Request for Proposal
Issued by:
The Ohio Department of Commerce
Medical Marijuana Control Program
RFP Issue Date: August 17, 2017
Inquiry Period Begins: August 17, 2017
Inquiry Period Ends: August 22, 2017
Closed Date: September 6, 2017

Open Video Management System
RFP Number: COM2018-ADM008

Table of Contents

I. Background ........................................ Page 2
II. Purpose ............................................ Page 3
III. Scope of Work .................................. Page 4
   a. System Capabilities Requirements .......... Page 4
   b. Technical and Operating Requirements ...... Page 6
   c. Deliverables .................................. Page 15
IV. Contractor Qualifications ................. Page 25
V. Cost Proposal .................................. Page 26
VI. General Instructions ......................... Page 27
VII. Proposal Submission Deadlines and Restrictions Page 30
VIII. Evaluation of Proposals and Award ........ Page 31

Attachments
Attachment 1 General Terms and Conditions .... Page 33
Attachment 2 State Security, Privacy, and Data Handling Requirements Page 57
I. Background

On September 8, 2016, House Bill 523 pertaining to the legalization of marijuana for medical purposes became effective. A summary and detailed documents related to this legislation can be found at https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA131-HB-523. The State has developed this RFP to support the State’s regulation, monitoring, licensing and ongoing operation and oversight of the Medical Marijuana industry as allowed by this legislation. A general overview of these Agencies, and their role in the State, and specific to the Medical Marijuana Control Program (MMCP) are as follows:

<table>
<thead>
<tr>
<th>State Department/Board</th>
<th>General Role &amp; Additional Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Medical Board of Ohio (“Medical Board”)</td>
<td>Licensing and Oversight of Physicians <a href="http://www.med.ohio.gov/">http://www.med.ohio.gov/</a></td>
</tr>
<tr>
<td>Pharmacy Board of Ohio (“Pharmacy Board”)</td>
<td>Recommendation Tracking, Patient and Caregiver Registry, and Regulation and Oversight of Dispensaries <a href="https://pharmacy.ohio.gov/">https://pharmacy.ohio.gov/</a></td>
</tr>
<tr>
<td>Ohio Department of Administrative Services, Office of Information Technology (“DAS/OIT”)</td>
<td>Systems, Technology and Contractual Matters Arising from this RFP <a href="http://das.ohio.gov/Divisions/InformationTechnology.aspx">http://das.ohio.gov/Divisions/InformationTechnology.aspx</a></td>
</tr>
</tbody>
</table>

The State’s MMCP has four distinct medical marijuana entities; cultivators, processors, testing labs, and dispensaries.

<table>
<thead>
<tr>
<th>Medical Marijuana Control Program Entity</th>
<th>Estimated Number of Facilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ohio Cultivators</td>
<td>Up to 12 Level I Cultivators and Up to 12 Level II Cultivators</td>
</tr>
<tr>
<td>Ohio Processors</td>
<td>Up to 40</td>
</tr>
<tr>
<td>Ohio Testing Labs</td>
<td>No limit</td>
</tr>
<tr>
<td>Ohio Dispensaries</td>
<td>Up to 60</td>
</tr>
<tr>
<td><strong>Approximate Facility Total</strong></td>
<td><strong>130</strong></td>
</tr>
</tbody>
</table>

Each of the medical marijuana entities is required, pursuant to rules promulgated under Chapter 3796 of the Revised Code, to utilize a video surveillance recording system. The estimated number of video cameras installed across the medical marijuana entity facilities is **at least 1000 video cameras**. Key requirements of each entity’s video surveillance recording system include:

- Video cameras that capture the entire facility, including direct placement near the entrances, exits, and parking areas;
Video cameras shall be directed at all approved safes, approved vaults, and any other area where medical marijuana is being cultivated, harvested, stored, or handled;

- Provide a direct feed and login capabilities to the Department of Commerce and Pharmacy Board to allow for real-time access and monitoring of the facility via the live video surveillance recording system;
- Twenty-four-hour live feed with motion-activated recording (decentralized local storage) capabilities from all video cameras, which the facility shall make available for immediate viewing by the Department of Commerce or Pharmacy Board upon request and shall retain the recordings (decentralized local storage) for at least forty-five days;
- Ability to immediately produce a clear color still photo from any camera image (live or recorded);
- Allow for exporting of still images in an industry standard image format, including .jpg, .bmp, .gif. Exported video shall have the ability to be archived in a proprietary format that ensures authentication of the video and guarantees that no alteration of the recorded image has taken place. Exported video shall also have the ability to be saved in an industry standard file format that can be played on a standard computer operating system; and
- Date and time stamp embedded on all recordings.

Further security rule details, that licensees must comply with, can be found in the applicable sections of the Ohio Revised Code and Ohio Administrative Code. For example, see the following language for Cultivators http://codes.ohio.gov/oac/3796:2-2-05v1.

II. Purpose

The State issues this Request for Proposal to accept bids from vendors to provide the State with an Open Video Management System (“VMS”) that enables the State to access, in real time, the live video surveillance cameras installed at all Ohio MMCP entity facilities. As an Open VMS, the requested system will be camera manufacturer agnostic, accepting input from any camera. The State’s goal is to have a tool that provides a well-organized single point of visibility, from a web based interface, to the entire population of cameras installed at the medical marijuana entities. The VMS will monitor and report on the camera population operational status (e.g. on/off ’system health’) as well as provide real-time visibility to facility activity. Given an initial camera population of over 1000 cameras across an Ohio medical marijuana entity facility population of 100+ facilities, the State requires an efficient means of monitoring camera operational status as well as an efficient path for identifying a particular camera at a particular facility for real-time camera viewing.

The successful Proposer will configure and implement a fully operational VMS, train Commerce and Pharmacy Board staff on its use, and provide maintenance and technical support services throughout the resultant contract term. The successful Proposer must also perform the deployment planning and execution activities for implementation of the VMS at the Columbus, Ohio-based Department of Commerce and the Pharmacy Board. Additionally, the successful Proposer must perform VMS onboarding/deployment at the first group of medical marijuana entity facilities (cultivators, test labs, processors, dispensaries) across Ohio. The first group of entity facilities are estimated to be approximately 130 entity facilities operational by September 8, 2018 (the Ohio Medical Marijuana Control Program operational date).

The State intends to award a contract pursuant to this RFP for a period from contract execution to June 30, 2019. Because the State cannot contract beyond the current biennium, it will reserve the right to renew any contract it awards pursuant to this RFP for two subsequent two-year periods (July 1, 2019 to June 30, 2021 and July 1, 2021 to June 30, 2023). Renewals are solely at State discretion and will be made in writing and delivered to the successful Proposer at least sixty days prior to the next renewal period. Performance by
the State under any contract or renewals entered into pursuant to this RFP are contingent on the availability of lawfully appropriated funds from the Ohio General Assembly. If the Ohio General Assembly fails at any time to continue funding for any payments due as a result of this RFP, any contract awarded or renewals entered into pursuant to it will terminate as of the date that the funding expires, without further obligation of the State.

The VMS must be delivered to the State in a production ready form and ready for deployment at medical marijuana entity facilities no later than April 1, 2018.

### III. Scope of Work

#### III.a VMS Capability Requirements

The VMS must be designed, implemented, and deployed to accomplish the following:

<table>
<thead>
<tr>
<th>Mandatory VMS Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open VMS shall be camera manufacturer agnostic providing live video access independent of the camera manufacturer. The VMS shall support both IP camera environments and analog cameras.</td>
</tr>
<tr>
<td>VMS provides on demand live camera feed access to a minimum of 1000 cameras which are located at the medical marijuana entity facilities.</td>
</tr>
<tr>
<td>VMS is a Hosted/Cloud Software Solution, fully usable from web-based interface, and does not require software installation onto user’s computers. Proposer will implement and support the VMS and the State’s use of it; however, such software shall be maintained on Proposer’s servers. Any reference to “software,” “VMS software,” “State software environment,” “State software platform,” or the like in this RFP is a reference to the VMS software referred to in the prior sentence.</td>
</tr>
<tr>
<td>VMS must be flexible to easily accommodate camera changes (e.g. camera additions, equipment changes, camera removals) occurring at entity facilities. State System Administrator(s) have authority to administer camera changes.</td>
</tr>
<tr>
<td>System must be scalable to handle significant growth in number of cameras due to medical marijuana entity expansion. The medical marijuana entities will initially have a minimum of 1000 cameras.</td>
</tr>
<tr>
<td>The State fulfills role of System Administrator. System enables authorized State users to be established based on various roles and permissions granted by the State System Administrator. State System Administrator manages user ID registration and termination (note, State users are anticipated to be in administrative and enforcement roles). State user access permissions need to default to the regulatory responsibilities and facility scope of the user’s Department/Board (e.g. Pharmacy Board regulatory and facility scope responsibility is dispensaries). On an exception basis, the system should have capability to allow an authorized State to be granted user access permissions outside of their home/default Department/Board.</td>
</tr>
<tr>
<td>System must be scalable to allow for growth in number of authorized State users. Estimated number of initial authorized State users is less than 30.</td>
</tr>
<tr>
<td>VMS offered as a subscription-based service for ongoing usage and technical support.</td>
</tr>
<tr>
<td>VMS shall have an enterprise base license that allows access to all features and functionality without any additional license fees for additional features/functionality.</td>
</tr>
</tbody>
</table>
VMS monitors cameras real-time operational status (on/off), provide reporting of camera status history across the medical marijuana entities, and provide alerts to notify State users if camera(s) not operational.

Support the use of imported maps to show camera placements at the individual medical marijuana entities. These maps will be in .jpg, .gif, or .bmp formats as determined by the administrator.

Solution must have security features that assure digital still image or video evidence will meet all standards for use in evidentiary situations in court.

VMS has file upload capability for still images and video captured by the entity facilities. Upload is from local facility-stored image and video to a State secured storage database. Note, uploaded still images and video are stored by State for compliance and enforcement purposes.

The locally-stored still images and video must be uploaded and stored in the State-secured storage database with the locally recorded/embedded date and time stamp. VMS allows State authorized personnel (e.g. State System Administrator) to add file label attributes such as facility and camera identifier, case/incident number, and image/video description.

VMS capabilities enable authorized State users to organize/manage and search the State-stored still images and video by name, date, event, device, case/incident number. This also includes the ability to tag and isolate stored images and videos that are involved in an investigation, court proceeding, or other matter that requires an indefinite retention period due to the facts and circumstances of each incident.

VMS provides access for viewing of the State-stored images and video based on the permissions granted by the System Administrator(s).

VMS provides ability for State System Administrator to specify retention date of all State-stored images and video.

VMS allows export/download of State-stored video clips or images to PC or to a USB connected media storage device (e.g., CD Burner, DVD Burner or USB memory stick) based on permissions granted by the System Administrator.

System allows for the State-stored images and video to be exported/downloaded in an industry standard file format (e.g. AVI, MPEG4) and supports multiple video compression standards (e.g. H.264/MPEG-4, JPEG). Note, third parties such as law enforcement officials need to access still image and video evidence using PC industry’s standard media player software applications.

Ability to preserve the raw still image and video files as view/read only, no editing allowed.

Log audit trail capturing State users who have accessed or copied State stored video to an external source (i.e. DVD / USB memory stick).

Solution must provide encryption in State-stored images and video as well as upload/download.

Ability for State user to remotely initiate camera video recording (override motion sensor initiated recording), which automatically locally stores still images and video recordings.
III.b Technical and Operating Requirements

General Requirements: Hosted/Cloud Software Solution

The Hosted/Cloud Software Solution will be hosted, operated and maintained by the Contractor as to adhere to the following Requirements and Service Level Agreements:

- All data and access to the system must strictly adhere to Ohio Executive Order 2011-12K, which, in general is a prohibition on offshoring any State data or processes.
- All State data must reside on a Federal Risk and Management Program (FEDRAMP) certified platforms that are FEDRAMP IAAS/SAAS Authorized with FEDRAMP Impact Level: Moderate or Higher.
- All data access, security, privacy and data handling requirements must be adhered to as contained in State Security, Privacy, and Data Handling Requirements.

System Environment Requirements

Based on the State’s typical systems development lifecycle, inclusive of ongoing operations and maintenance activities, the State has developed a set of Systems Environments that are required to support the initial implementation of the system and its ongoing use.

Proposers are encouraged to consider the merits of these Systems Environments and propose (if feasible and advisable) managing these environments to drive availability, releases, efficiency, cost, State licenses or subscriptions costs as applicable, and other consolidation/optimizations. Should the State agree with such approaches, the Proposer, as Contractor, must perform the consolidation/optimizations as contracted.

As part of the end-to-end project and ongoing service, the Contractor must include the management and maintenance, encompassing deployment/management, testing and training environments for the instances of the VMS Applications and supporting evolutions as required to support the State in the context of operating the Medical Marijuana business and comply with State laws and Federal guidelines.

The table below reflects the State’s requirements in terms of environments. To the extent the Proposer wishes to suggest alternatives based upon Contractor and Industry best-practices, the Proposer may do so in their response to this section.

