

Supplement One:

IT Optimization End-Point Computing Services

1. Overview

1.1. Background and Current Situation

The State, as part of its IT Optimization program and requirements to standardize end-user computing services has recently entered into two contractual relationships with Microsoft and McAfee for the provision of certain products designed to consolidate end-point computing functions for the State. In general the goals of this standardization effort include, but are not limited to:

- Implementation of a Common Desktop operating environment based on Windows 7 (Win7);
- Coordination through the State with Microsoft for the implementation of Microsoft Office365 (O365) and related cloud based functions for office productivity and document storage and sharing;
- Coordination through the State with McAfee or its reseller for the implementation of McAfee Security Products (McAfee) for end-point computing, this may require the installation of the McAfee agent by the offeror; and
- Incorporation of an Enterprise level Identity Domain (ID) based on Active Directory (AD) and Forefront Identify Manager functions (FIM).

The summary goals of this RFP and the contracted work are, at a high level, as follows:

- Development of an end-point discovery function to determine the most appropriate upgrade/update or replacement strategy and capability for the State;
- Implementation of the discovery function on a selected State Agency (in this case the Office of Medicaid) as a Proof of Concept (POC);
- Development, in collaboration with the State of a set of Policies and Procedures (or if applicable enhancements to existing policies) to identify, update, replace, administer and maintain the current Agency environment(s) to follow and adhere to State Standards;
- Implementation of these new Policies and Procedures initially for the selected State Agency, and to be extensible to Statewide computing following the successful conclusion of the POC inclusive of change management (people/processes), communications (awareness, rationale and expectation management) and feedback (customer and technical challenges/issues);
- Implementation of Updates / Replacements of existing Operating System(s), End-Point Security software/tools, O365, and incorporation into the State's ID Domain that results in a common desktop environment and experience;
- Updates to existing business processes and technical support Policies and Procedures to both support the new desktop environment as well as to accommodate both new Agency rollouts and incremental additions of new desktops to the POC Agency (the actual execution of which are outside of Contractor work in this RFP);
- Identification and removal/update/replacement of both non-standard tools in the POC Agency relative to the defined scope tools (i.e., Win7, O365, McAfee and ID) as well as anticipated incompatible software elements on the end-point devices that will or may conflict with, conflicted by, or rendered obsolete the in-scope tools; and
- Implementation of a temporary "virtual help desk" to be used during the POC period to support extended/enhanced care during the POC migration process as a support function to existing end-user help desk functions, but specific to the migration, and accommodation for knowledge transfer activities.

A detailed set of State requirements to achieve the above containing additional information, roles, deliverables and State functions follows.

1.2. Project Context and Organization

At a high level, the Project can be summarized as follows. Offerors may choose to alter the approach, relationships and organization of this Project Context diagram shown below as they see fit, as long as all deliverables, activities and work product requirements contained in this RFP are delivered as required.

Project Context: Windows 7, Office365, McAfee and State ID Project

Project Management Responsibilities

Project Planning and Mobilization

- Project Plans
- Communications
- Status
- Roles & Responsibilities

Agency Baseline and Discovery

- Scope / Approach
- Tools and Techniques
- Communications and Processes
- Variance to Standards
- Implementation Approach and Plan

Proof of Concept Agency Migration

- Office of Medicaid
- Implement Migration
- Refine Process and Tools
- Provide Virtual Help Desk
- Document method to be reusable for other Agencies

Policy and Change Management

- Computing Policies
- Security Policies
- Document Storage and Use Policies
- Communications and Awareness
- Job and Training Aids

Method & Tool Standardizations

- Update Technical Deliverables
- Update Process & Change Deliverables
- Provide Scoping and Estimating frameworks
- Enable State replication of Contractor process

1.3. Document Convention: Deliverable Identification

All items in this Supplement that are marked with a red star (★) shall be considered formal deliverables and be subject to the State's Deliverable Acceptance Process described in this RFP.

1.4. General Timing Considerations

The State requires that all work in this RFP be completed no later than August 31, 2014. The Evaluation Criteria of this RFP have special provisions pertaining to scoring of offeror responses with respect to project timing and completion. Offerors are to consider these provisions as part of their response.

