Requirements:

The Offeror proposed site must be served from a commercial power substation that is separated and diverse from that powering the State's SOCC at 1320 Arthur Adams Drive, Columbus. AEP is the current provider at the SOCC, and AEP may be used at the proposed site provided there is sufficient diversity in transmission, control and substations.

1. The Site will include an uninterruptable power service (UPS) and the UPS must be supplied by a generator system sufficient to power the State's facilities within the Site until such time as services are restored to the primary site in their entirety.
2. The Site will include a generator that must be capable of running the State's facility as long as fuel is available and maintain provisions for local replenishment from a reliable source before on-site fuel is depleted.
3. Incoming power has been calculated for at least 7.5KW/h watts per rack, which is contemporary with modern Tier II data center design considerations and intended State use and support of Contractor provided DRaaS and SRaaS services

Site Heating and Air Conditioning (HVAC) Requirements:

Heating Ventilation and Air Conditioning will be configured to support the State in the building prior to occupancy (generally Computer Room Air-Conditioners CRACs). The building owner/landlord must provide ductwork to ensure proper data center centric cooling options.

1. HVAC capabilities of the facility must provide for contemporary and efficient design techniques, which include one or more of floor to ceiling, ceiling to floor, hot row/cold row as well as raised floor heating and cooling.
2. The Site must be able to support a mean temperature of no greater than 78 degrees Fahrenheit for all raised floor (i.e., computing and related elements) at the power density (7.5KW/h per rack) required.
3. The Site must support a mean temperature of no greater than 75 degrees for common, administrative and personnel occupied location(s).

Site Physical Security Requirements:

1. The Contractor will be responsible for providing and managing 24 hour, 365 day per year security personnel who will strictly limit access to any State space, computing devices and other elements in the facility that provide service to the State.
2. The site will have cameras installed, monitored and recorded (DVR) in all public accessible, vital and State occupied locations. Recordings will be maintained for at least thirty (30) days and, upon reasonable request, the State will have right to review all access to the portions of the Contractor facility via these cameras and their recordings.
3. The State will be permitted to install its own cameras in State occupied spaces for State remote monitoring of State computing operations, assets and access.
4. Cages around State equipment must go from physical deck floor to deck/hard ceiling (to prevent unwanted access to State equipment)
5. Notification of unapproved entry to State elements or State vital portions of the Site will be reported to the State Chief Information Security Officer (CISO)
6. The State will have the ability to install and utilize secured (locked, via key code, badge or biometrics) racks within the space dedicated to the State
7. All entries (authorized or unauthorized) to the space utilized by the State will be tracked by the Contractor and these tracking records will be made available to the State upon request.

SSAE 16 Type 2 Reporting Requirements:

1. No less frequently than every calendar year, the Contractor will be responsible for supporting the State in conducting an independent third party SSAE 16 audit (Statements on Standards for Attestation Engagements No. 16, which superseded SAS-70 in June of 2011). The independent third party will be a nationally recognized firm qualified to perform such audits.
2. The SSAE 16 audit will cover at least the preceding six month period for the Contractor service locations or service types.
3. The audit will be a SSAE 16 SOC 1 Type 2 covering the common processes controlled and performed by the State and Contractor at primary Contractor locations in administering State accounts. A copy of each of the resulting audit reports will be delivered to the State no less than 45 days following the conclusion of the SSAE 16 audit.
4. The scope of the Contractor SSAE 16 Type 2 audits must include the elements of service including the physical environment, hardware, software and services as relevant supporting the State environment.
5. It is the sole obligation of the Contractor to remedy any written issues, material weaknesses, or other items arising from these audits, after mutual agreement on the underlying cause, as they pertain to services or capabilities provided by the Contractor to the State in conjunction with the Statement(s) of Work in effect at the time of the Audit. For items that arise as a result of State policies, procedures and activities, after mutual agreement on the underlying cause, remedial activity requirements and plan, State agrees to work, and under agreed terms, to effect the required changes to the Services delivery model to remediate issues discovered under a SSAE 16 Type 2 audit.

Facility IT Support Services Requirements:

The Contractor will be responsible for the management of all aspects of the facility and surrounding grounds, building operations and security and monitoring. The services, via this facility should be designed to provide continuous up time for the Service. The Contractor will operate all related systems as part of the Service including servers, storage, network elements, facility controls, battery and generator backup power feeds, communication feeds and redundant components in all critical systems, such as air conditioning, electrical distribution, fire protection, UPS systems and a building management system (BMS).

Services under this contract include the continuous operation of the computer and telecommunications equipment installed within the facility that supports State use of the Services.

The Offeror that is awarded this Contract will be responsible for the management, maintenance and tenant services described in this document.

The Offeror facility must be managed and maintained in accordance with all current industry standards and regulations and those designated in this RFP, including but not limited to the following:

1. Contractor must be responsible for managing and maintaining all building systems to the manufacturer's specifications and recommendations.
2. All systems/equipment identified in supporting the State's use of the Site must be maintained utilizing factory authorized service contracts.
3. Contractor must maintain current licenses and permits required by administrative rules, statutes, or other legal authorities.
4. Contractor must maintain and update operating manuals and blueprints for the State.
5. Contractor must prepare and submit a Standard Operating Procedures (SOP) manual describing the policies and procedures for the Contractor to use in operating the 2nd Site/DR Data Center Site. This manual must be submitted to the State Site Facilities Manager for review and approval within 60 calendar days of award of the Contract. Contractor must provide an electronic copy to the State and update and keep the manual current through the life of the Contract.

6. Design and coordinate installation of data cabling with the State Unified Network Service Provider and OARnet.

System Maintenance: The Contractor will be responsible for managing and maintaining, and demonstrating to the State that the systems and services listed below are maintained in accordance with manufacturer requirements (if applicable to the Contractor facility or Service).

- Uninterrupted Power Source (UPS)
- Emergency Generator Systems
- Emergency Power Off (EPO) System
- Electronic Control Systems
- Building Mechanical System
- Building Electrical System
- Building Plumbing and Water Treatment System
- Security and Closed Circuit TV Systems
- Heating/Ventilation/Air Conditioning (HVAC)
- Elevators
- Automated Fire Detection / Protection / Suppression systems
- Under floor Structured Cabling Systems
- Any other building system not listed here.

HVAC Operation and Maintenance: HVAC operations and maintenance will include all in-house and contract personnel that operate and maintain the central HVAC plant and associated equipment, chillers, ice tanks, cooling tower, various pumps and motors, boilers, units, air handlers and central systems.

Contractor must provide a method of energy accounting of the State's portion of the building's utility expenses for those services provided independent of DRaaS and SRaaS contained herein. This system must be capable of providing energy use and variance reports. The Contractor will use this information to make appropriate utilities conservation recommendations to the State for consideration.

Part 4: Disaster Recovery as a Service (DRaaS) Requirements

The State maintains a variety of IT systems that are designed to support critical and non-critical State functions, several of which will be the focus of this Service. In general these systems will be prioritized by the State and incorporated by the State to utilize the Contractor's provided DRaaS service based on their priority and criticality to the State, but will initially include those that support and provide: Public Safety and Security to the citizens and businesses of Ohio; State revenue collection and State operations of critical functions; and citizen facing life critical services in the health, human services and support domains, all of which are offered by a variety of State Agencies, Boards and Commissions. In general, the State will be responsible for the identification, design and implementation of DR services (or Recovery as a Service in general: RaaS) from an applications, infrastructure, data and business continuity perspective, but will be reliant upon the Contractor's provided facility and the DRaaS contained herein.

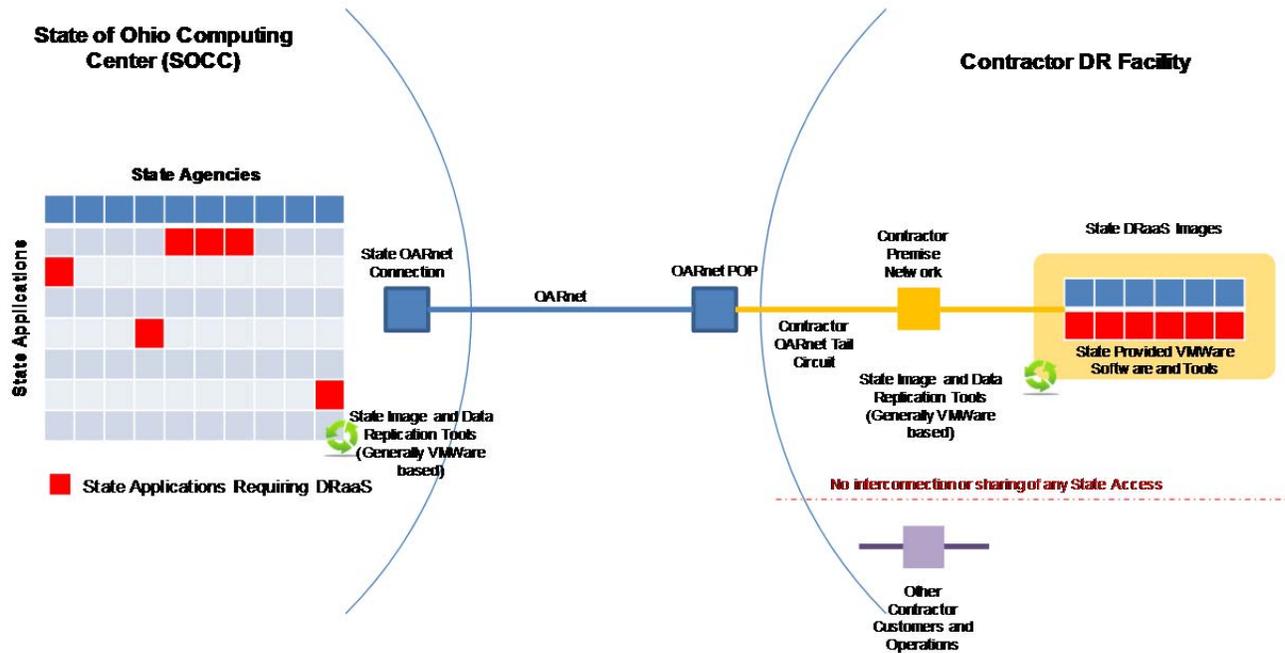
Offerors are to note that the Cost Collection form associated with this RFP includes the provision for a Termination Fee Schedule. Offerors are encouraged to populate this schedule with the cost of those assets that are procured and installed exclusively for State use that cannot otherwise be deployed or reconfigured to serve other customers of the Contractor following the termination of any agreement arising from this RFP prior to the term of the RFP and any extensions as allowed for under Attachment Four of this RFP.