<table>
<thead>
<tr>
<th>Desired but not Mandatory VMS Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile app for connection and usage of the VMS through a mobile device.</td>
</tr>
<tr>
<td>Ability to view facility cameras recording start time and recording stop time window (i.e. when was the motion activated surveillance camera recording started and when did recording end). Note that existing rules require facilities to embed date and time stamp on all recordings.</td>
</tr>
<tr>
<td>State stored image or video is accessible/viewable to multiple State users simultaneously.</td>
</tr>
<tr>
<td>Ability for State user to remotely operate a medical marijuana entity cameras Pan-Tilt-Zoom feature and camera automatically returns to default position.</td>
</tr>
<tr>
<td>Environment</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Demo/Sandbox/Proof of Concept</td>
</tr>
<tr>
<td>Patch Testing/Staging</td>
</tr>
<tr>
<td>Development &amp; Configuration</td>
</tr>
<tr>
<td>Quality Assurance/Testing</td>
</tr>
<tr>
<td>Acceptance Testing</td>
</tr>
<tr>
<td>Production</td>
</tr>
<tr>
<td>Training Delivery</td>
</tr>
</tbody>
</table>

Descriptions of the instances are as follows:

- **Demo/Sandbox/PoC**: This is the instance delivered by the Contractor for diagnostic purposes. All patches and bundles will be applied to this instance. No customizations, modifications or configurations will be made to this instance.

- **Patch Testing/Staging**: This instance is for developers to test Contractor delivered bundles and fixes.

- **Development & Configuration**: All development activity including customizations, modifications or configurations will be made in this instance as needed.

- **Quality Assurance / Testing**: This instance allows testers and pilot users to test the customizations, modifications or configurations made to the application before any changes are migrated to Production. This instance will be used for User Acceptance Testing and all forms of integration testing.

- **Acceptance Testing**: This instance allows State testers and pilot users to assess production acceptance issues and for performance testing.

- **Production**: This is the main transactional instance for the State Medical Marijuana VMS Application.

- **Training Delivery**: This instance is used for classroom and web-based training.

Other replicas of these environments to support SDLC activities and other efforts upon the request of the State.

**Production-Version Control and Release Management**

The Contractor will be responsible for working with the State and executing the production deployment and roll-out of any Release Package or Application to the State’s VMS software environment. Releases must include (at a minimum): new application(s) inclusive of Contractor developed applications; 3rd party developed or licensed VMS software extensions; State integrations (ESB or File-Based); production batch or scheduled job streams; and related VMS software reports, interfaces, conversions, forms, workflows or extensions (RICEFW).
Production deployment includes software deployment to the production instance of VMS software and (if applicable) interfaces to production tools and systems that orchestrate, manage, report or control those devices and services managed by the Proposer, identification of interfaces and any required conversions/migrations, installation of server software, and any required testing to achieve the proper roll-out of the Release Package software.

As part of this Service, the Contractor must:

- Establish for the State and thereafter comply with and enforce a repeatable State VMS software implementation and deployment procedure. This may include laboratory testing, migration procedures, the use of any pre-production or pseudo-production environment prior to production migration;
- For each Release Package submit to the State, for the State’s approval, a written deployment plan describing Contractor’s plan to manage each such implementation. The tasks and activities to be performed by Contractor as part of VMS software production deployment services;
- Establish and follow procedures and automated software versioning mechanism(s) to ensure that the entire contents of a Release Package, following State acceptance or authorization to implement to a production environment, are complete and maintain all elements that comprise the defined Release Package and the then current production version of the software prior to deployment of the Release Package;
- Develop, prepare and test emergency back out or roll back procedures to return the production system to its pre-deployment State as it pertains to correcting an errant, erroneous or defective deployment of a Release Package to the production environment inclusive of all code, data, middleware, infrastructure, tables and parameters;
- If, in the mutual opinion of the State and Contractor, the deployment of a Release Package to the production environment is errant, erroneous or otherwise defective, implement back-out or rollback procedures in their entirety upon the written authorization or direction of the State;
- If required, convert electronic data into a format to be used by the new solution using a data conversion program;
- Conduct production pilot(s) (including “day in the life” simulations) and fine tune solution as mutually agreed with the State as appropriate;
- Compile and maintain solution issue, defect and incident reports;
- Conduct quarterly post-Production Deployment quality and progress reviews with appropriate State personnel;
- Develop, and thereafter maintain and make available to the State, a knowledge base of documentation gathered throughout the Release Package’s life and allow for re-use of such documentation for future Projects; and
- Establish a performance baseline for the impacted business systems, and where appropriate document requirements for future enhancement of the business systems implemented as part of a future Project or Authorized Work.
Break/Fix Support

The Contractor must:

• Track, monitor and provide remediation for solution defects and incidents requiring system configuration or in-scope environment code or configuration changes arising from the application of any of VMS software, State contracted RICEFW enhancements to the State’s VMS software platform;
• Address any incompatibilities, inconsistencies or erroneous processing introduced to the State’s VMS software platform that arise from any production release, patch, update, upgrade or change in code or configuration values;
• Identify and implement required system or configuration changes to address solution defects;
• Test configuration changes to confirm resolution of defects;
• Support the State in performing applicable acceptance testing or review of any changes arising as a result of break/fix or patch/release Contractor responsibilities;
• Ensure compliance with any State Security/Privacy requirements or VMS software mandated patches or system levels to the extent and system enhancement turnaround time required given the nature of the security mandate and report to the State in writing any risks or issues that the Contractor becomes aware of in providing Service to the State. For example: patches designed to address immediate or active Security issues may be scheduled for a near-real-time release, where other less pressing releases may be implemented during a scheduled maintenance or outage period; and
• Maintain solution documentation (technical specifications and testing documentation) as well as a compendium of common problems, root causes and remedy to aid in the identification and remediation of underlying system incidents.

Problem Management Services

Problem Management identifies and resolves the root causes of service disruptions. As part of the delivery of the Service, the Contractor must:

• Perform Root Cause Analysis and identification;
• Develop and Submit Request for Changes to correct problems with State Applications;
• Prioritize resources required for resolution based on business need;
• Update the knowledge base with revised operating procedures and conventions upon resolution of problems;
• Analyze trends and participating in the State continuous improvement process striving to enhance its operations and identifying continuous improvement ideas;
• Share applicable best practices that may improve the State processes and enabling technologies;
• Conduct periodic knowledge exchanges between Contractor team and the State designated individuals; and
• Assist with implementing the State defined IT control requirements including updating security matrix spreadsheets, and implementing Supported server and Systems software configurations for access control.
VMS software and Application Licensing, Capacity Planning and Monitoring

The Contractor must:

- Review the State growth plans during quarterly service review meetings, and if requested due to an unforeseen requirement, participate in the required number of ad-hoc reviews coincident with these new requirements and VMS software application needs to correctly plan for licensing and capacity – periodic capacity increases as well as burst requirements.
- Monitor VMS software and State application usage and capacity, forecast capacity and review with the State Infrastructure Management on a quarterly basis.

The State will:

- Project future VMS software based trends and capacity requirements in conjunction with receipt of Contractor provided capacity usage reports, and in consultation with the Contractor, for new Projects and provide such information to the Contractor as it pertains to the Services;
- Review VMS software system performance, licensing and capacity and throughput for new applications before promotion into the production environment to resolve any overcapacity situations.

VMS Software Platform System Management and Administration

The Contractor must:

- Install, test, operate, troubleshoot, and maintain the VMS software;
- Identify and test packaging patches and other updates associated with the VMS software, as well as supporting additional security-related fixes associated with the VMS software;
- Manage the security functions related to the VMS software including administrative access and passwords (i.e., users with root, administrator, DBA or low-level read/write access) and the related security controls to maintain the integrity of the VMS software, based on the State’s security standards;
- Configure and maintain systems managed by the Contractor for network and remote access;
- Provide advisory services to support the VMS software administration and developer access services and roles;
- Review supported VMS software administration, set-up and configuration; and
- Support performance tuning of State application elements and perform performance tuning on VMS software elements.

The State will:

- Assist the Contractor in developing procedures for handling all planned and unplanned outages affecting the VMS software Platform and State Applications, including review, approval, communication, and proper documentation; and
- Notify the Contractor of any planned or emergency changes to the State’s environment affecting the Contractor's delivery of the Services.
Support of VMS Software Future Releases and State Applications as a Result of Changes

The Contractor must provide Support and Maintenance of the State’s VMS software platform that includes:

- VMS software platform-level administration, reporting, and support. VMS software platform support does not include end-user facing Help Desk functions, but does include technical, integration, and application/code based functions that are specific to VMS software and State integrations within the contracted scope of Services;
- Supporting the State in re-testing or validating State specified RICEFW objects coincident with VMS software system releases (see below);
- Application Break/Fix responsibility and Minor Enhancements to State specified RICEFW objects;
- Migration to Production of applications once meeting the State’s acceptance criteria;
- Environment refresh services for non-Production and quasi-Production uses;
- System change management and Production version control; and
- Review of system usage, performance and reliability reports and collaboration with State Infrastructure Staff to drive system usability, reliability, and performance.

Major/Minor Upgrades (Ongoing)

Release upgrades for packaged software are initiated through periodic releases of VMS software as Major or Minor releases. The State requires that the Contractor lead and coordinate efforts to analyze, install/apply, test/verify and utilize State specified RICEFW objects to these releases in the State’s environment.

Further, the State understands the importance of VMS software major and minor upgrades to its overall capabilities in support of the State’s mission and is committed to maintaining the VMS software at the most current proven release at all times, unless the State provides a written exception.

The Contractor is to comply with the following requirements:

- The State’s requirement is to always operate on a hosted/cloud Application that is on the current VMS software release and support model and terms as provided by VMS software;
- As part of annual planning and coincident with project review meetings, the Contractor is to inform the State in writing of any components that are moving beyond a current support model or would rendered unusable as a result of an upcoming release and present a plan to implement the required updates in a controlled manner to the applicable State environment(s) to maintain compliance VMS software support models;
- Based on review of any upgrade or update plan (inclusive of all elements required to effectively manage, resource, test, validate and implement the change) as outlined elsewhere in this statement of work, the State and the Contractor will schedule a mutually agreeable upgrade/update effort and authorize the Contractor to perform these upgrade services to maintain the required support model;
- Upgrade and update efforts must factor any regularly scheduled batch processing or system availability as well as any seasonal processing requirements and should be scheduled to maintain compliance with system availability in consideration of then prevailing development release or production schedule;
The Contractor will be responsible for the design, development, and implementation of the Minor/Major enhancements in the State environments including requirements/design discussions, applicable conference room pilots, design review/signoff, document design specification, document and execute unit and integration/interface tests, support of the State in executing UAT;

The Contractor must support the State in the planning and deployment of periodic releases of non-emergency patches and enhancements (e.g., test new functionality, regression test entire application, document release notes, coordinate with the State for end user change management/communication) as well as perform these responsibilities for all Contractor developed elements for the State;

The Contractor must verify and accept enhancements not developed by the Contractor (e.g., review designs, execute tests, migration to production); Notwithstanding Major and Minor Upgrade enhancement requirements as outlined above, the Contractor has an obligation to maintain all VMS software elements in keeping with a current support and in accordance with agreed procedures associated with the minimization of exposure to viruses, malicious software (malware), security holes or flaws, incompatibility issues, software patch currency, technical updates, corrections and other elements that directly influence the warrantee, support, performance and ongoing upgradeability of underlying software and State specified RICEFW objects of the VMS software platform service.

Program Management & Master Release Calendar

The Contractor must develop and thereafter publish and follow a Master Release Plan and support the State in the development, maintenance and publication of a Master Release Calendar that includes a schedule (with dates) including:

- Major and Minor Project Key Dates (i.e., Start, SDLC Gate Completion, Production Release, Completion) whether Contractor delivered or otherwise;
- Major/Minor and Scheduled Releases, Upgrades, Updates and Enhancements;
- Implementation of Projects, Minor Enhancements or Discretionary Work;
- Scheduled Maintenance Windows and Planned Outages; and
- Other pertinent dates that require end-user notification or coordination.

Minor Change and Enhancement Services

Based on the State’s experience with the management and ongoing operations of enterprise software environments, the State is requiring the Contractor to provide the capability to address minor alterations or enhancements (generally less than one month of duration per occurrence inclusive of analysis, design, construction, testing and implementation tasks, but extendable to larger efforts at the mutual agreement of the State and Contractor) to software within the scope of the Services that arise as a result of legal, regulatory, mandates or changes to the State’s business. See Cost Proposal for the line item addressing Enhancements.

Due to the sporadic nature of these requirements (e.g., minor display field changes, edits, reports, etc.), the State may require the Contractor to provide these services as needed.

- Ad-hoc requests do not require extensive customization of the VMS software environments (e.g., cosmetic enhancements, maintenance of configuration values, simple reports/views).
Routine tracking procedures must provide visibility of all ad-hoc requests to the State Authorized service representative. The Contractor and the State will develop a prioritization approach for ad-hoc requests based upon business impact and document such process as mutually agreed.

**Environment Backup and Restoration Services**

For each VMS software environment within the scope of the Contractor’s Service, the Contractor must perform backup processes as follows:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Scheduled Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>Pre-production image</td>
<td>Once</td>
</tr>
<tr>
<td>Daily Incremental Files</td>
<td>Data changes during the period</td>
<td>Daily</td>
</tr>
<tr>
<td>Full Data Files</td>
<td>All resident data files</td>
<td>Weekly (weekend)</td>
</tr>
<tr>
<td>Pre-Production Initiations</td>
<td>All initiation files during the Production introduction/implementation period</td>
<td>Daily</td>
</tr>
<tr>
<td>VMS software Platform and Related Commercial Software</td>
<td>All VMS software configuration files and related Commercial software</td>
<td>Monthly</td>
</tr>
<tr>
<td>Database</td>
<td>All Databases</td>
<td>Weekly (weekend)</td>
</tr>
<tr>
<td>Full Back up Copy</td>
<td>At request of State when a change is made to a State system a copy must be made before the change.</td>
<td>As needed</td>
</tr>
</tbody>
</table>

The Contractor must maintain backup retention periods as follows:

<table>
<thead>
<tr>
<th>Description</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>Until first annual + 1 month</td>
</tr>
<tr>
<td>Daily</td>
<td>6 Days</td>
</tr>
<tr>
<td>Weekly</td>
<td>4 Weeks</td>
</tr>
<tr>
<td>Monthly</td>
<td>12 Months</td>
</tr>
<tr>
<td>Annual</td>
<td>7 Years</td>
</tr>
</tbody>
</table>
Upon any return of Contractor created backup images or machine-readable media of State data, Contractor must provide any encryption keys, passwords, hardware decryption keys (e.g., dongles) as necessary to decrypt the data and restore the data.