2. Agency Baseline and Discovery Services

Agency Baseline and Discovery Services contain those elements designed to identify all end-user devices (e.g., desktops, laptops, and mobile/tablet computers) and departmental file servers that comprise the applicable scope for an agency migration. In general, end-point computers shall serve as the basis of this effort and the final scope, approach, work steps, change issues and resolutions and actual implementation of the migration to the identified technology elements shall be based on these end-point computers. The scope will not include non-Microsoft related devices and not include non-Microsoft related devices (e.g., Blackberry, iPhone/Pad, Android devices or user personal devices) that do not connect to State resources directly.

To complete this effort, the Contractor must:

- Provide an approach and toolset (both software technology, process and reporting/verification capability) to identify a final scope of migration elements for an Agency (in general) and the Office of Medicaid (Medicaid) specifically as a POC.
- Perform an active scan of State provided networks and sub-networks for Medicaid to identify and confirm the end-point inventory for the POC (and extensible to other Agencies under Section 6 of this RFP).
- During the scan, identify non-Standard or non-compliant operating systems, security software, user administration software and Microsoft Office versions to be the subject of migration to State Standards.

- ★ Provide a report to the State of all in-scope end-point devices discovered with identification of State Standard exceptions (e.g., non-Windows 7, non-Office 365, non-McAfee) and incompatible/conflicted software items that will be rendered obsolete or unusable as a result of the Agency migration to State Standard.
- Develop a phased technology rollout program based on end-user practicalities (e.g., workloads, processing cycles, availability, etc.) in light of the implementation approach (e.g., staged/rolling operating system upgrades, removal/replacement of Microsoft Office to O365, removal/replacement of security products to McAfee, notification of obsolete, unusable or incompatible product(s) with the above). The rollout program must be completed efficiently and minimize disruptions to agency operations.
- ★ Develop a day-by-day implementation plan based on all of the above for State review and approval to be executed and implemented in the POC described in Section 4 of this Supplement.

3. Policy, Process and Change Management

In parallel with Agency focused technical discovery tasks described in Section 2, the Contractor is to work with DAS/OIT Policy, Security and End-Point Services teams to review and revise (or replace if required) existing State Policies, Procedures and Processes to implement the new end-point operating environment (and if necessary, augment these policies with Agency specific considerations) Specifically the Contractor will:

- Collaborate with the DAS/OIT Policy group to review and update existing State end-point computing policies and provide advisory services as to changes required in a general “Standards” sense (e.g., operating system standards, windows update policies, security tools, scanning intervals, update to virus/malware definitions, etc.);
- Collaborate with the DAS/OIT Policy group to review and update State rules for the implementation of O365 ; OneDrive (formerly SkyDrive) features with respect to: i) personal document management and storage; ii) State confidential or PII materials; iii) migration of existing desktop stored documents and work products to OneDrive (formerly SkyDrive); iv) migration of existing departmental/agency documents and work products to either OneDrive (formerly SkyDrive) or a DAS/OIT provided SharePoint collaboration site(s) depending on the nature of the data and its use or other on premise Electronic Content Management (ECM) Solution; v) policies on the phased retirement of non-OneDrive (formerly SkyDrive) or SharePoint document management and collaboration services; migration of locally maintained mailboxes (Outlook or otherwise) to O365 based services and Storage; migration from existing end-point authentication services (or lack thereof) to the State Enterprise ID Domain based on Active Directory and Forefront security frameworks;
- Collaborate with DAS/OIT to develop and establish Policies for “Bring your own Device” (BYOD) Policies for State Personnel computing devices used in performance of State work (e.g., tablets/mobile devices, personal computers) as well as Policies for State contractor’s to follow in utilizing or accessing State infrastructure with their devices via Contractor collaboration and input by way of recommendations into the State’s Mobile Computing Strategy (issued under a separate RFP) which is a parallel effort to the work in this RFP;
- Establish guidelines and guiding principles for the use and adoption of Virtual Desktop Infrastructure (VDI) devices for centralized administrative use, call centers or other large concentrations of State personnel that perform their job responsibilities utilizing a substantially standard computing image and toolset;
- ★ Create an initial draft and incorporate State updates to this draft of all Policy changes based on the above for State review, approval and implementation;
- Based on the anticipated Policy changes, and specific to the POC in Section 4, develop a set of end-user communication and awareness documents (using the most appropriate method whether an email newsletter, YouTube™ video, PowerPoint presentation or similar) that helps the State communicate the rationale, change imperative, timing, steps and ongoing implications of these Policy changes;
- ★ Develop implementation and administration rules based on these policies for the State to implement and administer that include: on/off-boarding of non-Standard end-point products; removal/update/replacement of non-standard products with State standard products; removal/update/replacement of incompatible or obsolete components with suitable State provided replacements; incorporation of new end-user communities into DAS/OIT based Services (e.g., ID, SharePoint, O365, McAfee, etc.);
- ★ Develop an end-user job aid that (in simple, non-technical terms) describes what files (administrative, sensitive, PII, etc.) to store where (e.g., locally, OneDrive (formerly SkyDrive), SharePoint or elsewhere);
- ★ Develop a migration checklist to be used in Section 4 that is designed to validate compliance with State policies and implement:

- Standardization of Desktop Operating Environments;
 - Migration of Operating Systems to Windows 7;
 - Migration of Productivity Tools to Office365 (working with Microsoft resources to coordinate product implementation services);
 - Migration of Security Software to McAfee (working with McAfee or designated reseller resources to coordinate product implementation services), additionally, the selected offeror may be responsible for installing the McAfee client agent;
 - Migration of User Documents (within Policy) to OneDrive (formerly SkyDrive);
 - Migration of User Documents (within Policy) to SharePoint or secure State Storage;
 - Removal of Non-Standard Operating Systems, Productivity Tools and Security Software based on the successful migration to State Standard;
 - Identification and escalation to the State for resolution of local area network naming, IP addressing, Firewall and network access requirements and dependencies; and
 - Identification of Incompatible or Non-Standard Computing Software that will need remediation, removal or replacement as a result of the migration.
- ★ Develop a migration roles / responsibilities and timing or participation schedule inclusive of all State, Contractor, Agency and End-User participation as required to affect a successful migration including:
- Technical Infrastructure elements as required and provided by the State (e.g., ID Domain, Domain Integration, Domain Updates, Software Distribution and Update Services, License Administration, Monitoring and Tracking);
 - Agency Specific Elements including Agency Help Desks, Computing Devices, Software, End-User Management & Communications, training and job aids; and
 - Contractor Specific elements and requirements of the State including access to networks and end-user devices, installation and operation of scanning/inventory software servers/tools, software update servers/tools, end-user notification and coordination tools and processes and other Contractor scope items as defined or required herein.

3.1. State of Ohio Security and Privacy Policies

Current State of Ohio IT, IT Security and Privacy Policies are available to offerors for review at:

Item	Link
Statewide IT Standards	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITStandards.aspx
Statewide IT Bulletins	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITBulletins.aspx
IT Policies and Standards	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies/tabid/107/Default.aspx
DAS Computing and Operations Standards	100-11 Protecting Privacy), (700 Series – Computing) and (2000 Series – IT Operations and Management) http://das.ohio.gov/Divisions/DirectorsOffice/EmployeesServices/DASpolicies/tabid/463/Default.aspx

4. Technology and Process Migration Implementation Services – Proof of Concept (POC)

As part of the Contracted services required by the State under this RFP, the Contractor is to plan, execute, orchestrate State support and participation and perform certain post-migration activities utilizing a live Agency of sufficient size and scope to validate the overall approach, tools, processes, Policies and Procedures, execution of the migration and assembly of “lessons learned” as a result of completion of the migration. To that end, the State has identified and obtained the support of the Ohio Department of Medicaid to serve as an entry point for proof of concept of the requirements and goals contained herein before they are rolled out to other Statewide Agencies by

the State, the State and the Contractor, or other parties at the discretion of the State following the conclusion of the POC.