The State will implement VMware site recovery manager. The fail back will be controlled via the hypervisor. For servers outside of site recovery manager (e.g. SQL clusters, physical servers for application platforms) fail back will be controlled by application level controls. Storage failover and failback will be handled by the IBM SVC

storage hypervisor managed by the State of Ohio Storage Team. Failover will require the State of Ohio Storage Team to change the DR site storage from read only target to active read/write. Failback will be require reverse path storage replication followed by a coordinated storage/server/application switch back.

In general, this Service can be viewed as follows:

Conceptual Scope: DRaaS



The Contractor will organize and provide Disaster Recovery as a Service (DRaaS) as follows:

- Install, Provide, Operate and Maintain Windows, x86 (Linux) and Certain Unix Operating System Machine Images
- Utilize State Provided VMWare Licenses for Provision of Services
- Implement, with State Collaboration, VMWare based DRaaS Support Technology

Details and requirements for each will be presented in turn.

4.1 Install, Provide, Operate and Maintain Windows, x86 (Linux) and Certain UNIX Operating System Machine Images

The Contractor will:

- Acquire, install and provision x86, and upon request of the State (outside of this RFP, but under any contract arising from this RFP) certain Unix virtual machine hosts to support DRaaS services
- Upon receiving an Authorized service update request from the State in a mutually agreed format, the Contractor will provision a virtual machine image for the State and provide host name details, login/password and other credentials in order for the State to establish the DRaaS services
- Support the State in the identification and resolution of initial image provisioning issues such that the DRaaS may commence
- Add the provided image to the Contractor provided services inventory report and be authorized to bill the State for the image

- Monitor the availability and performance of the provided image(s) and produce a monthly report to the State as part of monthly Contractor invoicing processes
- Accept image Add/Change/Move requests from the State and process these requests in accordance with the Services Responsibility Matrix and applicable Service Level Agreements
- Establish with the State a calendar of maintenance and planned outage schedules that factors State processing criticality/availability requirements, seasonal processing, DRaaS testing services and other business events
- Allow the State to apply any security, system, operating system or other updates as to adhere to State security and privacy policies
- Install any Hardware level updates (e.g., BIOS, microcode, device drivers and the like) that require physical access to the machine(s)
- Maintain all hardware devices in accordance with State Standards contained herein or as modified and communicated to the Contractor in writing in advance of the change to these Standards
- Track, monitor and provide remediation for solution defects and incidents requiring system configuration or in-scope environment code or configuration changes;
- At State direction, identify, test, install and implement Third Party contractor-supplied patches and fixes for Third Party contractor-supplied packaged systems software (including OS, BIOS, microcode, patches, service packs and similar), as well as new releases.
- Comply with any State security mandated patches or system levels to the extent and system enhancement turnaround time required given the nature of the security mandate.
- Allow User access to the Contractor trouble ticketing system that contains all open tickets managed by the Contractor for that State as well as all Service Level impacting items, whether State or Contractor identified, in accordance with the mutually agreeable operations guides and supporting documents.

The State will:

- Be responsible for configuration, operation, data replication, database and application level and business continuity functions that utilize the Contractor provided DRaaS server images.
- Be responsible for working with the Contractor to schedule and execute regular (no less frequently than annually) Disaster Recovery Tests. Based on the outcome of these tests the State and Contractor agree to meet and the Contractor will address any items pertaining to Contractor provided DRaaS elements; support the State (where required) in addressing State/Contractor shared or co-dependent DRaaS elements; assist the State (where commercially reasonable) in resolving complex DRaaS elements.

4.2 Utilize State Provided VMWare Licenses for Provision of Services

The State maintains a variety of VMWare based software tools and elements that it uses to conduct virtualization and virtual image management, replication, provisioning and planning services. The State will provide to the Contractor, for State use only, select elements of its licensed VMWare software and tools for use in the provision, implementation, operation and maintenance of the DRaaS.

In general a variety of tools and approaches will be utilized by the State, with particular emphasis (for Contractor skill planning purposes) on VMotion and VMWare Site Recovery Manager. The contractor will demonstrate its acceptance of this requirement and its ability to perform VMWare specific services aligned with these tools as part of its response. The State will implement VMWare site recovery manager. The fail back will be controlled via the hypervisor. For servers outside of site recovery manager (e.g. SQL clusters, physical servers for application platforms) fail back will be controlled by application level controls. Storage failover and failback will be handled by the IBM SVC storage hypervisor managed by the State of Ohio Storage Team. Failover will require the State of Ohio Storage Team to change the DR site storage from read only target to active read/write. Failback will be require reverse path storage replication followed by a coordinated storage/server/application switch back.

The Contractor will:

1. Demonstrate expertise and provide qualified personnel to design and implement the initial DRaaS service in collaboration with the State.
2. Provide support for the DRaaS service through the application and installation of regular updates to the State provided VMWare software for those instances where these services cannot be performed remotely by the State
3. Assist the State in rebooting or performing other “smart hands” functions that require physical access to the hardware providing the DRaaS service upon written direction from the State.
4. Return all State provided software at the conclusion of any contract arising from this RFP.
5. Not permit any third party access to State provided software under any circumstances, or utilize State provided software for any other purpose than to provide services to the State.

The State will:

1. Provide the Contractor access to State software to be installed on Contractor equipment for State use;
2. Provide applicable documentation, releases, patches, updates and other VMWare provided materials to the Contractor in conjunction with the Contractor's responsibilities contained herein; and
3. Provide the Contractor State licenses for operating systems and other required software packages as required to host State DRaaS images and the applications that utilize these images.

4.3 Implement, with State Collaboration, VMWare based DRaaS Support Technology

The State will be responsible for the design, implementation and operation of State initiated virtual machine image replication services originating from or utilizing State virtual machine images. As the overall DRaaS service is based upon the availability, configuration and capacity of Contractor provided DRaaS services, the Contractor will support the State in:

- Designing and implementing, following State review and approval, all Contractor DRaaS facility based infrastructure components inclusive of network(s), racks, connectivity, power, cooling, space, hardware, storage and security devices to deliver the overall DRaaS as contracted;
- For UNIX based environments or State environments that cannot be virtualized, the State will require the Contractor to provide basic rack space, power, cooling and network connectivity for State provided UNIX hardware or machines that cannot be virtualized under VMWare products;
- Implementing virtual DRaaS images under the design direction of the State and in adherence with State Virtual Machine Standards contained herein;
- Incorporating State application specific design considerations based on Agency needs as conveyed in writing to the Contractor by OIT that may include baseline server images, configuration values, patches, updates, additive software or software enablers, network bandwidth requirements (within the capacity of the network between the State and Contractor site), exceptional processing and availability requirements, data privacy and security requirements and other factors as required to establish, operate, regularly test and decommission (when appropriate) the DRaaS services;
- Providing the State with inventory reports for all images included in the DRaaS inclusive of operating configuration values (in aggregate), capacities, run-time statistics and other items as mutually agreeable for both parties to monitor, manage and maintain the overall hardware that comprises and supports the DRaaS; and
- Working with the State prior to technology obsolescence or refresh cycles to revisit these designs in light of then contemporary hardware, storage, network and security Standards and capabilities to plan, design and implement new hardware over the course of any contract arising from this RFP that are designed to leverage technology advancements, provide a better Service as a result of these technology advances, and migrate the State's use to these new technologies while minimizing unplanned outages to the State's contracted DRaaS service.

4.4 State Virtual Machine Standards

The Contractor will provide machine images that utilize the following specification standard regardless of hosting x86 or Windows DRaaS images. Servers in this category are expected to have a planned service life of five years. Servers are expected to be acquired with a five-year on-site, next-business-day warranty. Options are available for extending the warranty to on-site, four-hour response may be requested by the State at an additional cost.

Specification for Standard Configuration Servers	
Processor	2 socket Intel Xeon E5-2670 v2 Processor
Memory	Memory to CPU Core ratio of 8GB per core. 10 x 16GB PC3-14900R Dual Ranked Memory
Network Adapter	Integrated Dual 1 Gigabit Controller or Integrated Dual 10 Gigabit Controller
Hard Drive	Optional
Power Supply	Dual Hot Swap Power Supply

4.5 Initial DRaaS Sizing Requirements

The Offeror will size and propose (in the Cost Collection Workbook as part of this RFP) baseline sizing based on the following configuration of Services. Offerors are to not include any OEM Operating System Licenses or VMWare software as this Service will utilize State provided licenses for all environments:

Image Type	DR Site	
	Initial Images based on Standard Configuration Server	Additional Images Purchased in Blocks of:
Windows x86	1500	100
Linux	250	50
AIX *	50	10

* Offerors should be prepared to support AIX based DR/SR services per the requirements in the RFP. Currently the State maintains approximately 90 AIX images on approximately 10 physical hosts, some of which will require DR/SR services. The actual quantity is not yet determined.

The State currently supports vCenter 5.5 Update 1, SRM 5.5, DCs run on Windows 2008 R2 Server Platform, DHCP served from Windows 2008 R2 Server Platform, AD 2008 Native Level. In addition, The State supports ESX vSphere 5.5 Update 1 or higher, Windows Server 2003R2 or higher, AIX 5 (or higher) Linux Red Hat 4.0 or higher, SUSE 9.0 or higher.

Initial images are based on virtual images on an aggregate basis. In general, the State (on current equipment) is realizing a 20:1 virtual to physical server ratio. The State will monitor the availability and performance of VSXi remotely. Should the State require local assistance (e.g., physical server reboot or network reset etc) the Contractor will assist the State in restoring remote access or physical server related tasks that require hands on access to the equipment.