**Service Level Requirements: Hosted/Cloud Software Solution**

**Service Availability:** Service Availability for the Hosted/Cloud Software Solution provided by the Contractor that the State utilizes commercially supporting State Medical Marijuana operations, development and maintenance activities, training, demonstration or supporting non-commercial use application usage.

- **Standard:** 99.5% available, 24 hours per day, 365 days per year less mutually agreed to and published scheduled maintenance windows not to exceed five hours per month.

**Severity 1 Outage Resolution Time.** Severity 1 Outage means that there is a Critical Function outage causing severe impact on VMS delivery and no alternative or bypass is available. The Contractor must provide notice to the State of Severity 1 incidents along with a preliminary diagnosis and estimated resolution time within 15 minutes of detecting the Incident or being informed by any County/Sheriff or detection of such outage.

A severe impact means: The Incident renders a business-critical function, System, Service, Software, Equipment or network component un-Available, substantially un-Available or seriously impacts normal State operations, in each case prohibiting the execution of productive work.

- **Standard:** Detection of Outage and Reporting to State estimated time of resolution: 15 Minutes, resolution of outage and return to contracted standards within 60 minutes.

**System Performance and Timeliness.** System performance must be measured by the Contractor and be subject to demonstration to the State for auditing and verification purposes upon the request of the State. System performance must meet the following standards:

- **Standard:** Web-based online page presentation transactions must be returned (allowing for network transit time) from origination by a User to return of a properly formatted response within five (5) seconds for at least 99% of all properly formatted State transactions during available hours.

- **Standard:** Industry-facing transactions must be returned (allowing for network transit time) from origination by a user (via the web or a published API) to return of a properly formatted response inclusive of logging/accepting a transaction and display (via the website) to the user within five (5) seconds for at least 99% of all properly formatted transactions during available hours.

- **Standard:** Notification emails and alerts should be constructed, queued to email notification element(s) of the system (generally an SMTP service or equivalent) and released to the user (allowing for network transit time) within 15 seconds of the existence of a condition by which a user notification is required to be originated and transmitted.

**Service Level Specific Performance Credits**

Failure to meet any Service level contained in this Section in a given month will result in a 5% fee credit of the total monthly charges for the service to the State for the service month following on a **per incident** basis identified by the State, and confirmed to be the failure of the Contractor or a Contractor provided element for failure to meet the contracted Standard(s).
III.c Deliverables

Deliverables must be provided on the dates agreed with the State. Any changes to the delivery date must have prior approval (in writing) by the State contract manager or designee.

The VMS must be delivered to the State in a production ready form and ready for deployment at medical marijuana entities (Deliverable 6) no later than April 1, 2018.

All deliverables must be submitted in a format approved by the State’s contract manager.

All deliverables must have acceptance criteria established and a time period for testing or acceptance.

If the deliverable cannot be provided within the scheduled time frame, the Contractor is required to contact the State’s contract manager in writing with a reason for the delay and the proposed revised schedule. The request for a revised schedule must include the impact on related tasks and the overall project.

A request for a revised schedule must be reviewed and approved by the State contract manager before placed in effect.

The State will complete a review of each submitted deliverable within specified working days of the date of receipt.

Work shall be quoted on a deliverable basis as a firm-fixed, not to exceed price.

The following deliverables are required by the State for developing a complete Open VMS solution:

- **Deliverable 1:** Project & Staffing Plan
- **Deliverable 2:** Requirements Catalogue, Operating Processes
- **Deliverable 3:** Solution Architecture & Build Completion Document
- **Deliverable 4:** Contractor System Test Completion & Training
- **Deliverable 5:** State Acceptance Test Completion, Contractor Performance Test
- **Deliverable 6:** Deployment/Onboarding Planning & Execution
- **Deliverable 7:** Final Acceptance
Deliverable 1. Project & Staffing Plan

Project Management and Coordination Services

The Project will follow the Governance structure defined by the State. Project Management will include the activities to manage the Project including directing the Project Team according to the Project work plan, reporting status, managing issues, assessing quality, leading project meetings, and monitoring schedule and scope changes. The Project Team must produce project status reports on a weekly basis. The format of the status report will be mutually agreed to by the State and the Contractor during the first week of the Project.

The Contractor must, in conjunction with performing the work:

- Be responsible for the coordination and delivery of the overall Project;
- Ensure that all efforts have an effective version control mechanism for all documents within the project document library that will be maintained on a State provided Microsoft SharePoint site;
- Work with the State leadership to ensure that the Project is staffed appropriately;
- Ensure that required testing activities across both technical and operational components are completed to minimize Project risk; and
- Collaborate with the task areas to ensure appropriate cross-team communication and delivery.

Create and Maintain Project Plan

The Contractor must produce a detailed Project Plan, in electronic and paper form, to the State Project Manager for approval within twenty business days after the State issues a purchase order or other written payment obligation under the Contract.

Thereafter, the Contractor must:

- Formally update the Project Plan, including work breakdown structure and schedule, and provide the updated Project Plan as part of its reporting requirements during the Project; and
- Ensure the Project Plan allows adequate time and process for the development for the State’s review, commentary, and approval.

The State will determine the number of business days it needs for such reviews and provide that information to the Contractor after award and early in the development of the Project Plan. Should the State reject the plan or associated deliverables, the Contractor must correct all deficiencies and resubmit it for the State’s review and approval until the State accepts the Deliverable at no additional cost to the State

Meeting Attendance and Reporting Requirements.

The Contractor’s project delivery approach must adhere to the following meeting and reporting requirements:

- Immediate Reporting - The Project Manager or a designee must immediately report any Project staffing changes to the State Project Representative.
- Attend Weekly Status Meetings - The State and Contractor Project Managers and other Project team members must attend weekly status meetings with the Project Representative and other members of the Project teams deemed necessary to discuss Project issues. These weekly meetings must follow an agreed upon agenda and allow the Contractor and the State to discuss any issues that concern them.

- Provide Weekly Status Reports - The Contractor must provide written status reports to the Project Representative at least one full business day before each weekly status meeting.

- At a minimum, weekly status reports must contain the items identified below:
  - Updated GANTT chart, along with a copy of the corresponding Project Plan files (e.g. MS Project) on electronic media acceptable to the State;
  - Project scope, budget, and schedule;
  - Updated Critical Path analysis with the aforementioned GANTT chart;
  - Status of currently planned tasks, specifically identifying tasks not on schedule and a resolution plan to return to the planned schedule;
  - Project status, including but not limited to issues encountered, proposed resolutions, actual resolutions, and variances to Project Plan;
  - The results of any tests, problem tracking report must be attached;
  - Anticipated tasks to be completed in the next week;
  - Task and Deliverable status, with percentage of completion and time ahead or behind schedule for tasks and milestones;
  - Proposed changes to key named resources, the Project work breakdown structure, or Project schedule, if any; and
  - Planned absence of Contractor staff and the expected return date.

Upon completion of each weekly status report, the State will immediately assess the health of the project and determine next steps for moving forward with the Project, within two business days of the meeting, which may include the following:

- Continue the Project;
- Terminate the Contract; or
- Suspend the Contract.

See General Terms and Conditions language in Attachment 1 for remedies for failure to deliver the proposed work.

**Utilize OIT’s Document Sharing/Collaboration Capability**

In conjunction with the delivery of the Project, coincident with the start of the project through its conclusion, the Contractor must use the State provided and hosted document management and team collaboration capability (e.g. Microsoft® SharePoint™) to provide access through internal state networks and secure external connections to all project team members, approved project stakeholders and participants. In conjunction with the utilization of this tool, the Contractor must:

- Structure the document management and collaboration pages and data structures in such a manner as to support the overall requirements of the Project;
▪ Be responsible for the maintenance and general upkeep of the designer configurations of the tool in keeping with commercially reasonable considerations and industry best practices as to not adversely impact the project delivery efforts performed by the Contractor and State; and

▪ At the conclusion of the Project, or upon request of the State, ensure that the State is provided a machine readable and comprehensive backup of the database(s) (e.g. Microsoft® SharePoint™) contained within the tool that is owned by the State and not proprietary to the Contractor or otherwise required by the State to maintain ongoing project documentation and artifacts (i.e., Contractor is to remove all Contractor proprietary or non-State owned or licensed materials from the tool).

**Maintaining Solution and Operations Documentation**

For all nonproprietary portions of the solution, and all elements of the solution that integrate with State systems, the Contractor must:

▪ Document the solutions developed or modified by the Contractor in accordance with established methods, processes, and procedures such that, at a minimum the State or a competent 3rd Party vendor can subsequently provide a similar scope of Services

▪ Develop and maintain, as agreed appropriate, the documentation on system environments. Where it is determined that documentation is inaccurate (for example, due to demonstrated errors or obsolescence), and such inaccuracy may negatively affect the Services, Contractor must correct such documentation as part of normal day-to-day operational support.

▪ Update programmer, End User and operational reference materials.

▪ Maintain all documentation on the State’s provided document management capability (e.g. Microsoft® SharePoint™).

**Deliverable 1. Project and Staffing Plan**

- Project scope and time; all Contracted Deliverables, Milestones and Work Products.
- Contractor Staff/Resource Loading.
- State Staff/Resource Loading.

**Deliverable 2. Requirements Catalogue, Operating Processes**

**Requirements Confirmation, Gap/Fit Analysis, Process Design/Validation**

The Contractor Team must review each of the functional and technical requirements provided by the State and conduct the VMS gap/fit analysis utilizing the VMS software. The Contractor will conduct the gap/fit analysis with the designated State subject matter expert(s) present.

The VMS gap/fit activity will confirm the software capabilities to fulfill the requirements and designate the means of fulfilling the requirements (out-of-the-box, configuration, customization).

The VMS gap/fit analysis may result in contractor or State recommendations for modifications to the State’s requirements. Recommendations for requirements changes will be documented by the Contractor and
reviewed by the State for acceptance. All changes to the State’s original functional requirements are to be clearly indicated in writing and agreed to by both parties.

The Contractor Team must document/edit the resulting business requirements in a State specified requirements file/database. Gaps must be identified if applicable as well as VMS customizations noted if applicable.

The gap/fit analysis will result in Contractor creating, or updating as appropriate, the VMS operating process documentation.

The operating process designs will be validated by the State stakeholder(s) impacted by the solution. As stated in the requirements, the initial number of State authorized users is estimated at less than 30.

The requirements analysis must also include, as necessary, the medical marijuana entity camera hardware requirements and camera-VMS connectivity requirements. If there are no requirements then specify as such. Requirement specifications will be documented to insure medical marijuana entities have a clear understanding of the camera hardware capabilities required for the VMS.

As an output of the process design validation, the Contractor will define the training audiences and courses that need to be developed in the subsequent phases.

The State team will be responsible for managing the Communication Plan, drafting and distributing communications to stakeholders

**Deliverable 2. Requirements Catalogue, Operating Processes**

- System Functional & Technical Requirements and Gap/Fit results.
  - Reporting requirements.
  - Alerts requirements.
- Medical marijuana entity camera hardware requirements & camera-VMS connectivity requirement specifications.
- Operating Processes documentation.
- Training audiences and courses.
Deliverable 3. Solution Architecture & Build Completion Document

The solution architecture depicts the VMS solution components including: hosted/cloud hardware and software architecture, environments, as well as the video connections to the network of medical marijuana entity facilities cameras.

The build completion work will fulfill all the requirements for the release scope as defined in Deliverable 2. The build work includes security to support the business processes, configuration, customizations and associated unit testing.

The build completion also results in creation and acceptance of environments for the solution development lifecycle and version control mechanisms are installed and functional. All development activity is subject to version control and managed by the appropriate environment prior to promotion to User Acceptance Test environment and ultimately Production environment.

Deliverable 3. Solution Architecture & Build Completion Document

- Solution Architecture document.
- Build Completion document.
Deliverable 4. Contractor System Test Completion & Training

System Test focuses on end-to-end testing of VMS processes and capabilities which includes customizations, configurations, and role security. For the VMS, there are no integrations planned with other State systems.

The Contractor is accountable for all activities associated with System Test, while the State will support these activities.

Test conditions and test scenarios to be included in the System Test will be mutually agreed upon by the Contractor and the State. These scenarios will be based on an analysis of the requirements, changes, and modifications that are approved for implementation.

The Contractor Team must prepare for testing and execute the system test. Testing preparation includes test plan, test conditions, test scripts, test schedule, and participation needs.

The Contractor Training Team must build training materials which include scenarios and training environment exercises, and job aids. The courses should contain “Real life” operating scenarios with data sets loaded into the training environment and training exercises to allow trainees to apply what they have learned.

The Contractor Training Team must deliver training to Department of Commerce and Pharmacy Board users.

Deliverable 4. Contractor System Test Completion & Training

- System Test Plan, Cases and Demonstration of Successful Completion of Same.
  - Validation of configuration and any customizations.
  - System Testing of all Reporting.
  - System Testing of all Alerts.
  - System Testing of security.
- Training Schedule and Training Environment Setup.
- Training Course scope and content.
  - Real-life operating scenarios with data sets for training environments.
  - Training materials needed including exercises, job aids.
- Training delivery.
Deliverable 5. State Acceptance Test Completion, Contractor Performance Test

UAT verifies the usability of the VMS and ensures that the system meets the requirements and business process needs of the organization. UAT leverages System Test Scripts and is executed by Department resources.