4.1. General – Ohio Department of Medicaid (Medicaid) Statistics and Operating Environment

The Ohio Department of Medicaid was established by legislation in July of 2013 as a Cabinet-Level Agency from certain elements of the Ohio Department of Jobs and Family Service (ODJFS). In support of this creation of a “new Agency” there has been a close working relationship established between DAS/OIT, ODJFS and Medicaid in the selection and implementation of IT processes and systems. Medicaid has several enterprise level projects and programs associated with delivering their core remit as well as the implementation of systems to support the Affordable Care Act.

The current operating environment can be described as a hybrid of former ODJFS services and newer DAS/OIT provided services and this effort is designed to better align Medicaid with existing and emerging State standards and software.

Offerors are advised that Medicaid, as part of routine technology refresh activities, will be replacing approximately 800 end-user desktops in the mid-March 2014 time period. These machines will be Windows7 based and in general have a consistent desktop image. These desktops are the subject of this RFP and offerors are to “retrofit” State Windows7 configurations, conventions, settings and the like, and add O365, McAfee, ID domain, networking, etc. elements to these desktops in accordance with the other requirements contained in this Supplement.

Offerors are advised (for scoping and planning purposes) that Medicaid, from a sizing statistics perspective is as follows:

Scope Element	Sizing / Description
End-Users (State Personnel)	778 (800 planned users)
FY 14 Computing Procurement	Medicaid is purchasing and anticipates the receipt of approximately 800 end-user computers as part of a scheduled technology refresh in mid-March 2014.
Desktop OS	In general Windows XP Professional, with certain localized/small deployments of Windows 7
Virtual Desktops	Small/localized implementations of Virtual Desktops/Thin-Client Systems, with one base image for all Thin-Client systems
Non-State Personnel	100-200 Contractors using their own end-user devices/computers but are subject to compliance with State IT and Security policies
Desktop Backup	Less than 1% of PCs have local backup / restore functionality. A process of purchasing and deploying local backup capabilities to all mobile and critical desktop systems is being scoped and planned by the Medicaid.
Departmental File Sharing/Collaboration	Generally Novell clients, certain filenet based data stores to be migrated to OneDrive (formerly SkyDrive), SharePoint or DAS/OIT shared services
Office Network Connectivity	Local Area Network (Novell clients, IP Addressable) 100Mb/s Private and Public 802.11g networks – public internet accessible on common ports Site connectivity to State DAS/OIT provided networks with internetworking to ODJFS networks Common DNS, SNMP, DHCP services available locally
Virus, Malware, Endpoint Security	Inconsistent/Mixed Microsoft, Symantec, McAfee and Kaspersky, but generally 99 percent have Computer Associates (CA) Antivirus installed and running.
Productivity	Microsoft Office 2010 (predominant) with small/localized Office 2007 installations
Other Desktop Applications and Considerations	Common Adobe PDF (read/write), OEM printer device drivers, departmental file and print services (shared Novell LAN drives)
Printing Environment	Local Print Servers (GroupWise) to be migrated to DAS/OIT provided/addressable print management and queues. In general printers are IP addressable as well, there may be direct users (i.e., non-queued) of Medicaid printers.
DAS/OIT Software Distribution & Management Frameworks	DAS/OIT currently has an installed deployment of Microsoft System Center and Big Fix for patch management, deployment and distribution functions. In addition, the State has access to BigFix services for similar functions and will be utilizing Tivoli Endpoint Manager (TEM) within the Data Center.

Should, upon completion of Discovery and Inventory activities under Section 2 of this Supplement the Contractor or State determine that deviations in these statistics are material to the Contractor's proposed cost and timing, the State and Contractor will adjust this Contract via a State approved change on a basis no less favorable than the unit cost provided in the Cost Proposal Form for this RFP for Migration Services related to this Section 4. For example, if the Contractor proposes completion of the migration for the aforementioned 778 desktops for \$10 each for a total of \$7,780 and subsequently the State and Contractor determine that there are in fact 878 desktops the Contractor, upon State approval, shall be entitled to initiate a Change Request for the incremental 100 desktops for the quoted unit cost of \$10 each for a total of \$1,000. Likewise, should less desktops be discovered or determined to be in scope, the amount may be reduced for the migration for the unit price of \$10 per end-user desktop. Offerors are to note that the values contained above are illustrative in nature and do not reflect State expectations as to the cost or value of this RFP.