Part 5: Storage Replication as a Service (SRaaS) Requirements

5.1 Overview

The State maintains a variety of IT systems that are designed to support the storage of critical and non-critical State functions and applications, several of which will be the focus of this Service. In general these systems will be prioritized by the State and incorporated by the State to utilize the Contractor's provided Storage Replication as a Service (SRaaS) storage services based on their priority and criticality to the State, but will initially include those that support and provide: Public Safety and Security to the citizens and businesses of Ohio; State revenue collection and State operations of critical functions; and citizen facing life critical services in the health, human

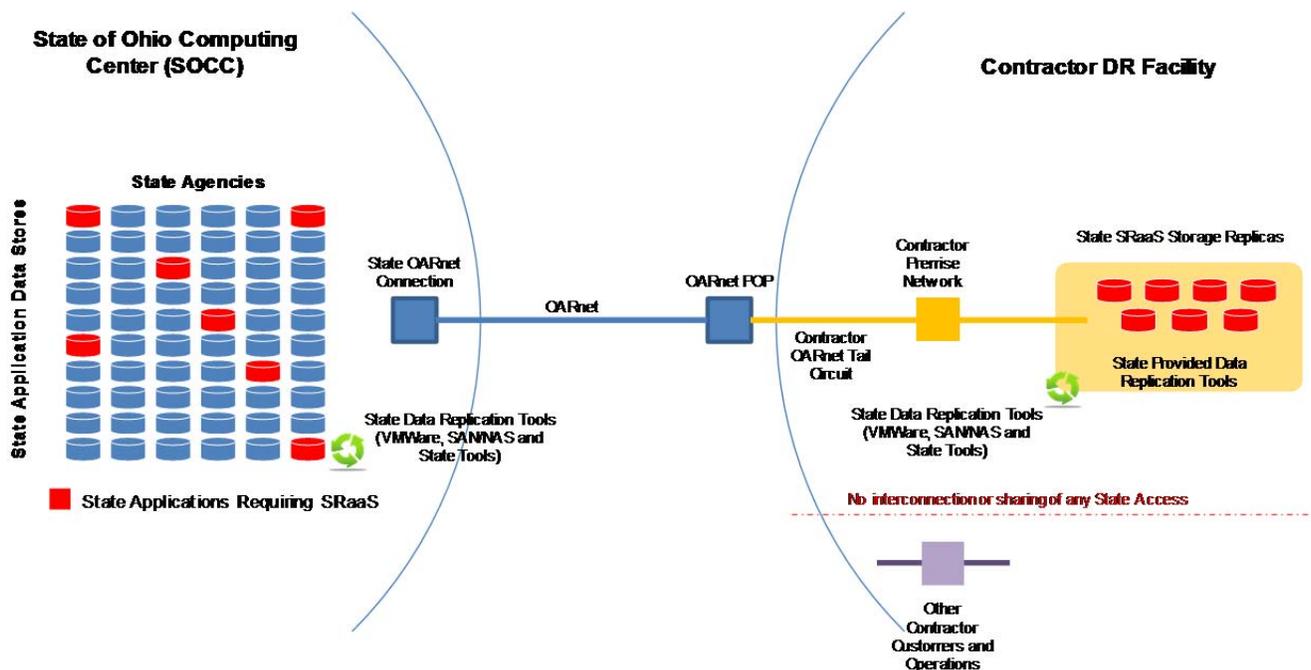
services and support domains, all of which are offered by a variety of State Agencies, Boards and Commissions. In general, the State will be responsible for the identification, design and implementation of these services from an applications, infrastructure, data and business continuity perspective, but will be reliant upon the Contractor's provided facility and the SRaaS contained herein.

In general, the SRaaS must be designed, implemented and to:

- Accept regular updates, replication, synchronization or copies of State critical data including operating system images, boot data, applications, configurations, interfaces, extensions, file systems, databases, structured and unstructured data used in conjunction with the operation of State systems (collectively: Primary Storage);
- Be designed, operated and maintained in a manner that is sufficient to perform in the event of a disaster or condition in which the State's primary data center is otherwise unavailable;
- Be aligned with the operational performance characteristics of the system(s) that require operation during the disaster/unavailable condition;
- Be available continuously to accept scheduled or real-time updates from source system(s) in the State to the SRaaS;
- Adhere to established Service Level Agreements contained herein; and
- Be implemented, operated and maintained using Contractor facility features (e.g., power, cooling, networking and other technical elements) in keeping with a TIA942 or Uptime Tier II facility.

The State will replicate its Primary Storage to the Contractor provided SRaaS and be responsible for ensuring that the data is replicated correctly, is accessible or useable in the event of a disaster or unavailability condition and is contemporary with the needs of the source State systems as to be usable during such a condition. Conceptually this capability is illustrated using the following scope diagram:

Conceptual Scope: SRaaS



The Contractor will organize and provide Storage Recovery as a Service (SRaaS) as follows:

- Install, Provide, Operate and Maintain Storage Replication Capacities as a Service

- Implement, with State Collaboration, replication based SRaaS Support Technologies

Details and requirements for each will be presented in turn.

5.2 Install, Provide, Operate and Maintain Storage Replication Capacities as a Service

The Contractor will:

- Acquire, install and provision for State access to storage upon request of the State certain Unix virtual machine storage capacities in accordance with the capacities and technical requirements contained herein to support SRaaS services;
- Upon receiving an Authorized service update request from the State in a mutually agreed format, the Contractor will provision storage for the State and provide name details, mount points, access details login/password and other credentials in order for the State to establish the SRaaS services;
- Support the State in the identification and resolution of initial storage provisioning issues such that the SRaaS may commence;
- Add the provided allocated storage to the Contractor provided services inventory report and be authorized to bill the State for the storage;
- Monitor the availability and performance of the provided storage and produce a monthly report to the State as part of monthly Contractor invoicing processes;
- Accept image Add/Change/Move requests from the State and process these requests in accordance with the Services Responsibility Matrix and applicable Service Level Agreements;
- Establish with the State a calendar of maintenance and planned outage schedules that factors State processing criticality/availability requirements, seasonal processing, SRaaS testing services and other business events;
- Allow the State to apply any security, system, operating system or other updates as to adhere to State security and privacy policies;
- Install any Hardware level updates (e.g., BIOS, microcode, device drivers and the like) that require physical access to the machine(s);
- Remove and replace any malfunctioning storage devices (e.g., disk drives) using on-site spares as required herein. For malfunctioned drives, the Contractor will either: provide a certification of destruction for the failing storage demonstrating that no State data is readable from the malfunctioning device as a unit or as parts; or return the drive to the State or a designated State agent for the destruction of State data contained on the device;
- Maintain all hardware devices in accordance with State Standards contained herein or as modified and communicated to the Contractor in writing in advance of the change to these Standards;
- Track, monitor and provide remediation for solution defects and incidents requiring system configuration or in-scope environment code or configuration changes;
- At State direction, identify, test, install and implement Third Party contractor-supplied patches and fixes for Third Party contractor-supplied packaged systems software (including OS, BIOS, microcode, patches, service packs and similar), as well as new releases;
- Comply with any State security mandated patches or system levels to the extent and system enhancement turnaround time required given the nature of the security mandate; and
- Allow User access to the Contractor trouble ticketing system that contains all open tickets managed by the Contractor for that State as well as all Service Level impacting items, whether State or Contractor identified, in accordance with the mutually agreeable operations guides and supporting documents.

The State will:

- Be responsible for configuration, operation, data replication, database and application level and business continuity functions that utilize the Contractor provided SRaaS storage.
- Be responsible for working with the Contractor to schedule and execute regular (no less frequently than annually) Disaster Recovery Tests. Based on the outcome of these tests the State and Contractor agree to

meet and the Contractor will address any items pertaining to Contractor provided SRaaS elements; support the State (where required) in addressing State/Contractor shared or co-dependent SRaaS elements; assist the State (where commercially reasonable) in resolving complex SRaaS elements.

- Schedule any large scale data replication with the Contractor as to minimize network, server or storage performance issues or interruptions, or at the State's sole discretion in scenarios where these issues or interruptions are unavoidable, provide temporary relief for Service Levels during the period of these large scale data replications.

5.3 Implement, with State Collaboration, Replication based SRaaS Support Technologies

The State maintains a variety of storage replication based software tools and elements that it uses to conduct data replication, copying, synchronization, provisioning and planning services. The State will provide to the Contractor, for State use only, select elements of its licensed software and tools for use in the provision, implementation, operation and maintenance of the SRaaS.

In general these tools are as follows:

- IBM SAN Volume Controller (SVC) including Advanced Copy, FlashCopy, Tivoli FlashCopy Manager and Metro Mirror for State SAN based assets
- VMWare VSphere and Site Recovery Manager
- EMC Storage Replication Manager
- Custom Methods using Operating System features including rsync, Windows DFS, Hyper-V Replica, shell/batch scripts etc

These tools and approaches will be utilized by the State, and remote support by the Contractor to monitor, reset, reboot or reestablish data replication services with State based primary storage pools. The Offeror will demonstrate its acceptance of these requirements and its ability to perform replication specific services aligned with these tools as part of its response.