The State is accountable for User Acceptance Testing (UAT) execution while Contractor will be responsible for creating and maintaining the necessary environments, test preparation, and management and tracking of UAT activities.

During this Phase, the State may, at its sole discretion, elect to perform a Security and Data Protection audit that includes a thorough review of Contractor: controls; security/privacy functions and procedures; data storage and encryption methods; backup/restoration processes; as well as Security Penetration Testing and validation as described in this RFP. The State may utilize a 3rd Party Contractor to perform such activities as to demonstrate that all security, privacy and encryption requirements of this RFP are met. State Acceptance testing will not proceed until the Contractor cures all findings, gaps, errors or omissions pertaining to this audit to the State’s written satisfaction. Such testing will be scheduled with the Contractor at a mutually convenient time during the development and finalization of the Project Plan as required under Section 8 of this Supplement.

The Contractor Team must prepare weekly status reports to monitor the progress of each test phase. The status reports will contain sections for condition creation, script creation, script execution, issue identification and resolution, and defect identification and resolution.

The Contractor Team must execute a Performance Test. The goal of the test is to confirm the VMS is able to accommodate growth in the camera population at the medical marijuana entity facilities and maintain connectivity performance to the real-time camera views.

Deliverable 5. State Acceptance Test Completion, Contractor Performance Test

- Completion of State User Acceptance Testing and an affirmation of same by State.
  - Acceptance of Functionality.
  - Acceptance of all Reporting.
  - Acceptance of all Alerts.
  - Acceptance of role security.
  - A list of all customizations and Reports, Interfaces, Configurations, Forms and Workflows (RICEFW) objects as accepted.
  - Complete User and System Administration Documentation that represent the system as accepted.

- Completion of Performance Test.
Deliverable 6. Deployment/Onboarding Planning & Execution

The Contractor Team must perform the deployment planning and execution activities for implementation of the VMS at the Columbus, Ohio-based Department of Commerce and the Pharmacy Board. The Contractor Team must also perform VMS onboarding/deployment at the first group of medical marijuana entity facilities (cultivators, test labs, processors, dispensaries) across Ohio. The first group of entity facilities are estimated to be approximately 130 entity facilities operational by September 8, 2018 (the Ohio Medical Marijuana Control Program operational date).

The entity facilities will have staggered startup dates over a period of approximately 6 months. The entity facility deployment schedule will be mutually agreed upon by the State and Contractor. The Contractor deployment execution resource(s) will be utilized as needed to complete the staggered startup of approximately 130 medical marijuana entity facilities.

The VMS deployment at an entity facility is anticipated to include at a minimum:

- Facility identifier added to VMS as well as facility placement on Ohio map;
- Facility map showing camera placements added to VMS;
- Implement facility cameras connectivity to VMS; and
- Confirm camera connectivity and confirm camera operational status monitoring is operational.

The Contractor team must transition VMS deployment responsibilities and transfer knowledge to the State upon the conclusion of Deliverable 7: Final Acceptance. Knowledge transfer will include the VMS functional and technical information to enable the State to:

- complete the work associated with new facility camera startups;
- perform ongoing changes to facilities network and cameras population at the facilities; and
- provide user Help Desk type support.

Deliverable 6. Deployment/Onboarding Planning & Execution

- Deployment/Onboarding.
  - Department of Commerce and Pharmacy Board.
  - Medical marijuana entity facilities.
  o Knowledge transfer to State.
**Deliverable 7. Final Acceptance**

The VMS must successfully perform (defined as no Severity 1, 2 or 3 defects, which are clearly defined in the Attachment General Terms and Conditions) for forty-five (45) days within the State’s production environment after the State Medical Marijuana Control Program is operational (scheduled for September 8, 2018). During the 45-day period the Contractor must:

- Ensure adequate staffing from the Contractor Project Team is on hand (or available remotely) to ensure that during this 45-day period all defects identified by the State and mutually committed to be resolved by the Contractor in this RFP or under any SOW are adhered to.

- This responsibility shall specifically include:
  - Prompt isolation, triage and repair of any Severity 1, 2, or 3 defects;
  - Performance Monitoring of the System to ensure that there are no statistically significant (i.e., +5%) deviations from actual production performance as compared to the system performance prior to the implementation of Contractor developed elements;
  - All system functions perform and function as specified;
  - Compile all final versions of the system documentation, work products and delivery materials and locate / organize them as ‘FINAL’ on the State provided SharePoint site.
  - Obtain a final acceptance document from the State and the Contractor confirming that all of the above has been delivered and accepted as final.

If, during the 45-day period immediately following the introduction to Production, a Severity 1, 2, or 3 defect occurs that can be directly attributable to the efforts of the Contractor, and not the State or other non-Project parties, the 45-day period will, at the sole discretion of the State, be reset for additional 45-day periods until such time as the system can perform without Severity 1, 2, and 3 defects.

**Deliverable 7. Final Acceptance**

- State Final Acceptance of System.
- Successful Completion of Production Handoff and Operational Support Period.
- All Documentation Transferred to State.
IV. Contractor Qualifications

The contractor shall meet the following minimum qualifications and shall be specified within their proposal. Once the contract has been award, the awarded contractor shall maintain these requirements during the term of the contract.

1. Contractor shall have an office within the United States, preferably within the State of Ohio and provide documentation of the full legal name of the owner and business, primary business address, and other office locations.

2. Contractor shall have at least five years’ experience in Open Video Management Systems (VMS) and can provide documentation of VMS experience similar to mandatory requirements specified in the Scope of Work Section III. Contractor shall provide documentation of a minimum of four (4) Open Video Management Systems and services that they have successfully performed within the past five (5) years similar to the mandatory requirements specified Scope of Work, Section III.

3. Contractor shall provide contact information for at least four Open Video Management System references (state and/or government agencies preferred). The contact information shall include name of business, business address, point of contact, and telephone number.

4. Contractor must provide proof and/or documentation that they have the ability to provide the Division with a fidelity bond, financial guaranty bond, fidelity insurance or other financial guaranty from an entity licensed in the State of Ohio which provides protection to the Department against theft, loss, or other illegal diversion of property or funds by the Contractor, or its employees, officers agents and subcontractors.

5. Contractor must provide proof and/or documentation that they have the ability to provide general liability insurance against any and all claims for injuries to persons or damage to property occurring or arising out of the contractor’s obligations. The amount of such insurance shall be the minimum limits as follows, unless otherwise approved by the Division. Insurance shall be in an amount not less than the following:
   
   a. Five Hundred Thousand Dollars ($500,000) on account of bodily injury to or death of one person,
   
   b. One Million Dollars ($1,000,000) on account of bodily injuries or death of more than one person as a result of any one accident or disaster, and

   c. Two Hundred Fifty Thousand Dollars ($250,000) for property damages in any one accident.
V. Cost Proposal

This Section shall set forth the total fee Contractor requests for its services, including itemization of the cost for each deliverable and service to be provided.

In the interest of ensuring that total cost is factored within the State RFP Evaluation Process, the State, for evaluation purposes only, seeks a fully costed, all-inclusive price for the Offeror’s solution.

Work shall be quoted as a firm-fixed price cost not to exceed for the following:

- VMS Project Implementation and Services Costs;
  - Individual Deliverable costs (Deliverables described in section III.c);
- Ongoing annual recurring (5 year period) VMS Technical and Operating Services Costs;
  - Software Licensing and Ongoing Operations Costs;
  - System Hosting, Management and Administration;
  - Ongoing Software Upgrades, Break/Fix support, Enhancements and Customizations;
  - Backup and Restoration Services
- Other Costs as required to implement the complete solution.
VI. General Instructions

Contractor responding to this solicitation shall submit a proposal with the following required elements in order to be considered:

1. Executive Summary: Contractor shall provide an Executive Summary in the form of a standard business letter, signed by an individual authorized to legally bind the contractor, and shall acknowledge receipt of all addenda. The contractor shall provide a summary of the contractor’s services along with the point of contact, telephone number, federal tax identification number, and business address.

2. Table of Contents: The table of contents should facilitate locating all key points in the proposal.

3. Contractor Qualifications: In order to be considered for this opportunity the Contractor shall state how the business meets the minimum qualifications summarized under Section 4 of the RFP. The Contractor must demonstrate that it has the ability, qualifications, staff and experience to provide the services described herein in a professional and ethical manner.

4. Proposal Requirements: The Contractor must address the elements of the RFP by responding as concisely as possible to the following areas as related to the Scope of Work outlined in Section III. The proposal must address each of the three Scope of Work components listed below:

4(a). Scope of Work: VMS Capability Requirements

The State needs to understand the fit of the Offeror’s VMS solution to the State’s mandatory and desired list of VMS capability requirements (Scope of Work IIIa). Offerors are to indicate how (i.e., “Approach” in the table below); by whom (i.e., “State” or “Contractor” or “3rd Party”); and the relative Contractor complexity and effort required to accomplish the requirement in it’s entirely (i.e., “Effort Complexity” in the table below). Offerors are required to address every requirement contained in this RFP section IIIa using the following terminology nomenclature:

<table>
<thead>
<tr>
<th>Approach / Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offeror-proposed Tool/Solution</td>
<td>Offerors are to include the name and major version number of the Proposed Tool/Solution to address the requirement (e.g., Acme Corporation® WidgetMaster™ v9.1).</td>
</tr>
<tr>
<td>Out of the Box</td>
<td>Offerors are to indicate, in systems development hours (i.e., inclusive of all design, configure/build, test, implement), to be spent implementing this requirement using as-delivered functions of the Offeror-proposed solution.</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>Offerors are to indicate, in systems development hours (i.e., inclusive of all design, configure/build, test, implement), to be spent implementing this requirement using configurable functions (e.g., interfaces, reports, workflows, screen elements) of the Offeror-proposed solution.</td>
</tr>
<tr>
<td>Customization</td>
<td>Offerors are to indicate, in systems development hours (i.e., inclusive of all design, configure/build, test, implement), to be spent implementing this requirement using customized functions (e.g., interfaces, reports, workflows, screen elements) of the Offeror-proposed solution.</td>
</tr>
</tbody>
</table>
Offerors are to indicate, in systems development hours (i.e., inclusive of all design, configure/build, test, implement), to be spent implementing this requirement using as extensions or interfaces (e.g., interfaces, reports, workflows, screen elements) of the Offeror-proposed S2S System, State interfaces, or other Offeror provided solution elements.

Offerors are to indicate, in full systems development hours (i.e., design, configure/build, test, implement), to be spent implementing this requirement using this category for any item which does not fit into the aforementioned categories.

<table>
<thead>
<tr>
<th>Effort Complexity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>The Contractor can design, configure, test and implement the requirement within a one (1) FTE week in consideration of all required work (e.g., accomplish the requirement within 40 hours)</td>
</tr>
<tr>
<td>Medium</td>
<td>The Contractor can design, configure, test and implement the requirement within a one (1) FTE month in consideration of all required work (e.g., accomplish the requirement within 180 hours)</td>
</tr>
<tr>
<td>High</td>
<td>The Contractor can design, configure, test and implement the requirement within a one (1) FTE quarter in consideration of all required work (e.g., accomplish the requirement within 500 hours)</td>
</tr>
<tr>
<td>Extreme</td>
<td>The Contractor can design, configure, test and implement the requirement within a one (1) FTE year in consideration of all required work (e.g., accomplish the requirement within 1,980 hours)</td>
</tr>
</tbody>
</table>

4(b). Scope of Work: Technical and Operating Requirements
The State needs to understand the Offerors ability, tools, and approach to fulfill the Technical and Operating Requirements. Offerors are required to provide a response to every requirement contained in this RFP section IIIb.

4(c). Scope of Work: Deliverables
The State needs to understand the Offerors ability, tools, and methodology/approach to fulfill the Deliverable requirements. Offerors are required to provide a response to every Deliverable contained in this RFP section IIIc.

5. Cost Proposal: This section shall set forth the total fee Contractor requests for each deliverable and service to be provided as described in the RFP section V.

6. Standard Terms and Conditions: Signature is required in responding to the Request for Proposal affirming that you have reviewed and are in agreement with Attachment 1 General Terms and Conditions of the Ohio Department of Commerce.

7. Assumptions: The offeror must list all the assumptions the offeror made in preparing the Proposal. If any assumption is unacceptable to the State, the State may at its sole discretion request that the offeror remove the assumption or choose to reject the Proposal. No assumptions may be included regarding the outcomes of negotiation, terms and conditions, or requirements. Assumptions should be provided as part of the offeror response as a stand-alone response section that is inclusive of all assumptions with reference(s) to the section(s) of the RFP that the assumption is applicable to. Offerors should not include assumptions elsewhere in their response.
8. 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.
VII. Proposal Submission Deadlines and Restrictions.

Any questions and/or inquiries related to this request should be submitted through the State Procurement Portal. The Ohio Department of Commerce will not be responding to any inquiries made via phone and/or email.

All proposals should be submitted by 5:00 p.m. EST on September 6, 2017. The Department will not respond to any inquiries made after this time. The Department may reject any proposals or unsolicited proposal amendments that are received after the deadline. The Department reserves the right to reject proposals regardless of the cause of the delay.

Completed proposals shall be submitted via email in a current PDF format to:

Contract Administrator: Joy McKee  
Phone Number: (614) 644-2005  
Email Address: Joy.McKee@com.ohio.gov

Please note that when you submit a proposal to the Ohio Department of Commerce you understand the following:

1. If the Department amends the RFP, Contractor may amend its proposal within the time specified by the Department. Withdrawals must be made in writing.

2. The Department may seek clarification of deficiencies in a proposal.

3. The Department may waive any defects in any proposal or in the submission process followed by Contractor if it is in the Department’s interest and will not cause any material unfairness to other Contractors.