4.2. Migration Requirements

The Contractor will perform and implement the following elements of the Migration for Medicaid:

- ✦ Automated Scanning and Inventory of all in-scope end-user computing devices and provision of interim (at scan midpoint or stop points) and final summarized reporting to the State;
- ✦ Development of a phased schedule to perform the upgrades/migrations based on the automated inventory scan that incorporates State specific maintenance windows and blackout periods;
- Creation of at least two Reference Desktop Images to be used to perform the migration that is accessible via State Software distribution server(s); State FTP site, secure removable media (e.g., DVD or encrypted USB drive) as mutually deemed appropriate to perform the migration that includes (at a minimum) an image file(s) that includes:
 - Image One: Incremental installation to the new Medicaid desktops (purchased in mid March) to bring them to State Standard for all in scope elements;
 - Image Two: Final "gold" version of State image for any new PCs that enter the environment subsequent to the mid-March purchase;
 - Installation Files/Images as Applicable to the Software Elements in this RFP (e.g., Win7, O365, McAfee);
 - Baseline configuration and settings for these Software Elements based on State approved values to attain compliance with State policies as developed under Section 3 of this Supplement;
 - Other Windows User Access Control (UAC) and Windows Registry configuration settings as required by policy and State Standards as well as to support the integration of monitoring updates and reporting back to the State (DAS/OIT) Security Information and Event Management (SIEM) service;
 - Common Win7/O365/McAfee Updates, Patches, Service Pack(s) to help preclude prolonged updates and network access upon initial use (e.g., machines should be installed and useable with as up to date a version of all software as possible) to maximize the initial user experience;
 - Integration with the States DAS/OIT ID Domain;
 - Installation of State specific PDF job aids pertaining to the migration and document storage policy on the User Desktop for easy reference;
 - Common helper applications (e.g., .NET, Oracle, JavaVM, Adobe PDF reader, Silverlight, Flash, browsers) with baseline configuration values set (e.g., State bookmarks, popup blockers, tracking, etc.) pre-configured; and
 - Other settings as deemed appropriate by the State and Contractor to help with the migration and maximize user satisfaction.
- Completion of the Windows 7 Upgrade, Migration to O365 (coordinating Microsoft resource effort for migration to O365 through the State), Migration to the McAfee Security Suite software update/replacements (coordinating McAfee or its reseller resource effort for migration to McAfee Security Suite through the State);
- Incorporation of all Medicaid users in the State ID domain;

- Incorporation of all McAfee clients into the State SIEM (monitoring and reporting);
- Support of the State in the rollout and execution of Policies Processes and Change Management communications as created by the Contractor and State under Section 3 of this Supplement;
- Creation of reporting for obsolete, replaced and non-compatible software elements as a result of the migration; and
- ★ Production of a final report, based on the in-scope inventory for State approval that validates and provides evidence that the migration is complete.

In support of Change Management elements, the Contractor will:

- Identify, Plan and Orchestrate Contractor team, State (DAS/OIT) required support, technology elements, software licenses and ID domain adoption;
- Support the State (DAS/OIT and Medicaid IT) in managing end-user expectations, risk and issue management;
- Support the State in change awareness programs inclusive of Policy, Rules Processes and change elements for those end-users participating in the migration; and
- Implement elements of the agreed change program as developed in Section 3 and required by the migration for the POC.