The Contractor will:

- Demonstrate expertise and provide qualified personnel to design and implement the initial SRaaS service in collaboration with the State;
- Provide support for the SRaaS service through the application and installation of regular updates to the State provided software when the State cannot perform these functions remotely for those instances where these services cannot be performed remotely by the State;
- Assist the State in rebooting or performing other "smart hands" functions that require physical access to the hardware providing the SRaaS service upon written direction from the State;
- Replace, following notification of the State any failed or failing storage devices that comprise the SRaaS;
- Return all State provided software at the conclusion of any contract arising from this RFP;
- Allow the State to supervise the secure destruction of all State data from Contractor provided devices upon the removal of the device from the Service, the failure of any device or at the completion of any contract arising from this RFP;
- Not permit any third party access to State provided software, devices or storage under any circumstances, or utilize State provided software, devices or storage for any other purpose than to provide services to the State;
- As the overall SRaaS service is based upon the availability, configuration and capacity of Contractor provided SRaaS services, the Contractor will support the State in: designing and implementing, following State review and approval, all Contractor SRaaS facility based infrastructure components inclusive of network(s), racks, connectivity, power, cooling, space, hardware, storage and security devices to deliver the overall SRaaS as contracted;
- Incorporating State application specific design considerations based on Agency needs as conveyed in writing to the Contractor by OIT that may include baseline storage volumes, configuration values, patches, updates, additive software or software enablers, network bandwidth requirements (within the capacity of the network between the State and Contractor site), exceptional processing and availability requirements, data privacy

and security requirements and other factors as required to establish, operate, regularly test and decommission (when appropriate) the SRaaS services;

- Providing the State with inventory reports for all storage included in the SRaaS inclusive of operating configuration values (in aggregate), capacities, run-time statistics and other items as mutually agreeable for both parties to monitor, manage and maintain the overall hardware that comprises and supports the SRaaS; and
- Working with the State prior to technology obsolescence or refresh cycles to revisit these designs in light of then contemporary hardware, storage, network and security Standards and capabilities to plan, design and implement new hardware over the course of any contract arising from this RFP that are designed to leverage technology advancements, provide a better Service as a result of these technology advances, and migrate the State's use to these new technologies while minimizing unplanned outages to the State's contracted DRaaS service.

The State will:

- Provide the Contractor access to State data replication software to be installed on Contractor storage equipment for State use;
- Provide applicable documentation, releases, patches, updates and other storage replication software provided materials to the Contractor in conjunction with the Contractor's responsibilities contained herein; and
- Be responsible for the initiation, verification and synchronization of all State data to the Contractor provided SRaaS originating from or utilizing State storage.

5.4 Storage Capacities, Performance and Other Technical Standards

All storage identified at this time is Fiber Channel block storage to be attached to a Cisco Dual SAN Director Class fabric (or equivalent) and required to be virtualized behind an IBM compatible VSC. The mix of various tiers are approximately 20% Performance, 60% General Purpose, and 20% Capacity as defined below from either a single or multiple arrays. The State will supply the IBM SVC infrastructure and licensing for the required storage capacities

Disk encryption for all "data at rest" is required to be provided by all vendor storage arrays. Any storage provided to meet this RFP must include disk encryption. Contractor storage must provide for encryption of all data at rest.

Storage replication will be done with IBM® SmartCloud™ Virtual Storage Center.

The State requires the following configurations for the SRaaS service based on State application performance, reliability and availability requirements:

Storage Type	Technical Requirements and Characteristics
High Performance	<ul style="list-style-type: none"> ▪ Raid 0+1 ▪ Cache 16MB or higher per drive ▪ Drive Speed 10,000 RPM or higher, 250MB/s transfer rate per drive or higher (SSD Preferred) ▪ SAN Connectivity 10Gb/E and 1Gb/E ▪ Connectivity Options: FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB, HTTP, FTP ▪ Maintain at least 10% plus One onsite spares for all total drives, network (SAN) cards and controllers ▪ Must be compatible with DRaaS Server Standards <p>Typical Uses: Life, Health, Safety, Revenue and State Critical Applications</p>
General Purpose Use	<ul style="list-style-type: none"> ▪ Raid 1 ▪ Cache 8MB or higher per drive ▪ Drive Speed 7,500 RPM or higher, 175MB/s transfer rate per drive or higher ▪ SAN Connectivity 10Gb/E and 1Gb/E ▪ Connectivity Options: FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB, HTTP, FTP ▪ Maintain at least 10% plus One onsite spares for all total drives, network (SAN/NAS) cards and controllers ▪ Must be compatible with DRaaS Server Standards <p>Typical Uses: State financial, accounting and transactional processing, State business and administrative functions, disbursements of funds, services or benefits, systems supporting development lifecycle activities</p>

	for critical systems where environment outages will result in low lost time/cost to the State
Commodity Replication / Archive	<ul style="list-style-type: none"> ▪ Raid 5 ▪ Cache 4MB or higher per drive ▪ Drive Speed 5,400 RPM or higher, 100MB/s transfer rate per drive or higher ▪ SAN Connectivity 1Gb/E or higher ▪ Connectivity Options: FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB, HTTP, FTP ▪ Maintain at least 10% plus One onsite spares for all total drives, network (SAN/NAS) cards and controllers ▪ Must be compatible with DRaaS Server Standards <p>Typical Uses: Virtual Tape Functions, Administrative File Replication, General Purpose Use, Common Office Files</p>

5.5 Initial SRaaS Sizing Requirements

The Offeror will size and propose (in the Cost Collection Workbook as part of this RFP) baseline sizing based on the following configuration of Services. Offerors are to not include any OEM Operating System Licenses or VMWare software as this Service will utilize State provided licenses for all environments:

Storage Type	DR Site	
	Initial Storage (TB) Usable Capacity	Additional Storage Purchased in Blocks of (TB) Usable Capacity:
High Performance	200	50
General Purpose Use	500	100
Commodity Replication / Archive	200	100

Part 6: Accommodation of State Specialized Equipment (SSE) Requirements

The State maintains a variety of State Specialized Equipment (SSE) that is designed to augment the State's business continuity functions in providing critical services to the general public and businesses in Ohio. These devices include, but are not limited to:

- **Check Printers and Scanners:** used for disbursement and receipt of funds;
- **High Speed/Volume Printers:** used for report generation and mailings;
- **Specialized Computing Equipment:** OEM specific high-performance devices that are not commonly or generally available in cloud based solutions (e.g., Oracle Exadata/Exalogic, Teradata Data Warehouse devices);
- **E911, First Responder, MARCS and Telephony Call Routing Equipment:** equipment used to dispatch, manage, coordinate and deliver life critical services across the State; and
- **Specialized Physical Computing Infrastructure:** infrastructure devices (e.g., Hardware, Storage, Networking and Security devices) that are State specific or otherwise cannot be offered by a Contractor due to cost, performance, availability, configuration or other reasons as determined by the State.

The State acknowledges that it is impractical for Contractors to procure, operate, support and maintain such equipment. However, the State requires the facility (e.g., uninterrupted power, HVAC, physical security and other attributed) to meet the State's need of SSE to be within the Contractor's facility.

The Contractor's responsibilities pertaining to SSE are as follows:

- Allow the State access to install, test, maintain, upgrade, replace and support this equipment upon mutually agreeable schedules
- Allow the State access to operate this equipment in the event of a disaster or situation that render's the State's primary equipment unusable or inaccessible;

- Provide powered rack space with sufficient cooling based on State provided specifications for SSE that can be racked in standard 42U (or larger) racks with (in general) a 7.5 KW/h design point and typical consumption (on average) of approximately 5.2 KW/h.
- Provide, upon State request under agreed pricing, 42U or larger racks for the above
- For non-rackable SSE (e.g., high speed printers and scanners) provide the State floor space within the area in the proposed facility reserved and secured for State use.
- Ensure that all SSE is powered and cooled commensurate with a TIA942 or Up-Time Tier II data center.
- Ensure that all Contractor provided network elements can provide access to SSE for interconnection with State networks

The State's responsibilities pertaining to SSE are as follows:

- The State will install, provision, operate, maintain, upgrade, support, replace and remove the above SSE. The Contractor will have no operational role other than the aforementioned responsibilities pertaining to SSE.
- The State will provide the following requirements as part of planning and locating SSE in the Contractor's facility:
 - space (generally floor dimensions);
 - power (standby, on, peak) requirements;
 - cooling (BTU); and
 - network connectivity (generally 100Mb/s-10Gb/s Ethernet based) .
- The State may require (for example E911) certain telecommunications access for call management and routing. Should these requirements arise, the Contractor will support the direct termination of these telecommunications circuits to the State location in the Contractor facility without interference, charges or delay.

While the exact requirements for SSE are currently undetermined, the Contractor will include (as part of the Cost Workbook for this RFP, detailed instructions contained therein) the following cost points:

- Twenty (20) 42U locking racks, installed within the State's location in the Contractor Facility (as a one-time charge)
- Ongoing monthly Charges for the aforementioned 20 42U racks powered at 7.5KW/h inclusive of all contractor charges (i.e., space, power, cooling, local networking)
- A powered square footage rate for non rackable equipment based on a 200 ft² increment inclusive of metered power, cooling, local networking. Contractors must assume a 4 foot by 30 foot printer/scanner with accommodation access and service walkways that yields approximately 200 ft²

Part 7: Adherence to Service Level Agreements (Site, DRaaS, SRaaS, SSE)

The State wishes to design, deploy and operate the contracted services in a manner that is consistent with contemporary standards in the commercial marketplace. As these are the fundamental building block for the support of disaster recovery for State applications and solutions that support the operation of the State and the State's services to constituents in the State of Ohio, it is critical Services are delivered in a fashion as to:

- Have high degrees of reliability, availability and performance;
- Be designed, provisioned and deployed in an agile manner that is flexible to accommodate the State's changing business needs;
- Be delivered in a seamless and predictable fashion as an enabler to State projects, applications and services;
- Be a clear step up in service quality from those services that an Agency could otherwise provide for themselves;

- Be delivered at a cost point that is commercially viable (aligned with market norms), attractive, future facing - an enabler of new computing models and a foundation for consolidation as opposed to an impediment for business opportunities.

Therefore, a comprehensive set of service level targets have been selected to deliver the Services contained in this RFP.

7.1 Determination of Service Level Fault

The following items will be considered **Contractor Fault** with respect to Service Level failures and will apply to Performance Credits and Overall Contract Performance considerations discussed later in this section:

- Failures that are in the Contractor responsibility area, or that are staffed or performed by Contractor provided personnel;
- Failures where personnel (Contractor or State) are following established Contractor processes where as a result of issues, defects, omissions or inconsistencies in these designed and provided processes are shown to be the primary source of the failure;
- Failures where Contractor provided personnel has an exclusive role or responsibility and is not dependent on State resources to complete the tasks associated with the failure;
- Failures resulting from a sub-contractor or small-dollar contractor working for, or at the direction of the Contractor;
- Failures arising from Contractor owned equipment or computing devices coincident with providing the in-scope services.