4. The Department reserves the right to cancel this RFP, reject all proposals, or seek to work through a new RFP, or other means.

5. If this RFP results in a contract award, it is acknowledged and understood by the Contractor that the contract will include this RFP, any written amendments to the RFP, the Contractor’s proposal, and written, authorized amendments the proposal, if any. It also will include any purchase orders and change orders issued under the contract.

6. Both parties acknowledge that the Department may enter into similar contracts with other parties, and that the Contract is not intended to establish an exclusive relationship for such services between the Department and Contractor.
VIII. Evaluation of Proposals and Award

Each Proposal will be reviewed to determine if it is responsive to the submittal requirements outlined in this Solicitation. A responsive Proposal is one which complies with the requirements of this Solicitation, includes all of the necessary documentation, is submitted in the format outlined in this Solicitation, is submitted in a timely manner and has the appropriate signatures as required on each document. Failure to comply with these requirements may result in the Proposal being deemed non-responsive.

An Evaluation Committee will review and evaluate the qualifications, prior experience, video management solutions, and price proposal of each Respondent. Respondents who have met the responsiveness requirements will be evaluated by the Committee in accordance with the criteria detailed under this Section. Evaluation Committee members will independently score the Proposals based on the merit of each Proposal, as determined by the Evaluation Committee members, to meet the requirements stated in this Solicitation. The total number of points scored by each Evaluation Committee member will be based on the maximum points available for each of the factors.

Criteria will be scored on a scale of “0” to “100” per evaluator with the maximum number of points available for each criterion as noted in this section. The maximum number of points to be scored under this process is 100 points. The final ranking will be based on a consensus score assigned by the Evaluation Committee, ranging from a score of “0” to “100.”

A) Video Management Solution (Maximum Points – 40)

This category is based on the Proposer’s VMS ability to meet the State’s needs, including, but not limited to the following:

- Video Management Solution requirements;
- Maintenance, Technical and Support services; and
- Additional Criteria (e.g. warranty, special features, etc.).

B) Experience, Qualifications, Staffing Plan (Maximum Points – 40)

This category is based on the Proposer’s experience and qualifications with focus on the successful implementation of similar programs.

C) Cost Proposal (Maximum Points – 20)

This category is based on the proposed price components, as well as price incentives and/or discounts, if any, offered by the Respondent.
Maximum Total Points: 100 (See Table Below)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Maximum Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>A) Video Management Solution</td>
<td>40</td>
</tr>
<tr>
<td>B) Experience, Qualifications, Staffing Plan</td>
<td>40</td>
</tr>
<tr>
<td>C) Cost Proposal</td>
<td>20</td>
</tr>
<tr>
<td>Maximum Evaluation Committee Member Score:</td>
<td>100</td>
</tr>
<tr>
<td>References</td>
<td>0</td>
</tr>
</tbody>
</table>

**References are not a scored criteria per se but are requested as part of this Solicitation and evaluation of the Solicitation.**

The Evaluation Committee may choose to invite Respondents to make a presentation and respond to questions from the Committee as part of the Evaluation process. Notice of assigned presentation times will be communicated in advance to the Respondent but may be given short notice of appearance. The Respondent’s presentation may clarify and summarize the content of its Proposal, but may not modify the prior written submission. Any communication between the Committee members and the Respondent made during the course of the interviews are intended primarily for purposes of providing clarification of the content the Proposal and are not to be construed as a "negotiation" of terms by either party. The final rankings shall be based on the scores issued by the Evaluation Committee based on either their review of the qualifications of each Proposal solely or the results of the Committee interviews, if any.

The State may award a Contract to the highest ranked firm based solely on their initial Proposal. Therefore, each initial offer should contain the Proposer’s best terms from a monetary and technical standpoint. Nonetheless, if the State proceeds to negotiate a Contract with the highest ranked firm and is unable to reach an agreement, the State reserves the right to terminate negotiations and may begin negotiations with the next ranked responsible and responsive Proposer. This process may continue until a contract acceptable to the State has been executed or all Proposals are rejected. No Proposer shall have any rights against the State arising from such negotiations or termination thereof.
ATTACHMENT ONE: GENERAL TERMS AND CONDITIONS

PART ONE: PERFORMANCE AND PAYMENT

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

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

Term. Unless this Contract is terminated or expires without renewal, it will remain in effect until the Project is completed to the satisfaction of the State, including all optional renewal periods for maintenance or continuing commitments, and the Contractor is paid. However, the current General Assembly cannot commit a future General Assembly to an expenditure. Therefore, this Contract will automatically expire at the end of each biennium, the first of which is June 30, 2019. The State may renew this Contract in the next biennium by issuing written notice to the Contractor of the decision to do so. This expiration and renewal procedure also will apply to the end of any subsequent biennium during which the Project continues, including any optional renewal periods. Termination or expiration of this Contract will not limit the Contractor’s continuing obligations with respect to Deliverables that the State paid for before or after termination or limit the State’s rights in such.

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

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

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

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

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

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

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

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

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

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

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

**Reimbursable Expenses.** The State will pay all reimbursable expenses identified in the RFP Documents, if any, in accordance with the terms in the RFP Documents and, where applicable, Section 126.31 of the Revised Code. The Contractor must assume all expenses that it incurs in the performance of this Contract that are not identified as reimbursable in the RFP Documents.

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

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

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

- (a) All statutory provisions under the Revised Code, including Section 126.07, have been met;
- (b) All necessary funds are made available by the appropriate State entities;
- (c) If required, the Controlling Board of Ohio approves this Contract; and
- (d) If the State is relying on federal or third-party funds for this Contract, the State gives the Contractor written notice that such funds are available.
Employment Taxes. All people furnished by the Contractor (the “Contractor Personnel”) are employees or subcontractors of the Contractor, and none are or will be deemed employees or contractors of the State. No Contractor Personnel will be entitled to participate in, claim benefits under, or become an “eligible employee” for purposes of any employee benefit plan of the State by reason of any work done under this Contract. The Contractor will pay all federal, state, local, and other applicable payroll taxes and make the required contributions, withholdings, and deductions imposed or assessed under any provision of any law and measured by wages, salaries, or other remuneration paid by or which may be due from the Contractor to the Contractor Personnel. The Contractor will indemnify, defend (with the consent and approval of the Ohio Attorney General), and hold the State harmless from and against all claims, losses, liability, demands, fines, and expense (including court costs, defense costs, and redeemable attorney fees) arising out of or relating to such taxes, withholdings, deductions, and contributions with respect to the Contractor Personnel. The Contractor’s indemnity and defense obligations also apply to any claim or assertion of tax liability made by or on behalf of any Contractor Personnel or governmental agency on the basis that any Contractor Personnel are employees or contractors of the State, that the State is the “joint employer” or “co-employer” of any Contractor Personnel, or that any Contractor Personnel are entitled to any employee benefit offered only to eligible regular fulltime or regular part-time employees of the State.

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

PART TWO: WORK AND CONTRACT ADMINISTRATION

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

Other Contractors. The State may hold other contracts for additional or related work, including among others independent verification and validation (IV&V) work for this Project. The Contractor must fully cooperate with all other contractors and State employees and coordinate its work with such other contractors and State employees as may be required for the smooth and efficient operation of all related or additional work. The Contractor may not act in any way that may unreasonably interfere with the work of any other contractors or the State’s employees. Further, the Contractor must fully cooperate with any IV&V contractor assigned to this Project. Such cooperation includes expeditiously providing the IV&V contractor with full and complete access to all project work product, records, materials, personnel, meetings, and correspondence as the IV&V contractor may request. If the State assigns an IV&V contractor to the Project, the State will obligate the IV&V contractor to a confidentiality provision similar to the Confidentiality Section contained in this Contract. Additionally, the Contractor must include the obligations of this provision in all its contracts with its subcontractors that work on this project.

Subcontracting. The Contractor may not enter into subcontracts related to the Project after award without written approval from the State. Nevertheless, the Contractor will not need the State's written approval to subcontract for the purchase of commercial goods that are required for satisfactory completion of the Project. All subcontracts will be at the sole expense of the Contractor unless expressly stated otherwise in the RFP Documents.
The State's approval of the use of subcontractors does not mean that the State will pay for them. The Contractor will be solely responsible for payment of its subcontractor and any claims of subcontractors for any failure of the Contractor or any of its other subcontractors to meet the performance schedule or performance specifications for the Project in a timely and professional manner. The Contractor must hold the State harmless for and must indemnify the State against any such claims.

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

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

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

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

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

If the Contractor fails to satisfy the requirements of the State with regard to security of information, or if an examination reveals information that would result in a continuing contractual relationship that causes the State to be in violation of any law, the State may terminate this Contract immediately without notice.
If the Contractor fails to satisfy the requirements of the State with regard to matters not related to items contained in the preceding two (2) paragraphs, the State will provide Contractor with notice and an opportunity to cure the failure within forty-five (45) days. If the failure is not cured by Contractor within such forty-five (45) day period, the State may terminate this Contract without further notice.

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

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

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

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

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

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

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

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

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

The Contractor may remove a person listed in the RFP Documents from the Project if doing so is necessary for legal or disciplinary reasons, or in the case of the person’s resignation of their employment with the Contractor or in the case of a leave of absence due to medical or personal extenuating circumstances. However, the Contractor must make a reasonable effort to give the State 30 calendar days’ prior written notice of the removal.

If the Contractor removes a person listed in the RFP Documents from the Project for any reason other than those specified above, the State may assess liquidated damages in the amount of $1,750.00 for every day between the date on which the individual was removed and the date that this Contract is terminated or the individual's qualified replacement, selected in accordance with the process identified in this section, starts performing on the Project. The State also may provide the Contractor with written notice of its default under this section, which the Contractor must cure within 30 days. Should the Contractor fail to cure its default within the 30 day cure period, this Contract will terminate immediately for cause, and the State will be entitled to damages in accordance with the Suspension and Termination Section of this Contract due to the termination. Should the State assess liquidated damages or otherwise be entitled to damages under this provision, it may offset these damages from any Fees due under this Contract.

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

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

(a) The State may assess liquidated damages in the amount of $1,750.00 for every day between the date on which the Contractor failed to provide the applicable notice, failed to provide the two replacement candidates, or the date the State rejected all candidates for cause and the date on which the Contractor affects a cure or the Contract expires without renewal or is terminated.

(b) The State may terminate this Contract immediately for cause and without any cure period.

Should the State exercise its option under item (a) above, it nevertheless will be entitled anytime thereafter to exercise its option under item (b) above. Additionally, should the State terminate this Contract under this provision, it will be entitled to damages in accordance with the Suspension and Termination Section of this Contract due to the termination. Should the State assess liquidated damages or otherwise be entitled to damages under this provision, it may offset these damages from any Fees due under this Contract.
The State may determine that the proposed replacement candidates meet the minimum qualifications of this Contract and still substantially reduce the value the State perceived it would receive through the effort of the original individual(s) the Contractor proposed and on whose credentials the State decided to enter into this Contract. Therefore, the State will have the right to reject any candidate that the State determines may provide it with diminished value.

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

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

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

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

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

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

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

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

The State will have the option of suspending this Contract in full or in part rather than terminating the Project, if the State believes that doing so would better serve its interests. In the event of a suspension for the convenience of the State, the Contractor will be entitled to receive payment for the work performed before the suspension. In the case of suspension of the Project for cause rather than termination for cause, the Contractor will not be entitled to any compensation for any work performed. If the State reinstates the Project after suspension for cause, rather than terminating this Contract after the suspension, the Contractor may be entitled to compensation for work performed before the suspension, less any damage to the State resulting from the Contractor’s breach of this Contract or other fault. Any amount due for work before or after the suspension for cause will be offset by any damage to the State from the default or other event giving rise to the suspension.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contractor acknowledges and agrees any individual providing personal services under this agreement is not a public employee for purposes of Chapter 145 of the Ohio Revised Code. Unless Contractor is a “business entity” as that term is defined in ORC section 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 Contractor shall have any individual performing services under this agreement complete and submit to the ordering agency the Independent Contractor/Worker Acknowledgement found at the following link:

https://www.opers.org/forms-archive/PEDACKN.pdf

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

**Ohio MBE Certification.** The MBE must maintain their certification throughout the term of the Contract, including any renewals. Failure to maintain such certification will be considered a breach of the Contract.
Publicity. The Contractor may not advertise or publicize that it is doing business with the State or use this Contract or the Contractor’s relationship with the State as a marketing or sales tool, unless the State agrees otherwise in writing.

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

Confidentiality. The State may disclose to the Contractor written material or oral or other information that the State treats as confidential ("Confidential Information"). Title to the Confidential Information and all related materials and documentation the State delivers to the Contractor will remain with the State. The Contractor must treat such Confidential Information as secret, if it is so marked, otherwise identified as such, or when, by its very nature, it deals with matters that, if generally known, would be damaging to the best interest of the public, other contractors, potential contractors with the State, or individuals or organizations about whom the State keeps information. By way of example, information must be treated as confidential if it includes any proprietary documentation, materials, flow charts, codes, software, computer instructions, techniques, models, information, diagrams, know-how, trade secrets, data, business records, or marketing information. By way of further example, the Contractor also must treat as confidential materials such as police and investigative records, files containing personal information about individuals or employees of the State, such as personnel records, tax records, and so on, court and administrative records related to pending actions, any material to which an attorney-client, physician-patient, or similar privilege may apply, and any documents or records excluded by Ohio law from public records disclosure requirements.