The State (DAS/OIT) will:

- Provide technical details, support and assistance in understanding the State's ID domain inclusive of Active Directory structures, roles rules, policies and procedures as reasonably required for the Contractor to implement the migration;
- Provide access to State software license and executable repositories (i.e., licenses, executables, installers, etc.) for the in scope software elements (generally Win7, O365 and McAfee) as required by the Migration;
- Provide access to SharePoint standards and implementation guides to facilitate any migrations from eRoom or departmental collaboration tools to SharePoint;
- Support and develop approaches to resolve or implement workarounds for Medicaid specific local area network addressing, naming, firewall and network access considerations that arise as a result of Medicaid utilizing legacy ODJFS computing infrastructure elements and DAS/OIT provided standards;
- In concert with Medicaid, provide expertise and council on related efforts such as network consolidation, SOCC remediation, eMail migration, Identity Domain inclusion, Medicaid Elevation, Medicaid Integrated Eligibility as they impact the Contractor's scope and efforts under that scope;
- Establish and support Contractor interactions with Microsoft and McAfee with respect to in-scope software elements;
- Establish SharePoint sites as requested for Contractor or Medicaid Use; and
- Support the Contractor in technical interactions with Microsoft, McAfee and DAS/OIT based services under the State's maintenance agreements with these OEMS.

The State (Medicaid) will:

- Provide a single point of technical contact to understand or broker understanding with Medicaid (and if required ODJFS) Subject Matter Experts;
- Provide initial awareness briefings and support the Contractor and DAS/OIT in project kickoffs, periodic updates (newsletters or localized face to face briefings) and scheduling/coordination of migration events;
- Provide technical details and environments as required and available as to existing Medicaid end-user configurations and conventions; and
- Provide a schedule of major business events, processing cycles and holidays to inform the Contractor's planning of the migration effort.

4.3. Virtual Help Desk Augmentation Services

During the migration process, the Contractor will establish and support a Virtual Help Desk that is designed to augment the State's existing end-user help desk and provide "hyper-care" to those State individuals that are included in each migration phase or event. These services are not designed to replace State help desks but to provide specific help for those users that require it as a result of the migration or as an augmentation service to existing help desk functions that the State will retain and maintain.

As part of the Virtual Help Desk, the Contractor will record statistics and common issues encountered specific to the migration and:

- Augment all Project materials (e.g., processes, communications, tools, installation images, etc.) to refine subsequent migration events or phases and serve to eliminate common problems;
- Develop a compendium of common issues and solutions, FAQs, workarounds and user issues that require specialized State/Contractor support or resolution; and
- Serve as an objective basis to "lessons learned" obligations as required under Section 6 of this Supplement.

Should the State require the extension of these Virtual Help Desk services for a duration longer than included in the offeror's proposal, the State may extend these services under terms no less favorable than contained in the offeror's proposal. Should this need arise, the State will consult with the Contractor and develop a mutually agreeable Change Request to accommodate State needs beyond what is proposed by the offeror.

The goal of these services is to minimize migration related issues as well as to develop a repeatable method for the State to execute under future migrations.

4.4. Post-Migration Obligations

Following the completion of the migration and concurrent with the State's acceptance of the migration, the Contractor will:

- Update all methods, plans, procedures, tools/techniques, guides, installation images and communications elements created or used during the Project to reflect a generic Agency target toolkit for a subsequent migration event;
- Develop, as a result of joint State and Contractor "lessons learned" an improvement document that streamlines the process (e.g., reduces or eliminates superfluous activities and efforts) and amplifies or includes those elements to foster a more efficient or high quality migration for the next Agency; and
- ★ Present the above for formal approval/acceptance by the State and post to the State provided Project SharePoint site for ongoing State use.

5. Standardization of Migration Method(s) and Tool(s)

Upon completion of 50% of the migration, the Contractor will update and package all deliverables and work products conducted under the Proof of Concept phase for Medicaid and ensure they are reusable and extensible for State use for all other Agencies in the State under a focused State-led migration program.

The Contractor will:

- Develop a standard toolkit to replicate and perform an Agency migration regardless of size that include: inventory and discovery tools;
- Provide accommodation for existing Agency tools or recommendations to the State for non-Contractor specific tools that could be functionally equivalent to those tools used by the Contractor for the POC;
- Update all processes, communications/change documents, rules and images to serve future State migrations;
- Suggest to the State any minor edits/alterations to Policy (if required) based on the lessons learned in the POC; and

- ★ Consolidate and post all of the above to the State provided Project SharePoint site and seek State acceptance of same.