The following items **not be considered Contractor Fault** with respect to Service level failures and therefore not apply to any Contractor Performance Credits or Overall Contract Performance considerations discussed later in this section:

- Failures outside of the scope of the Contractor responsibilities pursuant to the Services Responsibility Matrix, failures due to non-performance of State retained responsibilities pursuant to the Services Responsibility Matrix, or failure of an out-of-scope State element that directly impacts an in-scope State or Contractor element;
- Failures arising from State provided equipment or network;
- Failure of a State resource to follow and comply with Contractor provided processes and procedures except where: (i) State Policies and Contractor policies are in conflict in which case the State resource will notify the Contractor of the conflict and resolve which process applies or; (ii) in cases of emergency that would place the State resource at physical peril or harm;
- Failure of a State provided third party warranty or maintenance agreement to deliver services to the Contractor for in-scope services and infrastructure elements;
- The incident requires assistance for a State retained responsibility, is delayed at the State's request, or requires availability of State personnel that is not available;
- Mutually agreed upon temporary bulk storage replication periods that introduce network, server or storage performance issues as a result of the volume of data being replicated;
- Failures due to non-currency of State provided software (that are not supported by the OEM); and
- Mutually agreed upon service interruptions such as scheduled changes to the technical environment.

In the cases where a State resource is not performing to the level as required to support the Work at levels required by the Service Level Agreements, the Contractor is to notify the State of the Contractor perceived deficiency and allow the State (at the State's discretion) to remedy the situation via change in personnel, training or other development activities. Until such time as the resource can comply with the established roles and responsibilities the Contractor will be exempt from fault pertaining to all Service Level failures associated with the identified resource.

7.2 Monthly Service Level Reporting

As part of the service, the Contractor must develop a written report to the State which includes the following information (the “Monthly Service Level Report”):

- Quantitative performance for each Service Level;
- Each Individual Service Level’s “green, yellow and red” State;
- A year-to-date total trend for each Service Level and all the Service Levels;
- A “Root-Cause Analysis” (excluding those with zero weighting) and corrective action plan (including those with zero weighting) with respect to any Service Levels where the Individual SL state was not “Green” during the preceding month

7.3 Service Level Requirements

The following table provides Expected Service Levels that will be delivered by the Contractor in conjunction with the contracted services.

N ^e	Service Level	Green	Yellow	Red	Unit / Measure
1.	Incident Resolution – Severity 1 Outages (DRaaS, SRaaS)	90% <=4	90% 4-8	90% >8	hours
2.	Incident Resolution – Severity 2 and 3 Outages (DRaaS, SRaaS)	90% <=24	90% 24-48	90% >48	hours
3.	Service Availability –Servers (DRaaS)	99.5%+	99.5%-99.0%	<99%	Uptime
4.	Service Availability – Storage (SRaaS)	99.9%+	99.7%-99.9%	<99.7%	uptime
5.	Facility Service Availability – Contractor Facility (Power, HVAC, Network to State Services)	>= 99.749%	n/a	< 99.749%	uptime
6.	Scheduled Provisioning – Virtual Machines	>90%	80-90%	<80%	% provisioned within Committed Dates
7.	Scheduled Provisioning – Storage	>90%	80-90%	<80%	% provisioned within Committed Dates
8.	Capacity Monitoring and Usage Report	On time	1 Business Day late	> 1 Business Days Late	Timeliness of capacity usage report
9.	Service Quality – System Changes	>97%	92-97%	<92%	% changes implemented correctly first time
10.	Service Timeliness – System Changes	>97%	92-97%	<92%	% changes implemented on schedule

7.4 Contractor Fees at Risk as a Result of Non-Compliance with Service Levels

Each Service Level (SL) will be measured using the “Green-Yellow-Red” (GYR) 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 financial credit will be due to the State (a “Performance Credit”) in the event a specific Individual SLA GYR State falls in the “Yellow “or “Red” State for a SL that has an assigned weighting. 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.

The Fees at Risk will pertain to failure to meet the Service Levels set forth in the Agreement. Contractor will not be required to provide Performance Credits for multiple Performance Specifications for the same event, with the highest Performance Credit available to the State for that particular event to be applicable. 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 Contractor.

Contractor will not be liable for any 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 Contractor takes all steps to minimize the effect of such circumstances and to resume its performance of the Services in accordance with the SLAs as soon as possible.

Each Service Level category is assigned an equal weighting factor, as specified 1% for each of the 10 Service Levels that are reported to be in a red state and 0.85% for those in a yellow state. The Parties agree that the total of all Performance Credits for which Contractor is liable will in no event exceed 10% of the monthly recurring charges (MRC) associated with the Contracted Monthly Amount (“Fees at Risk”). The Monthly Recurring Charge (MRC) is the recurring fixed charge to be paid to Contractor for the Services which are set forth in the Cost Summary Form and which are fixed based on the contracted volumes during a given month.

For Service Levels that are in a non-Green state for two or more consecutive months, these Service Levels will be increased by 50% per month (cumulative) for each month the non-Green condition exists, up to and including reaching the maximum 11% Fees at Risk maximum. For example, in a given month one SLA is in a red state, the fee credit to the State pertaining to this SLA is 1%, in the second month if still red, the fee credit from this SLA will be 1.5% and in the third 2.25% and so on. The 50% consecutive increase will also apply to yellow SLAs based on the aforementioned 0.85% yellow fee credit and escalate according to the example.

7.5 Service Level Specifications

Specification:	Incident Resolution – Severity 1 Outages		
Definition:	<p>Incident Resolution time means the elapsed time measured from the time at which the event related to the Services is identified, received, and recorded in the incident tracking database and until the time at which the Critical Function is operational (though possibly at reduced functionality) or a workaround is in place.</p> <p>Severity 1 Outage means that there is a Critical Function outage causing severe impact on service delivery and no alternative or bypass is available. Contractor will provide notice of Severity 1 incidents along with a preliminary diagnosis and estimated resolution time within 2 hours of recording the Incident in the incident tracking database.</p> <p>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 business operations, in each case prohibiting the execution of productive work.</p>		
Formula:	Severity 1 Outage Resolution	=	Resolution within the timeframe provided in Section 7.3 $\frac{\text{Total Priority 1 Outage Service Requests}}{\text{Total Priority 1 Outage Service Requests}}$
Measurement Period:	Month		
Frequency of Collection:	Per incident		

Specification:	Incident Resolution – Severity 2 and 3 Outages		
Definition:	<p>Incident Resolution time means the elapsed time measured from the time at which the incident related to the Services is identified, received, and recorded in the incident tracking database and until the time at which the Critical Function is operational (though possibly at reduced functionality) or a workaround is in place.</p> <p>“Severity 2 Outage means that a Critical Function is down, degraded, or unusable with a potential severe impact on service delivery and no acceptable alternative or bypass is available. In the event of “go live” of new functionality, an Upgrade, or significant change in the architecture of the Application environment, this Service Level will be suspended temporarily from the time the “go live” of the applicable Change through two (2) business days following completion of stabilization criteria in accordance with the transition to production plan.</p> <p>“Severity 3 Outage means that a non-critical function (i.e. system, application) or procedure is down, unusable, or difficult to use with some operational impact, but no immediate impact on service delivery and an alternative bypass is available. Incidents that would otherwise be considered Severity 1 or Severity 2 but that have an acceptable alternative or bypass will also be designated a Severity Level 3.</p>		
Formula:	Severity 2 and 3 Outage Resolution	=	Resolution within the timeframe provided in Section 7.3 $\frac{\text{Total Priority 1 Outage Service Requests}}{\text{Total Priority 1 Outage Service Requests}}$
Measurement Period:	Month		
Frequency of Collection:	Per incident		

Specification:	Service Availability –Servers (DRaaS)		
Definition:	Server Availability for each in-scope server image that the State has contracted that is supporting State DR functions. Scheduled Business Hours are 24 hours per day, 7 days a week, excepting mutually agreed maintenance periods.		
Formula:	DRaaS Service Ability	=	$\frac{(\text{Actual Uptime less unplanned Downtime})}{\text{Scheduled Hours less Planned Downtime}} \times 100$
Measurement Period:	Month		
Frequency of Collection:	Per incident		

Specification:	Service Availability –Storage (SRaaS)		
Definition:	Server Availability for each in-scope server image that the State has contracted that is supporting State SR functions. Scheduled Business Hours are 24 hours per day, 7 days a week, excepting mutually agreed maintenance periods.		
Formula:	SRaaS Service Ability	=	$\frac{(\text{Actual Uptime less unplanned Downtime})}{\text{Scheduled Hours less Planned Downtime}} \times 100$
Measurement Period:	Month		
Frequency of Collection:	Per incident		

Specification:	Facility Service Availability – Contractor Facility (Power, HVAC, Network to State Services)		
Definition:	Server Availability for each in-scope server image that the State has contracted that is supporting State (DRaaS, SRaaS and SSE) functions. Scheduled Business Hours are 24 hours per day, 7 days a week, excepting mutually agreed maintenance periods.		
Formula:	Facility Service Ability	=	$\frac{(\text{Actual Uptime less unplanned Downtime})}{\text{Scheduled Hours less Planned Downtime}} \times 100$
Measurement Period:	Month		
Frequency of Collection:	Per incident		

Specification:	Scheduled Provisioning – Virtual Machines		
Definition:	<p>Scheduled provisioning of virtual machine environments is defined as the planning, management and configuration of the host server and their connectivity to data storage devices and made available with login credentials to the State.</p> <p>Contractor and the State will agree on a standard process and set of specifications to be applied to requests for provisioning, including:</p> <ul style="list-style-type: none"> Build Sheet approved by the Contractor and the State for server types Standardized Images approved by the Contractor and the State <p>The Contractor will turn over the server to the State for use within 2 business days. For provisioning requests that fall outside the standard approach or if the State makes more than 20 requests in a month or more than 5 requests in a week, the Parties will mutually agree on the timeframe (“Committed Date”) for implementation, taking into account the number of images, availability of a standard image, and existence of technical complications in the environment.</p>		
Formula:	Scheduled Provisioning Virtual Machines	=	$\frac{(\text{Total number of virtual machines scheduled provisioning requests}) - (\text{number of scheduled virtual machines not provisioned within required timeframe})}{(\text{Total number of virtual machines scheduled provisioning requests})} \times 100$

Measurement Period:	Month
Frequency of Collection:	Per Request

Specification:	Scheduled Provisioning – Storage		
Definition:	<p>Scheduled provisioning of virtual machine environments is defined as the planning, management and configuration of the data storage devices and made available with login credentials or mount points to the State.</p> <p>Contractor and the State will agree on a standard process and set of specifications to be applied to requests for provisioning, including:</p> <p>Build Sheet approved by the Contractor and the State for storage types</p> <p>Standardized storage allocation approved by the Contractor and the State</p> <p>The Contractor will turn over the server to the State use within 2 business days. For provisioning requests that fall outside the standard approach or if the State makes more than 20 requests in a month or more than 5 requests in a week, the Parties will mutually agree on the timeframe (“Committed Date”) for implementation, taking into account the number of images, availability of a standard image, and existence of technical complications in the environment.</p>		
Formula:	Scheduled Provisioning – Storage	=	$\frac{\text{(Total number of storage scheduled provisioning requests)} - \text{minus (number of scheduled storage not provisioned within required timeframe)}}{\text{(Total number of storage scheduled provisioning requests)}} \times 100$
Measurement Period:	Month		
Frequency of Collection:	Per Request		

Specification:	Capacity Monitoring and Usage Report Accuracy		
Definition:	<p>Capacity Monitoring and Usage Report Accuracy will be determined by comparing the Contractor provided and maintained Service Management Tracking system (the Contractor’s database to be utilized for tracking the State’s consumption of Contractor services and assets) records against a representative physical sampling (10%) of the actual assets, and Contractor invoiced amounts, performed annually. The scope of this comparison is in-scope assets and services operated and supported by the Contractor for use by the State, as set forth in the Contract. Contractor will not be responsible for accuracy errors that are not caused by Contractor.</p>		
Formula:	Capacity Monitoring and Usage Report Accuracy	=	$\frac{\text{(Number of accurate critical data elements within criteria)}}{\text{Number of critical data elements for sampled assets}} \times 100$
Measurement Period:	Month, Accumulated Annually		
Frequency of Collection:	Monthly, Concurrent with Contractor Invoice		

Specification:	Service Quality – System Changes		
Definition:	<p>The Service Quality & Timeliness System Changes measure is determined by monitoring compliance for the following:</p> <p>Scheduled changes (i.e. system changes, maintenance functions, or updates to the in-scope environment which includes, break fix, configuration, and patches) are implemented correctly the first time.</p> <p>This Service Level covers both planned and emergency changes, provided that emergency changes constitute no more than 10 percent of total changes.</p>		
Formula:	Service Quality – System Changes	=	$\frac{\text{(Total Number of System Changes)} - \text{(Total Number of instances change was not correctly implemented)}}{\text{(Total Number of total System Changes)}} \times 100$

Measurement Period:	Month
Frequency of Collection:	Monthly

Specification:	Service Timeliness – System Changes		
Definition:	<p>The Service Timeliness System Changes measure is determined by monitoring compliance with the following:</p> <p>Scheduled changes (i.e. system changes, maintenance functions, or updates to the in-scope environment which includes, break fix, configuration, and patches) will be performed within the approved timeframe.</p> <p>This Service Level covers both planned and emergency changes, provided that emergency changes constitute no more than 10 percent of total changes.</p>		
Formula:	Service Timeliness – System Changes	=	$\frac{(\text{Total Number of system changes}) - (\text{Total Number of system changes not completed in timeframe Contracted})}{(\text{Total Number of total System Changes})} \times 100$
Measurement Period:	Month		
Frequency of Collection:	Monthly		

Part 8: Services Responsibility Matrix (State and Contractor)

Services Responsibility Matrix	Contractor	State
Software Asset Tracking		
Maintain a list of State provided software to be tracked (SW Tracking List).	Perform	
Provide State Software to Contractor for State Use		Perform
Remove/Return State Software upon State direction	Perform	
Periodic Inventory		
Conduct a physical inventory of in-scope assets supporting Contractor services collecting information minimally consisting of: manufacturer, machine type (part number), model number, serial number, asset tag number, and location.	Perform	
Service Desk		
Command, Control, 2nd/3rd Level Support, Oversight; create process and procedures for State approval	Perform	
Single Point of Contact (all IT Services)	Perform	
Receive requests via phone call or other agreed process	Perform	
Provide Help Desk Support as per the contracted hours of operation.	Perform	
Perform initial problem determination (Level 1) in support of contracted scope of services with related hardware, software and services support as specified in the contract schedule	Perform	
Gather the End User inquiry information	Perform	
Validate entitlement for service	Perform	
Open/Update request in standard call management tool	Perform	
Update Asset information as required.	Perform	
Assign priority in line with contract expectations or as requested by the State	Perform	
Resolve problems/requests	Perform	
Refer problem/request to other support group as required.	Perform	
Provide problem record status upon request	Perform	
Post alerts for general system outages.	Perform	
Escalate problems - Initiate Service Outage process - Initiate Executive Alert process	Perform	
Close problem/request records with State agreement	Perform	
IMAC logging not coordination	Perform	
Document and maintain internal Helpdesk process and procedures	Perform	
Maintain Helpdesk ACD routing	Perform	
Communicate unplanned outages via ACD status message	Perform	
DRaaS, SRaaS - Service Systems Management: Windows, Linux, UNIX Servers – Physical / Virtual / VMWare		
Command, Control, 2nd/3rd Level Support, Oversight; create process and procedures for State approval	Perform	
Install the in-scope server operating system, system management software and operating system utilities.	Perform	
Support of the in-scope server operating system, system management software and operating system utilities, including minor upgrades (such as a release upgrade)	Perform	
Manage the operating system configuration including initial server configuration, modifying configuration files, system configuration documentation and access to system configuration files	Perform	
Manage operating system file systems including creating, maintaining and deleting volumes and directory structures, modifying file system sizes, verifying mount point availability, repairing defective file systems and modifying file system permissions	Assist	Perform

Services Responsibility Matrix	Contractor	State
Monitor and reduce operating system log files to prevent file systems from overfilling		Perform
Manage Operating System Processes (e.g., continuously running system subtasks, or daemons) including refreshing processes as required, establishing startup sequences, maintaining system clock synchronization and changing process priorities as appropriate		Perform
Apply operating system patch set updates as required	Assist	Perform
Maintain tools for remote management and alert monitoring		Perform
Maintain operational support procedures		Perform
Maintain the hardware and software configuration server information	Perform	
Coordinate in-scope server hardware service with the appropriate vendor	Perform	
Manage System IDs and domain structure		Perform
Evaluate planned changes to the server environment and advise of any requirements to support such changes	Assist	Assist
Enable passwords for servers to use to connect with other servers on the network		Perform
Adhere to standard security processes and procedures	Perform	Perform
Support trusted third party security servers authentication		Perform
Synchronize security information among servers		Perform
Create and modify system login/logon scripts		Perform
Assign account, workgroup and print managers		Perform
Define Print Queues		Perform
Administer file system directory distribution and replication		Perform
Provide health check and trending reports which include the following to include CPU, Memory (RAM), Disk and Server Red Action List (servers which have gone above defined set thresholds).	Perform	Assist
Manage State Applications and Data contained on virtual or physical machine instances		Perform
Manage State Data contained on Contractor or State provided Storage		Perform
Manage Backup/Restore of State Data or Machine Images		Perform
DRaaS, SRaaS Incident Management and Resolution		
Managing severity 1 incidents through service restoration	Perform	
Managing non-severity 1 incidents through service restoration	Perform	Assist
Escalating as required for non-severity 1 incidents	Perform	
Driving problem determination activities for non-severity 1 incidents	Perform	
Driving restoration plans for non-severity 1 incidents	Perform	
Confirm that the service has been restored to the State's satisfaction for incidents	Perform	
Facilitate and/or make service restoration decisions/recommendations for incidents	Perform	Assist
Facilitating that the progression of the problem restoration and all relevant times are documented for incidents	Perform	
Contributing to the outage review or root cause analysis process as required for incidents	Perform	
Execute notification and escalation activities for incidents	Perform	
Monitor managed hardware & software during in-scope service hours	Perform	
Perform basic problem determination on systems and components managed including hardware problems, system software problems and Contractor network problems	Perform	
Provide information for changes affecting the server environment	Perform	
Evaluate planned changes to the server environment and advise of any requirements to support such changes	Perform	
Monitor Up/Down status of system processes.	Perform	
Monitor and respond to system alerts and events	Perform	

Services Responsibility Matrix	Contractor	State
Monitor and respond to hardware alerts and events	Perform	
Monitor and maintain system error logs	Perform	
Restart failing components after an outage	Perform	
Provide operational status as required	Perform	
SRaaS File Management		
Command, Control, Support, Oversight; create process and procedures for State approval	Perform	
Manage non-root application file systems	Perform	
Modifying file system sizes	Perform	
Verifying mount point availability	Perform	
Repairing defective file systems	Perform	
Modifying file system permissions	Perform	
DRaaS/SRaaS Platform Configuration Management		
Manage the operating system configuration including Initial server configuration, modifying configuration files, documenting system configuration and controlling access to system configuration files	Perform	
Manage the operating system configuration including Initial server configuration, modifying configuration files, documenting system configuration and controlling access to system configuration files. Perform day to day support of the server environment around troubleshooting, problem determination, changes, security remediation		Perform
Maintain the hardware and software configuration server information	Perform	
Maintain the hardware and software configuration server information. Perform day to day support of the server environment around troubleshooting, problem determination, changes, security remediation		Perform
DRaaS/SRaaS Performance Management		
Manage queues for Incidents, Problems, Changes and other service requests pertaining to performance	Assist	Perform
Manage thresholds and alerts for usage of IT resources.	Perform	Assist
Analyze performance service level breaches, alerts, trends and root causes to restore service.	Perform	
Track and tune proactively performance of Contractor provided services elements through trend and exception reporting to avoid possible service level breaches.	Perform	Assist
Tune reactively to restore service for performance incidents and root causes	Perform	Assist
Provide corrective action to resolve system performance problems and provide recommendations to prevent possible future incidents	Perform	
Recommend changes to maintain agreed upon system performance levels	Assist	Assist
Implement performance changes as approved through a formal change management process	Perform	
Define performance related metrics and data collection, summarization, and storage requirements.	Perform	
Collect, summarize and store performance data	Perform	
Define performance alert thresholds to support agreed upon service levels	Perform	
Provide Standard Performance Reporting	Perform	
Provide Ad hoc Performance Reporting for analysis of incidents to restore service	Perform	
DRaaS/SRaaS Capacity Management		
Define capacity related metrics and data collection, summarization, and storage requirements.	Perform	
Collect, summarize and store capacity data	Perform	
Provide Standard Capacity Reporting	Perform	

Services Responsibility Matrix	Contractor	State
Define capacity alert thresholds to support agreed upon service levels	Perform	
Track capacity measures against defined thresholds and notify State when managed system resource reaches critical or alert levels as identified by managed console operations	Perform	
Manage queues for Incidents, Problems, Changes and other service requests pertaining to capacity	Perform	
Provide Ad hoc Capacity Reporting for analysis of incidents to restore service	Perform	
Analyze capacity measures and forecasting of physical resource requirements	Perform	
Track and document the usage of physical IT resources and provide the information to the State for use in determining future capacity requirements.	Perform	
Recommend corrective actions to resolve capacity problems and prevent possible future incidents	Assist	Assist
Recommend to the State any system configurations or modifications necessary to enable Contractor to maintain acceptable resource utilization	Perform	
SRaaS Storage Management		
Manage SAN/NAS resources, including fiber-based hubs, switches, NAS and directors.	Perform	
Manage SAN/NAS device configurations, including setting up zoning, worldwide addresses, and LUN masking.	Perform	
Manage or Identify firmware upgrades for SAN/NAS resources	Perform	
Perform SAN/NAS device problem determination and resolution	Perform	
Perform SAN/NAS Monitoring and Health checking	Perform	
Manage SAN/NAS resources, including fiber-based hubs	Perform	
Configure the disk storage arrays. For disk arrays, this includes setting up Raid groups, spares.	Perform	
Define logical volumes, metavolumes, hipervolumes, striping, etc. in the storage arrays.	Perform	
Identify and Perform storage device firmware upgrades.	Perform	
Coordinate and managing microcode with Technical Support teams, State and OEMs	Perform	
Perform storage device problem determination and resolution	Perform	
Problem determination and resolution	Perform	
Perform storage device I/O Device Driver research and patch management, and apply fixes.	Perform	
Configure Network Attached Storage Devices	Perform	
Manage queues for Incidents, Problems, Changes and other service requests pertaining to storage subsystem capacity	Perform	
Implement SAN/NAS storage allocation requests if storage exists.	Perform	
Recommend corrective actions to resolve storage subsystem capacity problems.	Perform	
Manage queues for Incidents, Problems, Changes and other service requests pertaining to SAN performance.		Perform
Provide support for performance incidents to ensure SAN/NAS hardware such as storage arrays and switches are operating as expected.		Perform
Respond to operational alerts such as disk or switch port failures that may impact performance.		Perform
Engage third party vendors as needed to perform detailed diagnostics of hardware in support of performance incidents.	Assist	Perform
State Emergency Response Support Services		
Command, Control, 2nd/3rd Level Support, Oversight; create process and procedures for State approval	Perform	
Within approximately one hour after receiving Customer's call or email for an Emergency Incident Declaration, host a conference call with Customer's designated personnel to discuss the symptoms Customer is observing, actions taken and similar items	Perform	
Prepare and provide an After-Incident Report to Customer Point of Contact describing the	Perform	

Services Responsibility Matrix	Contractor	State
computer security incident, causes and effects, actions taken by Contractor, and recommended future actions to mitigate risk		
Allow State to operate via Contractor facility (both onsite and remote) during a declared disaster		
Management of Privileged User IDs and Contractor User IDs		
Provision and manage Contractor user IDs and privileged user IDs for the systems, software tools and networking devices within the scope of the service, to the extent allowed by State's environment.		Perform
Perform the provisioning, maintaining and de-provisioning in-scope privileged user IDs ensuring authorization based on business need		Perform
Perform the provisioning, maintaining and de-provisioning groups and their association with in-scope privileged user IDs		Perform
Perform the assignment of standard authorities/privileges to in-scope privileged user IDs		Perform
Remove in-scope user IDs when no longer required		Perform
Manage and control access to passwords for in-scope privilege user IDs		Perform
Management of compliance tasks for Contractor user IDs and privileged user IDs on systems, software tools and network devices within the scope of the service provided:	Perform	Assist
Perform monthly employment verification and necessary removal for Contractor user IDs	Perform	Assist
Perform annual privileged revalidation (one way confirmation – no response required) and removal of privileges associated with the user IDs, based on the continued business need which is associated with security authorities/privileges and/or group membership. Non-Contractor IDs with privileges will be communicated to State for revalidation.	Perform	Assist
Advise Contractor teams on Identity and Access Management State policies and standards definition and implementation	Assist	Perform
Provide and retain audit records for privileged user ID approvals, verifications and revalidations for two years	Perform	
Provide for State review and approval non-expiring passwords and policy exception requests	Perform	
Providing audit records for privileged user ID approvals	Perform	
Verify privilege assignments to ensure that only authorized users have privileges	Perform	Assist
Contractor Data Center LAN, SAN/NAS Fabric Management Services		
Command, Control, 2nd/3rd Level Support, Oversight; create process and procedures for State approval	Perform	
Network host software, TCP/IP, etc.	Perform	
DHCP support	Perform	
Firewalls (including 24x7 security event log monitoring for firewall and IDS/IPS)	Perform	
Policy Definition	Perform	
State Network Interconnectivity Management	Perform	
DMZ, Security design and administration	Perform	
DMZ Architecture & Architecture	Perform	
Monitor & report network equipment and bandwidth utilization	Perform	
Develop and implement solutions for network performance and capacity problems	Perform	
Schedule installation and cut-over activities	Perform	
Resolve hardware-related problems	Perform	
Interface with vendors for scheduling and problem resolution	Perform	
Perform regular maintenance	Perform	
Provide connectivity to State Wide Area Network		Perform
Provide connectivity within Contractor locations	Perform	
Provide redundant connectivity within Contractor locations		Perform

Supplement 2:

Security and Privacy Requirements

State IT Computing Policy Requirements

State Data Handling Requirements

Contents

Supplement 2: 1

1. General State Security and Information Privacy Standards and Requirements 3
1.1. State Provided Elements: Contractor Responsibility Considerations.....	4
1.2. Periodic Security and Privacy Audits.....	5
1.3. Annual Security Plan: State and Contractor Obligations.....	5
1.4. State Network Access (VPN).....	6
1.5. Security and Data Protection.....	6
1.6. State Information Technology Policies	6
2. State and Federal Data Privacy Requirements 7
2.1. Protection of State Data.....	8
2.2. Handling the State's Data	9
2.3. Contractor Access to State Networks Systems and Data	9
2.4. Portable Devices, Data Transfer and Media.....	10
2.5. Limited Use; Survival of Obligations.....	11
2.6. Disposal of PI/SSI.....	11
2.7. Remedies.....	11
2.8. Prohibition on Off-Shore and Unapproved Access.....	11
2.9. Background Check of Contractor Personnel	12
3. Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues	... 12
3.1. General	12
3.2. Actual or Attempted Access or Disclosure	12
3.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities.....	13
3.4. Security Breach Reporting and Indemnification Requirements.....	13
4. Security Review Services	... 13
4.1. Hardware and Software Assets	13
4.2. Security Standards by Device and Access Type.....	14
4.3. Boundary Defenses	14
4.4. Audit Log Reviews	14
4.5. Application Software Security	14
4.6. System Administrator Access	14
4.7. Account Access Privileges.....	15
4.8. Additional Controls and Responsibilities	15

Overview and Scope

This Supplement will 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 will 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 will prevail.

1. General State Security and Information Privacy Standards and Requirements

The Contractor will be responsible for maintaining information security in environments under the Contractor's management and in accordance with State IT Security Policies. The Contractor will implement an information security policy and security capability as set forth in this agreement.

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

- Provide vulnerability management Services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed.
- Support the implementation and compliance monitoring for State IT Security Policies.
- Develop, maintain, update, and implement security procedures, with State review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- 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.

1.1. State Provided Elements: Contractor Responsibility Considerations

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

1.2. Periodic Security and Privacy Audits

The State will 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 would 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 will comply with State security and privacy policies.

1.3. 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)

1.4. 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.

1.5. 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.

1.6. 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 will 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 will 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 will 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 will 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 will 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.

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

2. State and Federal Data Privacy Requirements

Because the privacy of individuals’ personally identifiable information (PII) and State Sensitive Information, generally information that is not subject to disclosures under Ohio Public Records law, (SSI) is a key element to

maintaining the public's trust in working with the State, all systems and services will be designed and 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 will 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 will still be implemented and, when applicable, aligned to other law or regulation.

All parties to this agreement specifically agree to comply with state and federal confidentiality and information disclosure laws, rules and regulations applicable to work associated with this RFP including but not limited to:

- United States Code 42 USC 1320d through 1320d-8 (HIPAA);
- Code of Federal Regulations, 42 CFR 431.300, 431.302, 431.305, 431.306, 435.945, 45 CFR 164.502 (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.

2.1. Protection of State Data

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

- Maintain in confidence any personally identifiable information ("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 will 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.

2.1.1. Disclosure

Disclosure to Third Parties. This Agreement will 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.

2.2. Handling the State's Data

The Contractor must use due diligence to ensure computer and telecommunications systems and services involved in storing, using, or transmitting State Data are secure and to protect that data from unauthorized disclosure, modification, or destruction. "State Data" includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State. To accomplish this, the Contractor must adhere to the following principles:

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

2.3. Contractor Access to State Networks Systems and Data

The Contractor must maintain a robust boundary security capacity that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems that hold State Data, limiting access to only these points, and disable all others.

To do this, the Contractor must:

- Use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available.
- Use two-factor authentication to limit access to systems that contain particularly sensitive State Data, such as personally identifiable data.
- Assume all State Data and information is both confidential and critical for State operations, and the Contractor's security policies, plans, and procedure for the handling, storage, backup, access, and, if

appropriate, destruction of that data must be commensurate to this level of sensitivity unless the State instructs the Contractor otherwise in writing.

- Employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access the State's Data, as well as attacks on the Contractor's infrastructure associated with the State's data. Further, the Contractor must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with the State's Data.
- Use appropriate measures to ensure that State Data is secure before transferring control of any systems or media on which State Data is stored. The method of securing the State Data must be appropriate to the situation and may include erasure, destruction, or encryption of the State Data before transfer of control. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under this Contract.
- Have a business continuity plan in place that the Contractor tests and updates at least annually. The plan must address procedures for response to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Contractor maintains the State's Data in case of loss of that data at the primary site. The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State's Data in the case of a disaster or other business interruption. The Contractor's business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to the State's Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Contractor also must provide for reviewing, testing, and adjusting the plan on an annual basis.
- Not allow the State's Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Contract properly. Even then, the Contractor may permit such only if adequate security measures are in place to ensure the integrity and security of the State Data. Those measures must include a policy on physical security for such devices to minimize the risks of theft and unauthorized access that includes a prohibition against viewing sensitive or confidential data in public or common areas.
- Ensure that portable computing devices must have anti-virus software, personal firewalls, and system password protection. In addition, the State's Data must be encrypted when stored on any portable computing or storage device or media or when transmitted from them across any data network.
- Maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

2.4. Portable Devices, Data Transfer and Media

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

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

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

2.5. Limited Use; Survival of Obligations.

Contractor may use 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.

2.6. 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 will provide written certification to the State that Contractor has returned, or destroyed, all such PI/SSI in Contractor's possession.

2.7. Remedies

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

2.8. Prohibition on Off-Shore and Unapproved Access

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

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

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

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

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

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

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

2.9. Background Check of Contractor Personnel

Contractor agrees that (1) it will conduct 3rd party criminal background checks on Contractor personnel who will perform Sensitive Services (as defined below), and (2) no Ineligible Personnel will perform Sensitive Services under this Agreement. "Ineligible Personnel" means any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, or money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a Specially Designated National, or (b) has been convicted of a felony.

"Sensitive Services" means those services that (i) require access to Customer/Consumer Information, (ii) relate to the State's computer networks, information systems, databases or secure facilities under circumstances that would permit modifications to such systems, or (iii) involve unsupervised access to secure facilities ("Sensitive Services").

Upon request, Contractor will provide written evidence that all of Contractor's personnel providing Sensitive Services have undergone a criminal background check and are eligible to provide Sensitive Services. In the event that Contractor does not comply with the terms of this section, the State may, in its sole and absolute discretion, terminate this Contract immediately without further liability.

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

3.1. General

If over the course of the agreement a security or privacy issue arises, whether detected by the State, a State auditor or the Contractor, that was not existing within an in-scope environment or service prior to the commencement of any Contracted service associated with this agreement, the Contractor must:

- notify the State of the issue or acknowledge receipt of the issue within two (2) hours;
- within forty-eight (48) hours from the initial detection or communication of the issue from the State, present an potential exposure or issue assessment document to the State Account Representative and the State Chief Information Security Officer with a high level assessment as to resolution actions and a plan;
- within four (4) calendar days, and upon direction from the State, implement to the extent commercially reasonable measures to minimize the State's exposure to security or privacy until such time as the issue is resolved; and
- upon approval from the State implement a permanent repair to the identified issue at the Contractor's cost; and

3.2. Actual or Attempted Access or Disclosure

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

3.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities

Contractor must, as soon as is reasonably practicable, make a report to the State including details of the Disclosure and/or Intrusion and the corrective action Contractor has taken to prevent further Disclosure and/or Intrusion. Contractor must, in the case of a Disclosure cooperate fully with the State to notify the effected persons as to the fact of and the circumstances of the Disclosure of the 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 will 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 will take precedence over this notification. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.

3.4. Security Breach Reporting and Indemnification Requirements

- In case of an actual security breach that may have compromised State Data, the Contractor must notify the State in writing of the breach within two (2) hours of the Contractor becoming aware of the breach and fully cooperate with the State to mitigate the consequences of such a breach. This includes any use or disclosure of the State data that is inconsistent with the terms of this Contract and of which the Contractor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this Contract by an employee, agent, or subcontractor of the Contractor.
- The Contractor must give the State full access to the details of the breach and assist the State in making any notifications to potentially affected people and organizations that the State deems are necessary or appropriate. The Contractor must document all such incidents, including its response to them, and make that documentation available to the State on request.
- In addition to any other liability under this Contract related to the Contractor's improper disclosure of State data, and regardless of any limitation on liability of any kind in this Contract, the Contractor will be responsible for acquiring one year's identity theft protection service on behalf of any individual or entity whose personally identifiable information is compromised while it is in the Contractor's possession. Such identity theft protection must provide coverage from all three major credit reporting agencies and provide immediate notice through phone or email of attempts to access the individuals' credit history through those services.

4. Security Review Services

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

4.1. 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 must 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

4.2. 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

4.3. 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

4.4. 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.

4.5. 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

4.6. 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

4.7. 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

4.8. 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

Exhibit 1

OARnet POP Location Addresses

A list of OARnet POP Location addresses is provided as a Microsoft Excel Spreadsheet.

RFP A01134 - State of Ohio Disaster Recovery Site RFP

OARnet POP Location Addresses

State of Ohio Sensitive Information - Not for Public Disclosure - Protected under Ohio Revised Code 149.433

Destroy Upon Submission of RFP Response or Immediately in the Case of Non-Response

No	OARnet POP Address	100Gb/s	Ethernet	Upgradeable Router
1	1 Cascade Plaza Akron OH 44308 (Ste 1210)	■		■
2	567 E Patterson St Alliance OH 44601			
3	1701 Central Ave Ashland KY 41101			
4	160 W Union St Athens OH 45701 (Ste 179A)	■		■
5	19950 County Highway 339 Richwood OH 43344			
6	199 N Poplar St Chillicothe OH 45601			■
7	301 Virginia St E Charleston WV 25301			
8	4000 Chester Ave Cleveland OH 44103			
9	50 Public Square Cleveland OH 44113			■
10	1255 Euclid Ave Cleveland OH 44114 (Ste 640)	■		■
11	1 Riverside Plaza Columbus OH 43215			■
12	1121 Kinnear Rd Columbus OH 43210			■
13	251 Neilston St Columbus OH 43215 (B)	■		■
14	2470 N Star Rd Columbus OH 43221			■
15	180 E Broad St Columbus OH 43215 (Basement)			■
16	30 E Broad St Columbus OH 43215			■
17	1320 Arthur E Adams Dr Columbus OH 43221			■
18	320 W 8th Ave Columbus OH 43201			■
19	90 West Broad St. Columbus OH 43215			■
20	635 W Mehring Way Cincinnati OH 45202			■
21	205 W 4th St Cincinnati OH 45202 (Ste 920)	■		■
22	301 Cleveland Ave SW Canton OH 44702	■		■
23	2121 Euclid Ave Cleveland, OH 44115		■	
24	10900 Euclid Ave Cleveland OH 44106		■	
25	6566 Kilgour Pl Dublin OH 43017 (FI 2)			■
26	565 Metro Pl S 300 Dublin OH 43017 (Ste 300)			■
27	1738 Liberty Rd Delaware OH 43015			■
28	130 W Second St Dayton OH 45402 (FI 15)	■		■
29	10000 Reading Rd Evendale OH 45241			■
30	3200 Bright Rd Findlay OH 45840			■
31	11941 Township Road 108 Findlay OH 45840			■
32	33 E College Street Hillsdale MI 49242			■

- 33 1122 7th Ave Huntington WV 25701
- 34 800 Hilltop Dr Kent OH 44242
- 35 1125 Risman Dr Kent OH 44242 (FI 15)
- 36 1688 N Sugar St Lima OH 45801 (Rm 305A)
- 37 5707 North West Street Lima OH 45807
- 38 2284 Sugar Grove Rd SE Lancaster OH 43130
- 39 8180 Green Meadows Dr Lewis Center OH 43035
- 40 521 S Patterson Ave Oxford OH 45056
- 41 4871 Township Road 128 Cardington OH 43315
- 42 22921 County Highway 198 Marysville OH 43040
- 43 98 Maple St Ashville OH 43103
- 44 185 Stonecreek Rd NW New Philadelphia OH 44663
- 45 10605 Blue Jay Rd Heath OH 43056
- 46 N012 County Rd 17d Okolona OH 4355
- 47 1224 Kinnear Rd Columbus OH 43212
- 48 1790 E State St Port Clinton OH 43452
- 49 800 Gallia St Portsmouth OH 45662 (FI 5)
- 50 300 S Craig St Pittsburgh PA 15213
- 51 US 33 and Old Wv 56 Western WV 26164
- 52 535 Scherers Ct Columbus OH 43085
- 53 8425 Columbus Cincinnati Rd South Charleston OH 45368
- 54 1290 Fletcher Pike South Charleston OH 45368
- 55 4818 Angola Road Toledo OH 43615
- 56 222 N Erie St Toledo OH 43604
- 57 2801 W Bancroft St Toledo OH 43606
- 58 245 Troup Avenue Bowling Green OH 43402
- 59 2125 Eagle Pass Wooster OH 44691
- 60 345 Collegeview Road Westerville OH 43081
- 61 4151 Executive Pkwy 150 Westerville OH 43081 (Rm 150)
- 62 1801 Dayton Xenia Rd Xenia OH 45385
- 63 1343 Belmont Ave Youngstown OH 44504
- 64 Federal Plaza E Youngstown OH 44503 (Rm 1000)
- 65 120 S Walnut St Youngstown OH 44503
- 66 410 Wick Ave Youngstown OH 44503