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

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

The Contractor's obligation to maintain the confidentiality of the Confidential Information will not apply where such:

1. was already in the Contractor's possession before disclosure by the State, and such was received by the Contractor without obligation of confidence; (2) is independently developed by the Contractor; (3) except as provided in the next paragraph, is or becomes publicly available without breach of this Contract; (4) is rightfully received by the Contractor from a third party without an obligation of confidence; (5) is disclosed by the Contractor with the written consent of the State; or (6) is released in accordance with a valid order of a court or governmental agency, provided that the Contractor (a) notifies the State of such order immediately upon receipt of the order and (b) makes a reasonable effort to obtain a protective order from the issuing court or agency limiting disclosure and use of the Confidential Information solely for the purposes intended to be served by the original order of production. The Contractor must return all originals of any Confidential Information and destroy any copies it has made on termination or expiration of this Contract.
Information that may be available publicly through other sources about people that is personal in nature, such as medical records, addresses, phone numbers, social security numbers, and similar things are nevertheless sensitive in nature and may not be disclosed or used in any manner except as expressly authorized in this Contract. Therefore, item (3) in the preceding paragraph does not apply, and the Contractor must treat such information as Confidential Information whether it is available elsewhere or not.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PART FOUR: REPRESENTATIONS, WARRANTIES, AND LIABILITIES

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

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

The warranties regarding material defects, merchantability, and fitness are one-year warranties. All other warranties will be continuing warranties. If any portion of the Project fails to comply with these warranties, and the Contractor is so notified in writing, the Contractor must correct such failure with all due speed or must refund the amount of the compensation paid for such portion of the Project. The Contractor also must indemnify the State for any direct damages and claims by third parties based on a breach of these warranties. This obligation of indemnification will not apply where the State has modified or misused the Deliverable and the claim is based on the modification or misuse. The State will give the Contractor notice of any such claim as soon as reasonably practicable. If a successful claim of infringement is made, or if the Contractor reasonably believes that an infringement claim that is pending may actually succeed, the Contractor must
do one of the following things: (1) modify the Deliverable so that it is no longer infringing; (2) replace the Deliverable with an equivalent or better item; (3) acquire the right for the State to use the infringing Deliverable as it was intended for the State to use under this Contract; or (4) remove the Deliverable and refund the amount the State paid for the Deliverable and the amount of any other Deliverable or item that requires the availability of the infringing Deliverable for it to be useful to the State.

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

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

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

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

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

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

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

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

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

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

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

**Limitation of Liability.** Neither party will be liable for any indirect, incidental, or consequential loss or damage of the other party, including but not limited to lost profits, even if the parties have been advised, knew, or should have known of the possibility of such damages. Additionally, neither party will be liable to the other for direct or other damages in excess of two times or $5,000,000 whichever is greater of the Not-To-Exceed Fixed Price of this Contract. The limitations in this paragraph do not apply to any obligation of the Contractor to indemnify the State against claims made against it or for damages to the State caused by the Contractor’s negligence or other tortious conduct.

**PART FIVE: ACCEPTANCE AND MAINTENANCE**

**Standards of Performance and Acceptance.** There will be a period for performance testing of the completed Project. During the performance period, the State, with the assistance of the Contractor, will
perform acceptance testing. The performance period will last up to 90 calendar days, during which time the Project must meet the standard of performance required by the RFP Documents for 45 consecutive calendar days. The performance criteria in the RFP Documents will be supplemented with the relevant user manuals, technical materials, and related writings, to the extent that the specifications in those writings supplement and refine rather than contradict the performance criteria in the RFP Documents. Acceptance of the Project depends on a successful completion of the performance period defined in this section and the RFP Documents. This section applies to the Project, and any part of it, as well as replacements or substitutes for the Project after completion of a successful performance period.

Project - Severity Defect Definitions:

- “Severity 1 Defect Service Request” means an incident where the State’s use of a solution service element has stopped or is so severely impacted that the State personnel cannot reasonably continue to work.

- “Severity 2 Defect Service Request” means an incident where the State’s Software or Processing Error that results in a partial or intermittent system outage or unavailability, performance items that result in undue delay of processing business cycle data and creation of a processing backlog, system performance and availability levels not adhering to agreed-upon SLAs, the State’s traditional performance levels, and generally accepted and customary industry standards for similar functions or capabilities, a temporary workaround identified but due to processing, hardware, labor or other considerations is deemed unreasonable by the State, or may be a recurring issue with identified or indeterminate cause.

- “Severity 3 Defect Service Request” means an incident where the State’s Software or Processing Error that results in a partial or intermittent system outage or unavailability, performance items that result in periodic, but not otherwise undue delay of processing business cycle data and creation of a processing backlog that spans a business cycle, system performance and availability levels not adhering to agreed-upon performance parameters, the State’s traditional performance levels, and generally accepted and customary industry standards for similar functions or capabilities, errors or omissions in the software, related software elements, operational processes or software integration suite for which a workaround exists, but have been reported to and accepted by the Contractor, an acceptable State agreed workaround has been identified and implemented, temporary workaround identified with State acceptable processing, hardware, labor or other considerations, may be a recurring issue with identified or indeterminate cause, and items otherwise not classified as a Severity 1 or Severity 2 Defect.

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

If the Project fails to meet the standard of performance after 90 calendar days from the start of the second performance period, the Contractor will be in default and will not have a cure period. In addition to all other remedies the State may have under this Contract, the State may request a correction or replacement of the relevant portion of the Project.
The Project may have components that can be tested for acceptance individually. If that is so, there may be acceptance criteria listed on the RFP Documents for each part of the Project that will be independently tested and accepted. However, unless the RFP Documents expressly provide otherwise, the failure of any independently tested component to meet its acceptance criteria will give the State the right to reject the entire Project. Alternatively, if the State determines that it is in the State's interest to reject only the part of the Project that was independently and unsuccessfully tested, it may do so. If the State chooses this option, the State will be entitled to a refund or credit toward the Contractor's Fee equal to the cost of acquiring a replacement for the rejected component.

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

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

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

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

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

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

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

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

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

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

The following services are outside the scope of this Contract:

a. Maintenance to bring the Equipment into compliance with any law, rule, or regulation if such law, rule, or regulation was not in effect on the acceptance date.

b. Repair and replacement work or increase in maintenance time as a result of damage or loss resulting from casualty or the State's misuse of the Equipment, damage resulting from improper packing or failure to follow prescribed shipping instructions (if such is done by the State), failure of electrical power, air conditioning or humidity control, use of supplies not approved by the original manufacturer of the Equipment as described or included in the Contractor's Proposal, or causes other than ordinary use of the Equipment.

c. Furnishing supplies or accessories, making specification changes, or adding or removing approved accessories, attachments, or other devices.
d. Maintenance or any increase in maintenance time resulting from any maintenance or inappropriate connection to other equipment (not done by the Contractor) that results in damage to the Equipment.

e. Activities required to restore the Equipment to good operating condition if the problem has resulted from someone other than Contractor's authorized service personnel repairing, modifying, or performing any maintenance service on the Equipment.

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

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

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

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

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

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

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

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

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

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

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

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

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

**PART SIX: CONSTRUCTION**

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

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

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

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

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

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

Notices. For any notice under this Contract to be effective, it must be made in writing and sent to the address of the appropriate contact provided elsewhere in the Contract, unless such party has notified the other party, in accordance with the provisions of this section, of a new mailing address. This notice requirement will not apply to any notices that this Contract expressly authorized to be made orally.
Continuing Obligations. The terms of this Contract will survive the termination or expiration of the time for completion of Project and the time for meeting any final payment of compensation, except where such creates an absurdity.

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

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

PART SEVEN: LAW AND COURTS

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

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

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

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

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

Equal Employment Opportunity. The Contractor will comply with all state and federal laws regarding equal employment opportunity and fair labor and employment practices, including Ohio Revised Code Section 125.111 and all related Executive Orders.
Before a contract can be awarded or renewed, an Affirmative Action Program Verification Form must be submitted to the Department of Administrative Services Equal Opportunity Division to comply with the affirmative action requirements. Affirmative Action Verification Forms and approved Affirmative Action Plans can be found by going to the Ohio Business Gateway at: http://business.ohio.gov/efiling/.

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

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

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

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

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

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

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

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

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

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

Any foreign corporation required to be licensed under O.R.C. § 1703.01-1703.31, which transacts business in the state of Ohio, without being so licensed, or when its license has expired or been canceled, shall forfeit not less than $250.00 nor more than ten thousand dollars. No officer of a foreign corporation (http://codes.ohio.gov/orc/1703.01 ) shall transact business in the state of Ohio, if such corporation is required by O.R.C. § 1703.01-1803.31 to procure and maintain a license, but has not done so. Whoever
violates this is guilty of a misdemeanor of the forth degree. Questions regarding registration should be directed to (614) 4663910, or visit [http://www.sos.state.oh.us](http://www.sos.state.oh.us).

**Compliance with the Ohio Revised Code.** It is expressly agreed by the parties that none of the rights, duties, and obligations herein shall be binding on either party if award of this Agreement would be contrary to the terms of Ohio Revised Code (“ORC”) Sections 127.16 or 3517.13 or ORC Chapter 102.

**Appropriation of Funds.** Performance by Department under this Agreement is contingent on the availability of lawful appropriation of funds by the Ohio General Assembly. If the Ohio General Assembly fails at any time to continue funding for any payments due under the Agreement, the Agreement will terminate as of the date that the funding expires without further obligation of Department.
Attachment 2: State Security, Privacy, and Data Handling Requirements
Open Video Management System

State IT Computing Policy Requirements
State Architecture and Computing Standards Requirements
State Security and Privacy Requirements
State Data Handling Requirements

Version Identifier | Date:
--- | ---
2.0 | 8/29/2016
3.0 | 9/27/2016
4.0 | 1/10/2017
5.0 | 1/31/2017

Contents

1. Overview and Scope ................................................................................................................. 62

2. State IT Policy Requirements ................................................................................................. 62

   3.1. Requirements Overview...................................................................................................... 62
   3.1.1. State of Ohio Standards ................................................................................................. 63
   3.1.2. Offeror Responsibilities ................................................................................................. 63
   3.2. Compute Requirements: Client Computing ........................................................................ 63
   3.2.1. Compute Requirements: Server / OS ........................................................................... 63
   3.2.2. Ohio Cloud: Hypervisor Environment ......................................................................... 64
   3.3. Storage and Backup Requirements .................................................................................... 64
   3.3.1. Storage Pools ................................................................................................................. 64
   3.3.2. Backup .......................................................................................................................... 64
   3.4. Networking Requirements: Local Area Network (LAN) / Wide Area Network (WAN)........... 65
   3.5. Application Requirements ................................................................................................. 65
   3.5.1. Application Platforms .................................................................................................... 65
   3.5.2. Open API’s ..................................................................................................................... 65
   3.5.3. SOA (Service Oriented Architecture) ........................................................................... 65
   3.6. Database Platforms ............................................................................................................ 66
   3.7. Enterprise Application Services ........................................................................................ 66
   3.7.1. Health and Human Services: Integrated Eligibility ....................................................... 66
   3.7.2. The Ohio Business Gateway (OBG) ............................................................................. 66
   3.7.3. Ohio Administrative Knowledge System (OAKS) ........................................................ 67
   3.7.4. Enterprise Business Intelligence ................................................................................... 68

RFP Number: COM2018-ADM008
4. General State Security and Information Privacy Standards and Requirements

5. State and Federal Data Privacy Requirements

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

7. Security Review Services

RFP Number: COM2018-ADM008
7.2. Security Standards by Device and Access Type ................................................................. 85
7.3. Boundary Defenses ........................................................................................................ 85
7.4. Audit Log Reviews ......................................................................................................... 85
7.5. Application Software Security ....................................................................................... 86
7.6. System Administrator Access ....................................................................................... 86
7.7. Account Access Privileges ........................................................................................... 86
7.8. Additional Controls and Responsibilities ....................................................................... 86

** Page numbers specific to Attachment 2, not the entire RFP.**
1. **Overview and Scope**

This Supplement shall apply to any and all Work, Services, Locations and Computing Elements that the Contractor will perform, provide, occupy or utilize in conjunction with the delivery of work to the State and any access to State resources in conjunction with delivery of work.

This scope shall specifically apply to:

- Major and Minor Projects, Upgrades, Updates, Fixes, Patches and other Software and Systems inclusive of all State elements or elements under the Contractor’s responsibility utilized by the State;
- Any systems development, integration, operations and maintenance activities performed by the Contractor;
- Any authorized Change Orders, Change Requests, Statements of Work, extensions or Amendments to this contract;
- 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 contract. In the event of a conflict for whatever reason, the highest standard contained in this contract shall prevail.

2. **State IT Policy Requirements**

The Contractor will comply with State of Ohio IT policies and standards. For the purposes of convenience, a compendium of IT policy and standard links is provided in the table below.

<table>
<thead>
<tr>
<th>Item</th>
<th>Link</th>
</tr>
</thead>
</table>
| DAS Policies              | 100-11 Protecting Privacy  
700-00– Technology / Computer Usage Series  
2000-00 – IT Operations and Management Series  

3. **State Architecture and Computing Standards Requirements**

3.1. **Requirements Overview**

Offerors responding to State issued RFQ/RFP requests, and as Contractors performing the work following an award, are required to propose solutions that comply with the standards outlined in this document. In the
event Offeror finds it necessary to deviate from any of the standards, a variance may be requested, and the Offeror must show sufficient business justification for the variance request. The Enterprise IT Architecture Team will engage with the Contractor and appropriate State stakeholders to review and approve/deny the variance request.

3.1.1. State of Ohio Standards

The State has a published Core Technology Stack as well as Enterprise Design Standards as outlined in this document and, due to State preferences, each are subject to improvements, elaboration and replacement. The State also provides numerous IT Services in both the Infrastructure and Application categories, as outlined in the State’s IT Services Catalog at: http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx

3.1.2. Offeror Responsibilities

For this RFP, offerors can only propose hosted cloud-based solutions. Offerors cannot propose on-premise solutions. Thus, requirements pertaining to on-premise solutions are not applicable.