6. Lessons Learned and Approach following Successful POC

6.1. General

- ★ To assist the State in developing a scalable and extensible migration approach, the Contractor will develop a Lessons Learned Deliverable that includes:
 - Agency Communications and Engagement Frameworks;
 - Common issue compendium for networks (e.g., names, addresses, firewalls, access) user software (e.g., non-Standard, obsolete, conflicting or otherwise incompatible) and other items discovered during the POC or, in the experience of the Contractor are common under similar migrations, with approaches, techniques and tools to resolve such issues;
 - Estimating guides (cost, timing, duration, resources);
 - A phasing strategy based on State provided profiles of Agency computing functions (e.g., large/small Agency, degree of standardization, software fragmentation, version compliance, cultural considerations, etc.); and
 - Recommendations for the State to implement and maintain for the Ongoing Maintenance, Administration and Updates to the Policies, processes, tools and conventions developed herein.

Upon request the State may require a formal quotation from the Contractor for certain elements of future migrations. In the event of this circumstance, any Contract arising from this RFP shall allow and provide for continuance of Contractor services to perform mutually agreeable Migration or Support of State Migrations by the Contractor. The State is under no obligation to accept this quotation and the Contractor shall not perform any services outside of the scope of this RFP pertaining to other Agency migrations without the expressed written consent of the State under an approved change to the Contract that arises from the Award of this RFP. Offerors are advised not to include the likelihood of obtaining such a change in the construction and submission of their response to this RFP.

6.2. Project Methods and Tools: State Employee Knowledge Transfer and Education

- ★ In addition to the requirements in this section, and coincident with the conclusion of the work contained in this Supplement, the Contractor will design and create materials and provide a statewide implementation approach for State employees, which is designed to convey project and technical knowledge associated with performing similar projects at other State Agencies. The Contractor will conduct knowledge and documentation transfers for the final project processes and tasks and work to help ensure an overall body of knowledge is created to assist State employees in reasonably performing similar roles in keeping project quality, timeliness and accuracy considerations associated with the delivery of the POC.
- As part of the above, provide Agency to State and State to Agency processes and procedures to address post Migration/Implementation/ Steady-state support and issue resolution/ escalation processes that includes the definition of both Agency and State: roles and responsibilities; hand-off points; Service Level Agreement frameworks; and issue tracking and ticket management for Agency and Central Support Help Desk/Service Center interactions. This effort includes Internal State processes for Level 2 and 3 support across different OIT Central support divisions and functions (e.g., Network, Server, Storage, Desktop, Active Directory, etc.) which are to be based upon processes and solutions using State ServiceNow tools.

7. General Project Management and Reporting Conventions and Requirements

In conducting this Project for the State, the Contractor will:

- Be responsible for overall Project completion;
- Maintain the overall Project Workplan;

- Ensure deliverables have a detailed project sub plan as required by the State to ensure timely delivery and appropriate quality;
- 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;
- Ensure that an appropriate “Project Kickoff” occurs and that all integrated work plans are agreed to by the State from project commencement;
- Complete status reporting adhering to the PMO policies;
- 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.

7.1. Create and Maintain Project Plan

The Contractor must produce a detailed Project Plan, in electronic and paper form, to the Project Representative for approval within twenty business days after the State issues a purchase order or other written payment obligation under the Contract. The Contractor must lead a planning session which ensures the following:

- A common understanding of the work plan has been established;
- A common vision of all deliverables has been established;
- Contains a critical path that identifies all major milestones, dependences (both internal and external to the project), resources by name and resource assignments and is complete and inclusive of the entire work effort from commencement until conclusion of all contracted activities; and
- Clarity on scope of overall project and the responsibilities of the Contractor has been defined and agreed to by the State.

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 at no additional cost to the State, correct all deficiencies and resubmit it for the State’s review and approval until the State accepts the Deliverable.