When proposing on-premise solutions, Offerors and Contractors must comply with State requirements including using the State’s Virtualized Compute Platform. Offerors proposing on-premise solutions are required to install third party applications on State-provided compute platforms. Dedicated server platforms are not compliant with the State’s Virtualization Requirements.

In addition, Offerors are required to take advantage of all published IT Application Services where possible, (i.e., Enterprise Service Bus, Content Management, Enterprise Document Management, Data Warehousing, Data Analytics and Reporting and Business Intelligence). When dedicated Application components (i.e., Application Servers, Databases, etc.) are required, they should comply with the Core Technology standards. In addition, Offerors are required to take advantage of all published IT Application Services where possible, i.e. Enterprise Service Bus, Content Management, Enterprise Document Management, Data Warehousing, Data Analytics and Reporting and Business Intelligence. When dedicated Application components are required, i.e. Application Servers, Databases, etc., they should comply with the Core Technology standards.

3.2. Compute Requirements: Client Computing

Offerors must not propose solutions that require custom PC’s, Laptops, Notebooks etc. The State will source its own Client computing hardware and the Offeror’s proposed solutions are required to be compatible with the State’s hardware.

3.2.1. Compute Requirements: Server / OS

Offerors must propose solutions that comply with the State’s supported Server / OS versions.

The following are the State’s Required Server and OS versions.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
<th>Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows Server</td>
<td>2012, 2012 R2</td>
<td>Standard, Enterprise, &amp; Datacenter</td>
</tr>
</tbody>
</table>
When Offerors are proposing on-premise solutions, these solutions must comply with the State’s supported Server Compute Platforms.

The State hosts and manages the Virtual Server hardware and Virtualization layer. The State is also responsible for managing the server’s Operating System (OS). This service includes 1 virtual CPU (vCPU), 1 GB of RAM and 50 GB of Capacity Disk Storage. Customers can request up to 8 vCPUs and 24GB of RAM.

For Ohio Benefits and the Ohio Administrative Knowledge System (OAKS) – Exalogic Version 2.0.6.0.2

### 3.2.2. Ohio Cloud: Hypervisor Environment

When Offerors are proposing on-premise solutions, these solutions must comply with the State’s supported VMware vSphere, and IBM Power Hypervisor environment.

For Ohio Benefits and OAKS – Oracle Virtual Manager Version 3.3.1, Xen

### 3.3. Storage and Backup Requirements

#### 3.3.1. Storage Pools

The State provides three pools (tiers) of storage with the ability to use and allocate the appropriate storage type based on predetermined business criticality and requirements. Storage pools are designed to support different I/O workloads.

When Offerors are proposing on-premise solutions, these solutions must take advantage of the State’s Storage Service Offerings.

For Ohio Benefits and OAKS - HA (High Availability) storage used with Mirror configuration.

The pools and their standard use cases are below:

<table>
<thead>
<tr>
<th>Table 2 – State Supported Storage Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Storage Pool</strong></td>
</tr>
<tr>
<td><strong>Performance</strong></td>
</tr>
<tr>
<td><strong>General</strong></td>
</tr>
<tr>
<td><strong>Capacity</strong></td>
</tr>
</tbody>
</table>

#### 3.3.2. Backup

When Offerors are proposing on-premise solutions, these solutions must take advantage of the State’s Backup Service Offering.
Backup service uses IBM Tivoli Storage Manager Software and provides for nightly backups of customer data. It also provides for necessary restores due to data loss or corruption. The option of performing additional backups, archiving, restoring or retrieving functions is available for customer data. OIT backup facilities provide a high degree of stability and recoverability as backups are duplicated to the alternate site.

For Ohio Benefits - Symantec NetBackup is the Enterprise backup solution.

3.4. Networking Requirements: Local Area Network (LAN) / Wide Area Network (WAN)

Offerors must propose solutions that work within the State’s LAN / WAN infrastructure.

The State of Ohio’s One Network is a unified solution that brings together Design, Engineering, Operations, Service Delivery, Security, Mobility, Management, and Network Infrastructure to target and solve key Government challenges by focusing on processes, procedures, consistency and accountability across all aspects of State and local government.

Ohio One Network can deliver an enterprise network access experience for their customers regardless of location or device and deliver a consistent, reliable network access method.

The State provides a high bandwidth internal network for internal applications to communicate across the State’s LAN / WAN infrastructure. Normal traffic patterns at major sites should be supported.

Today, the State’s WAN (OARnet) consists of more than 1,850 miles of fiber-optic backbone, with more than 1,500 miles of it operating at ultrafast 100 Gbps speeds. The network blankets the state, providing connectivity to all State Government Agencies.

The State of Ohio Network infrastructure utilizes private addressing, reverse proxy technology and Network Address Translation (NAT). All applications that are to be deployed within the infrastructure must be tolerant of these technologies for both internal product interaction as well as external user access to the proposed system, infrastructure or application.

The State network team will review applications requirements involving excessive bandwidth (i.e. voice, video, telemetry, or applications) deployed at remote sites.

3.5. Application Requirements

3.5.1. Application Platforms

When Offerors are proposing on-premise solutions, these solutions must be developed in open or industry standard languages (e.g. Java, .NET, PHP, etc.)

3.5.2. Open API’s

Proposed vendor applications must be developed with standards-based Open API’s. An open API is an application program interface that provides programmatic access to software applications. Proposed vendor applications must describe in detail all available features and functionality accessible via APIs.

3.5.3. SOA (Service Oriented Architecture)
When Offerors are proposing on-premise solutions, these solutions *must* be developed using a standards-based Service Oriented Architecture (SOA) model.

3.6. **Database Platforms**

Proposed vendor application designs must run on databases that comply with the State’s supported Database Platforms.

- IBM DB2 Version 10
- Microsoft SQL Server 2012 or higher
- ORACLE 11G and 12C

3.7. **Enterprise Application Services**

The State of Ohio Office of Information Technology (OIT) provides a number of Enterprise Shared Services to State agencies as outlined in the IT Services Catalog available at: [http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx](http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx)

At a minimum, proposed vendor application designs that include the following Application Services *must* use the Application IT Services outlined in the IT Services Catalog.

3.7.1. **Health and Human Services: Integrated Eligibility**

The Integrated Eligibility Enterprise platform provides four key distinct technology domains / capabilities:

- **Common Enterprise Portal** – includes User Interface and User Experience Management, Access Control, Collaboration, Communications and Document Search capability
- **Enterprise Information Exchange** – includes Discovery Services (Application and Data Integration, Master Data Management (MDM) Master Person Index and Record Locator Service), Business Process Management, Consent Management, Master Provider Index and Security Management
- **Analytics and Business Intelligence** – Integration, Analysis and Delivery of analytics in the form of alerts, notifications and reports
- **Integrated Eligibility** – A common Enterprise Application framework and Rules Engine to determine eligibility and benefits for Ohio Public Benefit Programs

3.7.2. **The Ohio Business Gateway (OBG)**

The Ohio Business Gateway (OBG) offers Ohio's businesses a time-and-money-saving online filing and payment system that helps simplify business' relationship with Government agencies.

- **New Business Establishment** – Provides a single, portal based web location for the establishment of new businesses in Ohio, file with the required State agencies and ensure that business compliance requirements of the State are met.
- **Single Point Revenue and Fee Collection** - Manage payments to State’s payment processor (CBOSS) and broker payment to multiple agencies while creating transaction logs and Business Customer “receipts”.
- **Business One-Stop Filing and Forms** - Provides guides and forms to Business Users through complex transactions that have multiple steps, forms and / or filing requirements for users on procedures to complete the process including Agencies and (if applicable) systems they will need to interact with.
▪ Scheduling and Reminders - Notify Business Customers of a particular event that is upcoming or past due (Filing due) using a “calendar” or “task list” metaphor.
▪ Collections and Confirmations – Provides a Payment Card Industry (PCI) certified web-based payment solution that supports a wide range of payment types: credit cards, debit cards, electronic checks, as well as recurring, and cash payments.

3.7.3. **Ohio Administrative Knowledge System (OAKS)**

OAKS is the State’s Enterprise Resource Planning (ERP) system, which provides central administrative business services such as Financial Management, Human Capital Management, Content Management via myOhio.gov, Enterprise Learning Management, and Customer Relationship Management. Core System Capabilities include (but are not limited to):

**Content Management (myohio.gov)**
- Centralized Communications to State Employees and State Contractors
- OAKS alerts, job aids, and news
- Statewide Top Stories
- Portal to OAKS applications
- Employee and Contractor Management

**Enterprise Business Intelligence**
- Key Financial and Human Resources Data, Trends and Analysis
- Cognos driven standardized and adhoc reporting

**Financial Management (FIN)**
- Accounts Payable
- Accounts Receivable
- Asset Management
- Billing
- eBid
- eCatalog (Ohio Marketplace)
- eInvoicing
- eSupplier/Offeror Maintenance
- Financial Reporting
- General Ledger
- Planning and Budgeting
- Procurement
- Travel & Expense

**Customer Relationship Management (CRM)**
- Contact / Call Center Management

**Enterprise Learning Management (ELM)**
- Training Curriculum Development
- Training Content Delivery
Human Capital Management (HCM)
  ▪ Benefits Administration
  ▪ Payroll
  ▪ Position Management
  ▪ Time and Labor
  ▪ Workforce Administration: Employee and Contingent Workers
  ▪ Employee Self-Service
  ▪ eBenefits
  ▪ ePerformance
  ▪ Payroll

3.7.4. Enterprise Business Intelligence
  ▪ Health and Human Services Information
    ▪ Eligibility
      ▪ Operational Metrics
      ▪ County Caseworker Workload
    ▪ Claims
    ▪ Long Term Care
  ▪ Financial Information
    ▪ General Ledger (Spend, Disbursement, Actual/Forecast)
    ▪ Travel and Expense
    ▪ Procure to Pay (AP/PO/Offeror/Spend)
    ▪ Capital Improvements
    ▪ Accounts Receivable
    ▪ Asset Management
  ▪ Workforce and Human Resources
    ▪ Workforce Profile
    ▪ Compensation
    ▪ MBE/EDGE

3.7.5. SharePoint

Microsoft SharePoint Server 2013 portal setup and hosting services for agencies interested in internal collaboration, external collaboration, organizational portals, business process workflow, and business intelligence. The service is designed to provision, operate and maintain the State’s enterprise Active Directory Accounts.

3.7.6. IT Service Management

ServiceNow, a cloud-based IT Service Management Tool that provides internal and external support through an automated service desk workflow based application which provides flexibility and ease of use. The IT Service Management Tool provides workflows aligning with ITIL processes such as Incident Management, Request Fulfillment, Problem Management, Change Management and Service Catalog.
3.7.7. **Enterprise Geocoding Services**

Enterprise Geocoding Services (EGS) combine address standardization, geocoding, and spatial analysis into a single service. Individual addresses can be processed in real time for online applications or large numbers of addresses can be processed in batch mode.

3.7.8. **GIS Hosting**

GIS Hosting delivers dynamic maps, spatial content, and spatial analysis via the Internet. User agencies can integrate enterprise-level Geographic Information Systems (GIS) with map capabilities and spatial content into new or existing websites and applications.

3.8. **Productivity, Administrative and Communication Requirements**

3.8.1. **Communication Services**

The State of Ohio Office of Information Technology (OIT) provides a number of Enterprise Shared Services to State agencies as outline in the IT Services Catalog available at: [http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx](http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITServiceCatalog.aspx)

At a minimum, proposed vendor application designs that include the following Communication Services **must** use the Communication Services outlined in the IT Services Catalog.

**Exchange**
- Exchange Mail
- Office 365
- Skype for Business Instant Messaging & Presence
- Enterprise Vault
- Clearwell eDiscovery
- Exchange Web Services
- Bulk Mailing
- External Mail Encryption
- Outbound Fax
- Mobile devices

**EDI/Application Integration/Medicaid EDI**

**Lyris Listserv**

**On-premise application based FAX**

**eFAX**
- Fax2Mail is a “hosted” fax solution that allows agencies to seamlessly integrate inbound and outbound Fax with their existing desktop E-mail and back-office environments. Fax2Mail is a “cloud-based” solution.

**Voice over Internet Protocol (VoIP)**

**Audio Conference**

**Video Conference**

**Call Centers**
4. General State Security and Information Privacy Standards and Requirements

The selected Contractor will accept the security and privacy requirements outlined in this supplement in their entirety as they apply to the services being provided to the State. 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 Contract. The Contractor shall provide the State with contact information for a single point of contact for security incidents.

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. As a minimum, the Contractor shall provide vulnerability scan results to the State monthly.
- 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 contract. The Contractor will submit a draft Information Security Controls 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 the contractor with contact information for security and program personnel for incident reporting purposes.
- 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.

- Conduct a Security and Data Protection Audit, if deemed necessary, as part of the testing process.
- 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.

4.1. State Provided Elements: Contractor Responsibility Considerations

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

To the extent that Contractor’s accesses or utilizes State-provided networks, the Contractor is responsible for adhering to State policies and use procedures and doing so in a manner that does 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 contract 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. Notification is to be provided to the State for suspected as well as verified security events. For suspected events, the Contractor shall provide regular updates to the State on the status of efforts to verify the event as an actual security event.
- Provide vulnerability management services including supporting remediation for identified vulnerabilities as agreed.
- Support 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 to security risks and 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.

4.2. Periodic Security and Privacy Audits

The State shall be responsible for conducting periodic security and privacy audits, and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue or finding be discovered, the following resolution path shall apply:

- If a security or privacy issue exists in any of the IT resources furnished to the Contractor by the State (e.g., code, systems, computer hardware and software), 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. The Contractor is responsible for resolving any security or privacy issues that exist in any of the IT resources they provide to the State.
- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

4.2.1. State Penetration and Controls Testing

The state may, at its sole discretion, elect to perform a Security and Data Protection Audit, at any time, that includes a thorough review of contractor controls; security/privacy functions and procedures; data storage and encryption methods; backup/restoration processes; as well as security penetration testing and validation. The state may utilize a third party contractor to perform such activities as to demonstrate that all security, privacy and encryption requirements are met.

State Acceptance Testing will not proceed until the contractor cures all findings, gaps, errors or omissions pertaining to the audit to the state’s written satisfaction. Such testing will be scheduled with the contractor at a mutually convenient time during the development and finalization of the project plan, as required by the state.
4.3. **Annual Security Plan: State and Contractor Obligations**

The Contractor will develop, implement and thereafter maintain annually a Security Plan, that is in alignment with the National Institute of Standards and Technology ("NIST") Special Publication (SP) 800-53 (current, published version), for review, comment and approval by the State Information Security and Privacy Officers. As a minimum, the Security Plan 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)

4.4. **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 or Duo Security solutions.

4.5. **Security and Data Protection.**

All Services must also operate at the [moderate level baseline] as defined in NIST (SP) 800-53 (current, published version) [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. Services 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.

4.6. **State Information Technology Policies**

The Contractor is responsible for maintaining the security of information in environment elements under direct management of the Contractor 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 contract 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 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, providing incident investigation support with the agency’s assistance, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State Data access rules are not compromised.
Where the Contractor identifies a potential issue in maintaining an “as provided” State infrastructure element with the more stringent requirement of an agency security policy (which may be federally mandated or otherwise required by law), identifying to agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.

The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue be discovered the following resolution path shall apply:

- If a security or privacy issue is determined to be pre-existing to this Contract, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
- If over the course of delivering services to the State under this Statement of Work for in-scope environments the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Contractor is to notify the State within two (2) hours. This notification shall not minimize the more stringent Service Level Contracts pertaining to security scans and breaches contained herein, which due to the nature of an active breach shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

The Contractor will comply with State of Ohio IT policies and standards. For the purposes of convenience, a compendium of IT policy and standard links is provided in Section 2, State IT Policy Requirements.

5. **State and Federal Data Privacy Requirements**

Because the privacy of individuals’ personally identifiable information (PII) and State Sensitive Information, generally information that is not subject to disclosures under Ohio Public Records law, (SSI) is a key element to maintaining the public’s trust in working with the State, all systems and services shall be designed and shall function according to the following fair information practices principles. To the extent that personally identifiable information in the system is “protected health information” under the HIPAA Privacy Rule, these principles shall be implemented in alignment with the HIPAA Privacy Rule. To the extent that there is PII in the system that is not “protected health information” under HIPAA, these principles shall still be implemented and, when applicable, aligned to other law or regulation.

The Contractor specifically agrees to comply with state and federal confidentiality and information disclosure laws, rules and regulations applicable to work associated with this RFP including but not limited to:

- United States Code 42 USC 1320d through 1320d-8 (HIPAA);
- Code of Federal Regulations, 42 CFR 431.300, 431.302, 431.305, 431.306, 435.945,45 CFR164.502 (e) and 164.504 (e);
▪ Ohio Revised Code, ORC 173.20, 173.22, 1347.01 through 1347.99, 2305.24, 2305.251, 3701.243, 3701.028, 4123.27, 5101.26, 5101.27, 5101.572, 5112.21, and 5111.61; 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 SP 800-53 (current, published version).
▪ IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies

5.1. Protection of State Data

▪ Protection of State Data. “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, including, but not limited to, PII and SSI. To protect State Data as described in this Contract, 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 Contract;
▪ Use and permit its employees, officers, agents, and independent contractors to use any PII/SSI received from the State solely for those purposes expressly contemplated by the Contract;
▪ Not sell, rent, lease or disclose, or permit its employees, officers, agents, and independent contractors to sell, rent, lease, or disclose, any such PII/SSI to any third party, except as permitted under this Contract or required by applicable law, regulation, or court order;
▪ Take all commercially reasonable steps to (a) protect the confidentiality of PII/SSI received from the State and (b) establish and maintain physical, technical and administrative safeguards to prevent unauthorized access by third parties to PII/SSI received by the Contractor from the State;
▪ Give access to PII/SSI of the State only to those individual employees, officers, agents, and independent contractors who reasonably require access to such information in connection with the performance of Contractor’s obligations under this Contract;
▪ Upon request by the State, promptly destroy or return to the State in a format designated by the State all PII/SSI received from the State;
▪ Cooperate with any attempt by the State to monitor Contractor’s compliance with the foregoing obligations as reasonably requested by the State from time to time. The State shall be responsible for all costs incurred by Contractor for compliance with this provision of this subsection;
▪ Establish and maintain data security policies and procedures designed to ensure the following:
  ▪ Security and confidentiality of PII/SSI;
  ▪ Protection against anticipated threats or hazards to the security or integrity of PII/SSI; and
  ▪ Protection against the unauthorized access to, disclosure of or use of PII/SSI.

5.1.1. Disclosure

Disclosure to Third Parties. This Contract shall not be deemed to prohibit disclosures in the following cases:
▪ Required by applicable law, regulation, court order or subpoena; provided that, if the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether PII/SSI or otherwise, pursuant to court or administrative order, subpoena, summons, or other legal process or otherwise believes that disclosure is required by any law, ordinance, rule
or regulation, Contractor will promptly notify the State 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 the scope of such disclosure and the nature of wording of such disclosure) and Contractor will use commercially reasonable efforts to obtain confidential treatment for the information;

- 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.

5.2. 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 State Data from unauthorized disclosure, modification, use or destruction. 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 of State Data.
- 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.

5.3. 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 information.
- Assume all State Data is both confidential and critical for State operations. The Contractor’s security policies, plans, and procedure for the handling, storage, backup, access, and, if appropriate, destruction of State 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 State Data, as well as attacks on the Contractor’s infrastructure associated with the State 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 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 secure overwriting, 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 State Data in case of loss of State Data at the primary site. The Contractor’s backup solution must include plans to recover from an intentional deletion attempt by a remote attacker with compromised administrator credentials (e.g., keeping periodic copies offline, or in write-only format).

The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State 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 Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Contract. If necessary for such performance, the Contractor may permit State Data to be loaded onto portable computing devices or portable storage components or media 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. In addition, all state data on portable media shall be encrypted.
- Ensure that portable computing devices have anti-virus software, personal firewalls, and system password protection. In addition, the State 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.

5.4. Portable Devices, Data Transfer and Media

Any encryption requirement identified in this document 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 devices 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 contract.

5.5. Limited Use; Survival of Obligations.

Contractor may use PII/SSI only as expressly authorized by the Contract and for no other purpose. Contractor’s limited right to use PII/SSI expires upon conclusion, non-renewal or termination of this Agreement for any reason. Contractor’s obligations of confidentiality and non-disclosure survive termination or expiration for any reason of this Agreement.

5.6. Disposal of PII/SSI.

Upon expiration of Contractor’s limited right to use PII/SSI, Contractor must return all physical embodiments to the State or, with the State’s permission; Contractor may destroy PII/SSI. Upon the State’s request, Contractor shall provide written certification to the State that Contractor has returned, or destroyed, all such PII/SSI in Contractor’s possession.

5.7. Remedies

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

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

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

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

The Contractor shall not use State data for any engagements outside of the scope of the contracted agreement. Using State of Ohio data to test or provide proof-of-concept for other engagements is expressly prohibited.

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](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](http://www.hhs.gov/ocr/privacysummary.pdf).

5.9. 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 Contract. “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 (c) 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.

5.10. Federal Tax Information

Contract Language for General Services

5.10.1. Performance

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by its employees with the following requirements:

- All work will be done under the supervision of the Contractor or the Contractor's employees.
- Any return or return information made available in any format shall be used only for the purposes of performing this Contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Disclosure to anyone other than an officer or employee of the Contractor will be prohibited.
- All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of its computer facility, and no output will be retained by the Contractor after the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or its designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy...
printouts, and will provide the agency or its designee with a statement containing the date of
destruction, description of material destroyed, and the method used.

- All computer systems receiving, processing, storing, or transmitting Federal Tax Information must
meet the requirements defined in IRS Publication 1075. To meet functional and assurance
requirements, the security features of the environment must provide for the managerial, operations,
and technical controls. All security features must be available and activated to protect against
unauthorized use of and access to Federal Tax Information.

- No work involving Federal Tax Information furnished under this Contract will be
subcontracted without prior written approval of the IRS.

- The Contractor will maintain a list of employees authorized access. Such list will be provided to the
agency and, upon request, to the IRS reviewing office.

- The agency will have the right to void the Contract if the Contractor fails to provide the safeguards
described above.

5.10.2. Criminal/Civil Sanctions

1. Each officer or employee of any person to whom returns or return information is or may be
disclosed will be notified in writing by such person that returns or return information disclosed to
such officer or employee can be used only for a purpose and to the extent authorized herein, and
that further disclosure of any such returns or return information for a purpose or to an extent
unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as
$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
Such person shall also notify each such officer and employee that any such unauthorized further
disclosure of returns or return information may also result in an award of civil damages against
the officer or employee in an amount not less than $1,000 with respect to each instance of
unauthorized disclosure. These penalties are prescribed by IRCs7213 and 7431 and set forth at 26
CFR 301.6103(n)-1.

2. Each officer or employee of any person to whom returns or return information is or may be
disclosed shall be notified in writing by such person that any return or return information made
available in any format shall be used only for the purpose of carrying out the provisions of this
Contract. Information contained in such material shall be treated as confidential and shall not be
divulged or made known in any manner to any person except as may be necessary in the
performance of the Contract. Inspection by or disclosure to anyone without an official need-to-
know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as
$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.
Such person shall also notify each such officer and employee that any such unauthorized inspection or
disclosure of the officer or employee (United States for Federal employees) in an
amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or
disclosure with respect to which such defendant is found liable or the sum of the actual damages
sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case
of a willful inspection or disclosure which is the result of gross negligence, punitive damages,
plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.

3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the
Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C.
552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her
employment or official position, has possession of or access to agency records which contain
individually identifiable information, the disclosure of which is prohibited by the Privacy Act or
regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations provided for the performance of any work under this Contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with Contract safeguards.

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

6.1. **General**

If, over the course of the Contract 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 Contract, 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 a 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.

6.2. **Actual or Attempted Access or Disclosure**

If the Contractor determines that there is any actual, attempted or suspected theft of, accidental disclosure of, loss of, or inability to account for any PII/SSI by Contractor or any of its subcontractors (collectively “Disclosure”) and/or any unauthorized intrusions into Contractor’s or any of its subcontractor’s facilities or secure systems (collectively “Intrusion”), Contractor must immediately:

- Notify the State within two (2) hours of the Contractor becoming aware of the unauthorized Disclosure or Intrusion;
- Investigate and determine if an Intrusion and/or Disclosure has occurred;
- Fully cooperate with the State in estimating the effect of the Disclosure or Intrusion’s effect on the State and fully cooperate to mitigate the consequences of the Disclosure or Intrusion;
- Specify corrective action to be taken; and
- Take corrective action to prevent further Disclosure and/or Intrusion.

6.3. **Unapproved Disclosures and Intrusions: Contractor Responsibilities**
The Contractor must, as soon as is reasonably practicable, make a report to the State including details of the Disclosure and/or Intrusion and the corrective action Contractor has taken to prevent further Disclosure and/or Intrusion. Contractor must, in the case of a Disclosure cooperate fully with the State to notify the effected persons as to the fact of and the circumstances of the Disclosure of the PII/SSI. Additionally, Contractor must cooperate fully with all government regulatory agencies and/or law enforcement agencies having jurisdiction to investigate a Disclosure and/or any known or suspected criminal activity.

Where the Contractor identifies a potential issue in maintaining an “as provided” State infrastructure element with the more stringent of an Agency level security policy (which may be Federally mandated or otherwise required by law), identifying to Agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.

If over the course of delivering services to the State under this Statement of Work for in-scope environments the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Contractor is to notify the State within two (2) hour. This notification shall not minimize the more stringent Service Level Contracts pertaining to security scans and breaches contained herein, which due to the nature of an active breach shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.

6.4. 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. In the case of a suspected breach, the Contractor must notify the State in writing of the suspected breach within twenty-four (24) hours of the Contractor becoming aware of the suspected breach.

The Contractor must fully cooperate with the State to mitigate the consequences of such a breach/suspected 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/suspected breach and assist the State in making any notifications to potentially affected people and organizations that the State deems necessary or appropriate. The Contractor must document all such incidents/suspected 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.
7. Security Review Services

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

7.1. Hardware and Software Assets

The Contractor will support the State in defining and producing specific reports for both hardware and software assets. At a minimum this should include:

- Deviations to hardware baseline
- Inventory of information types by hardware device
- Software inventory against licenses (State purchased)
- Software versions and then scans of versions against patches distributed and applied

7.2. 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

7.3. Boundary Defenses

The Contractor will:

- Work with the State to support the denial of communications to/from known malicious IP addresses*
- Ensure that the System 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 System

7.4. Audit Log Reviews

The Contractor will:

- Work with the State to review and validate audit log settings for hardware and software
- Ensure that all 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.
7.5. **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

7.6. **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, particularly 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

7.7. **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

7.8. **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 System security program plan
- Update and Implement Risk Assessment Policies and procedures
- Update and implement incident response procedures