7.2. Meeting Attendance and Reporting Requirements.

The Contractor’s project management 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 (i.e. MS Project) on electronic media acceptable to the State;
 - Status of currently planned tasks, specifically identifying tasks not on schedule and a resolution plan to return to the planned schedule;
 - Issues encountered, proposed resolutions, and actual resolutions;
 - The results of any tests;
 - A Problem Tracking Report must be attached;
 - Anticipated tasks to be completed in the next week;
 - Task and Deliverable status, with percentage of completion and time ahead or behind schedule for tasks and milestones;
 - Proposed changes to the Project work breakdown structure and Project schedule, if any;
 - Identification of Contractor staff assigned to specific activities;
 - Planned absence of Contractor staff and the expected return date;
 - Modification of any known staffing changes; and
 - System integration/interface activities.
- The Contractor's proposed format and level of detail for the status report is subject to the State's approval.
- Prepare Monthly Status Reports – During the Project, the Contractor must submit a written monthly status report to the Project Representative by the fifth business day following the end of each month. At a minimum, monthly status reports must contain the following:
 - A description of the overall completion status of the Project in terms of the approved Project Plan (schedule and cost, if applicable);
 - Updated Project work breakdown structure and Project schedule;
 - The plans for activities scheduled for the next month;
 - The status of all Deliverables, with percentage of completion;
 - Time ahead or behind schedule for applicable tasks;
 - A risk analysis of actual and perceived problems;
 - Testing status and test results; and
 - Strategic changes to the Project Plan, if any.

7.3. Develop, Submit, and Update Detailed Activity Plans.

As part of the Project and no later than twenty business days following the commencement of the effort, the Contractor must develop a Project Management Plan (Project Plan). The Contractor also must update the plans with more detail throughout subsequent Project phases coincident with Project Status reports or upon reasonable request of the State Project Manager to address, at a minimum, the following subjects:

- ★ Project Plan including (at a minimum):
 - Project Integration;
 - Project Scope;
 - Project Time;
 - Project Quality;
 - Project Staffing;
 - Project Communications;
 - Project Risks/Issues; and
 - Project Procurement.

The offeror must develop these plans from information that the State's Project personnel provide. These State personnel have varying percentages of time to devote to this Project, and the offeror must consider (and specify) time commitment expectations to the Project in creating the Project schedule and when obtaining information from State staff to create the above plans.

7.4. Utilize DAS/OIT's Document Sharing/Collaboration Capability

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

- Structure the document management and collaboration pages and data structures in such a manner as to support the overall requirements of the Project;
- Be responsible for the maintenance and general upkeep of the designer configurations of the tool in keeping with commercially reasonable considerations and industry best practices as to not adversely impact the project delivery efforts performed by the Contractor and State; and
- At the conclusion of the project, or upon request of the State, ensure that the State is provided a machine readable and comprehensive backup of the SharePoint™ database(s) contained within the tool that is owned by the State and not proprietary to the Contractor or otherwise required by the State to maintain ongoing project documentation and artifacts (i.e., Contractor is to remove all Contractor proprietary or non-State owned or licensed materials from the tool).

7.5. Project Management Cost Considerations

The offeror will provide project management costs for each element of this Supplement by Major Work Effort (i.e., Sections 1 to 7 inclusive) by month of the project.

7.6. Project Management Methodology, Minimum Standards

The State maintains a project management and reporting methodology that is used at varying levels for complex, transformational Information Technology projects. This methodology is designed to provide a substantive and objective framework for the reporting and review of projects to impacted stakeholders and, should the need arise, identify the need for corrective action for one or many of the participants in a project (e.g., State, Contractor, Customer, Stakeholder).

The State acknowledges that various contractors that may do business with the State may maintain unique or proprietary project management methodologies, but seeks to ensure that the overall project is delivered to the State as contracted. Therefore a minimum standard project management reporting standard has been created to serve the State's project management and oversight needs while not adversely impacting or influencing Contractor provided delivery methodologies.

The Contractor must provide a summary Project Plan as requested by the State. For purposes of a summary project plan specific phase and gate dates, effort and costs are a sufficient minimum.

Following the award of this Contract, and during the project mobilization phase Contractors must include all deliverables and milestones within their detailed project plans and methodologies at a minimum upon commencement of the project: