Vendor Instructions for Business (BR) and Technical (TR) Requirements

Vendor Response Column: Place a “Yes” if the current release of the software can fully support ALL the functionality described in the row, without special customization. A “Yes” can only be used if the delivery method is Standard (see delivery method instructions below). Otherwise, enter an "No"; A "No" can only be used with delivery method Future, Custom, or Not Available/Not Proposing (see delivery method instructions below).

Criticality Column:
(M) Indicates a requirement that is "Mandatory". The State considers it to be of such great importance that it must be met in order for the proposal to be accepted. If the proposer believes that there is something about their proposal that either obviates the need for this requirement or makes it of less importance this must be explained within the comments. The State retains the right to accept a proposal if the need of the requirement is reduced or eliminated by another feature of the proposal.
(P) Indicates a requirement which is "Preferred". This requirement is considered by the State to be of great usefulness but the lack of this feature is not considered serious enough to disqualify the proposal.
(O) Indicates a requirement which is "Optional". This requirement is considered by the State to be one which useful or potentially useful but not a central feature of the Project.

Delivery Method Column:
Complete the delivery method using a Standard, Future, Custom, or Not Available/Not Proposing (as defined below) that indicates how the requirement will be delivered.

Standard - Feature/Function is included in the proposed system and available in the current software release.
Future - Feature/Function will be available in a future release. (Provide anticipated delivery date, version, and service release in the comment area.)
Custom - Feature/Function can be provided with custom modifications. (Respondent must provide estimated hours and average billing rate or flat cost for the software modification in the comment area. These cost estimates should add up to the total cost for software modifications found in the cost summary table in Section X of the RFP).
Not Available/Not Proposing - Feature/Function has not been proposed by the Vendor. (Provide brief description of why this functionality was not proposed.)

Comments Column:
For all Delivery Method responses vendors must provide a brief explanation of how the requirement will be met. Free form text can be entered into this column.

Vendor Instructions for Activity, Deliverable, and Milestone

Vendor shall complete the Activity Deliverable, and Milestone Table identifying estimated delivery date and price.

BUSINESS REQUIREMENTS					
			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
GENERAL SPECIFICATIONS					
B1.1	Data Migration: The cloud-based database must be able to upload data from the LIHEAP database (SQL 2019) and other systems into the cloud-based database in order to create and maintain the previous program particpants and a WAP waiting list, including tracking and archiving from the list units that have been previously weatherized. Existing applications or data must be migrated into the new cloud-based database to assure that the transition will be accompanied with minimal manual intervention and impact on NHDOE staff	M			
B1.2	Supports all major web browsers with responsive design to work with various screen resolutions. Support use of software on portable devices such as; smart phones, I pads, tablets	M			
B1.3	The cloud-based database must perform all tasks necessary to provide end users with a single point of access that includes information such as: administrative and fiscal data; client intake, eligibility and supporting documentation, and property and whole-house assessment data	M			
B1.4	Capability to maintain and edit data for individuals and families (including individuals sharing a household) at any point in time and with traceable history of edits and how they are linked. Changes pre populate to all programs. Capability to remove duplicate client records. Capability to merge partial separate records on the same individual and family.	M			
B1.5	The cloud-based database must accept data input by the state and Subgrantees using multiple funding sources for the purposes of reimbursement and eligibility. Reimbursement can be received through multiple funding sources and must be tracked separately by program year, funding source, measure, client, and unit	M			

B1.6	The cloud-based database needs to have the capacity to accept on-line applications, electronic signatures and document uploads/downloads with security assurances throughout the system. Must have a multi-lingual option. Must provide a method of aging and retrieving uploaded applications and documentation to be associated with a particular applicant's record. Allow applicant to edit, view and upload to the application until it is submitted. Once submitted for processing, ability for applicant to check application status and agency download for processing. Include a timeframe for applications ie: after 30 days of no activity, online application is no longer valid.	M			
B1.7	Ability and option to do electronic payments to vendors or check writing through the system with related accounting functions such as; invoice entry, check reconcilliations, 1099s	M			
B1.8	Capability to import customer data or service data from a flat file or other external source. Capability to upload documents, files and images so that files may be audited online or electronically; accept scanned supporting documents while associating those files with a given beneficiary's records.	M			
B1.9	Ability for NHDOE to access all subgrantee records in one combined access point. Ability to choose by agency or a statewide search	M			
B1.10	Ability to process vendor files and agreements into system with data recording on case record.	M			
B1.11	Software must include basic customization tools to allow Agency System Administrators the ability to update maintenance tables such as towns, landlords and employers, and business rules to correspond with program rules, create an online library of commonly used forms.	M			
B1.12	Ability to retain participant data from one program year to the next to allow for pre populating a new year’s application. Application would be assigned a new program year and case number.	M			
B1.13	System must be able to support 175 users with growth in the future, along with online users.	M			
B1.14	Ability to perform a nightly EDI transmission to the respective utility for the EAP	M			
B1.15	Ability to track eligibility time period and provide a method of managing the cases requiring recertification.	M			

B1.16	Provide ability to perform accounting functions such as; Fiscal Budgets and Monthly and Quarterly Expenditures, Balance Sheet, Income Statement, Annual Audit System, vendor payments and associated financial functions to meet program fiscal requirements ie; check reconciliations, payment lookups, inoice entry, produce 1099s for landlord payments, voided checks, refunds are returned to client record and tracked.	M			
B1.17	The cloud-based database must be capable of importing data from the NH specific energy audit, currently Targeted Retrofit Energy Analysis Tool (TREAT) and attach to a particular case record. Data from the TREAT tool can be exported/imported in the following formats; PDF, Excel, HPXML or Word.	M			
B1.18	Ability to update vendor files including a check off for vendor requirements met. Ability to activate and de activate vendors.	M			
B1.19	Ability to track case benefit amounts and payments and balances. Ability to limit expenditures based on benefit provided, contract limits, expenditures per home.	M			
B1.20	Support multiple programs, each with different requirements and data fields. The system must have ability tosupport new programs as they arise.	M			
B1.21	Ability to update programs as needed with changes such as: eligibility determination, benefit levels, reporting requirements within a 5 day period, notification and vendor letters.	M			
Reporting					
B2.1	Capability to dynamically generate reports based on selected parameters, dates and other terms. Such parameters may include; starting date, ending date, gender, family size, income level, zip code, ward, age, educational level completed, source of income, program or service provider, type of housing. Capability to store reports history for repeated use. Capability to export a user-created report to a Word document, Excel or Adobe.	M			
B2.2	Capability to produce required Federal Reports for FAP and WAP and state specific reports.	M			
B2.3	Fraud detection mechanisms to provide a system wide check across all subgrantees via a SSN check to prevent duplication of services. Pop up with information of which agency application is active at.	M			

B2.4	Provide a mechanism for Agency and subgrantee, if authorized, to IMPORT/EXPORT data directly to/from proposed database (using XML or similar protocol). This would include the ability to generate real-time reports to support service delivery, planning, monitoring, quality assurance, scheduling appointments and other reporting requirements.	M			
B2.5	System updates that keep NH DOE programs in compliance with grantees are included as part of ongoing maintenance	M			
B2.6	Capability for staff persons to generate a report of pending follow -up actions needed.	M			
B2.7	Provide a process where the program years are defined and a "rollover" of the current applications in system convert to the new program year. The rollover will automatically deobligate all case benefits. Retain household data to pre populate new applications in subsequent years. Retain data in an accessible manner for a period of 5 years.	M			
Security					
B3.1	Personally Identifiable Information (PII) must be encrypted during transit, use and at rest.	M			
B3.2	Ability to provide vendors with a secure method ie: portal to upload and download participant documents., check on eligibility status and benefit amount.	M			
B3.3	System administration permissions and ability to assign user security levels. Ability to add, disable, and delete users and agencies. Ability to assign administrators within the agency to manage their users. Administrative access must operate within SSO.	M			
B3.4	Back-up of Data: Security of the web-based database must also include an automatic backup of all data entered in a secure secondary location on a daily basis.	M			
B3.5	The Vendor shall ensure all applicable technologies used will meet appropriate security configurations. For example, this may include, but is not limited to, current components of the National Institute of Science and Technology (NIST) SP 800 series guidelines, Open Web Application Security Project (OWASP) Top 10 vulnerabilities list, and Social Security Administration (SSA) requirements.	M			
B3.6	Vendor shall ensure that during the term of the contract, it shall maintain possession or control of any Agency data in a confidential and secure manner and it must have the ability to encrypt critical data.	M			

B3.7	The Vendor shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of Agency data and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.	M			
B3.8	All employees of Vendor who will have access to Agency data shall be advised by the awarded Vendor of the confidential nature of the information and that unauthorized disclosures of client information may result in the imposition of possible criminal penalties.	M			
B3.9	The Vendor agrees to assume responsibility for protecting the confidentiality of Agency data it is provided access to or uses in the performance of any contract awarded under this RFP that is not publicly available information.	M			
B3.10	Vendor will accept responsibility for all data breaches resulting from vulnerabilities within the Vendor's System including but not limited to notification of affected parties and corrective actions determined by Agency, all at Vendor's sole cost and expense.	M			
B3.11	Utilize computer back-up and recovery systems and procedures to prevent loss of data required for ADES reports and any disruption or degradation of services.	M			
B3.12	Develop an executable exit strategy that would allow data portability and transition to another solution should this become necessary in the future.	M			
B3.13	System administration permissions and ability to assign user security levels. Current security levels. Ability to assign administrators within the agency to manage their users security levels.	M			
B3.14	SSO – Single Sign On – The users are authenticated using a single sign on to gain access to areas of the application for which they have access permissions – e.g., user, admin, etc..	M			
B3.15	MFA – Multi-Factor Authentication – User's logon authentication requires multiple authentication methods – e.g., username and password, plus at least one other authentication method	M			
B3.16	Insure all data is backed up on a nightly basis.	M			
TESTING REQUIREMENTS/TRAINING					

B4.1	Training: The Bidder(s) must provide training sessions for users of the cloud-based database at dates and locations to be determined by NHDOE. The trainings must be in-depth and on-site/virtual for NHDOE and Subgrantee personnel at the initiation of the web-based database to ensure that end user understands how to properly use the database and perform work in an efficient manner	M			
B4.2	The cloud-based database must be able to direct those that are not technologically inclined to the next step in the process. The web-based database must contain “Help” and “What’s This?” features, as well as a user manual so that the average person can easily navigate through the web-based database. Use of a "bug site" or method to report issues is desirable.	M			
B4.3	Test Environment for NHDOE Staff to preview, try, and to train system - annual subscription with Hosting/Support for secondary server staging environment including regular updating of data	M			
B4.4	Updates and Upgrades: The Bidder(s) must provide training at times when substantial updates are implemented and must provide pre-and post- launch support for the pre- and post-launch maintenance to include updates, user manual updates, upgrades, error correction(s), and training NHDOE staff and Subgrantee on use and maintenance of the software, at no additional cost	M			
B4.5	Provide users with a software manual, outlining all functions. Provide updates to manual within 5 days	M			
B4.6	On-line Training: The Bidder(s) must develop an on-line training tool for the web-based database for usage by NHDOE staff, Subgrantees, and other potential users	M			
B4.7	The Bidder(s) must provide in-depth training and assistance as needed to ensure that technical staff understand how to perform operations, maintenance, remote management, and on-site support of the web-based databas	M			
B4.8	Provide a ongoing test site that is available to all users for training purposes with data updated as needed.				

APPLICATION REQUIREMENTS

State Requirements			Vendor		
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
GENERAL SPECIFICATIONS					

A1.1	Ability to access data using open standards access protocol (please specify supported versions in the comments field).	M			
A1.2	Data is available in commonly used format over which no entity has exclusive control, with the exception of National or International standards. Data is not subject to any copyright, patent, trademark or other trade secret regulation.	M			
A1.3	Web-based compatible and in conformance with the following W3C standards: HTML5, CSS 2.1, XML 1.1	M			
APPLICATION SECURITY					
A2.1	Verify the identity or authenticate all of the system client applications before allowing use of the system to prevent access to inappropriate or confidential data or services.	M			
A2.2	Verify the identity and authenticate all of the system's human users before allowing them to use its capabilities to prevent access to inappropriate or confidential data or services.	M			
A2.3	Enforce unique user names.	M			
A2.4	Enforce complex passwords for Administrator Accounts in accordance with DoIT's statewide User Account and Password Policy.	M			
A2.5	Enforce the use of complex passwords for general users using capital letters, numbers and special characters in accordance with DoIT's statewide User Account and Password Policy.	M			
A2.6	Encrypt passwords in transmission and at rest within the database.	M			
A2.7	Establish ability to expire passwords after a definite period of time in accordance with DoIT's statewide User Account and Password Policy.	M			
A2.8	Provide the ability to limit the number of people that can grant or change authorizations.	M			

A2.9	Establish ability to enforce session timeouts during periods of inactivity.	M			
A2.10	The application shall not store authentication credentials or sensitive data in its code.	M			
A2.11	Log all attempted accesses that fail identification, authentication and authorization requirements.	M			
A2.12	The application shall log all activities to a central server to prevent parties to application transactions from denying that they have taken place.	M			
A2.13	All logs must be kept for 90 days.	M			
A2.14	The application must allow a human user to explicitly terminate a session. No remnants of the prior session should then remain.	M			
A2.15	Do not use Software and System Services for anything other than they are designed for.	M			
A2.16	The application Data shall be protected from unauthorized use when at rest.	M			
A2.17	The application shall keep any sensitive Data or communications private from unauthorized individuals and programs.	M			
A2.18	Subsequent application enhancements or upgrades shall not remove or degrade security requirements.	M			
A2.19	Utilize change management documentation and procedures.	M			
A2.20	Web Services : The service provider shall use Web services exclusively to interface with the State's data in near real time when possible.	M			

TESTING REQUIREMENTS

State Requirements			Vendor		
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**

APPLICATION SECURITY TESTING					
T1.1	All components of the Software shall be reviewed and tested to ensure they protect the State's web site and its related Data assets.	M			
T1.2	The Vendor shall be responsible for providing documentation of security testing, as appropriate. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide the necessary confidentiality, integrity and availability.	M			
T1.3	Provide evidence that supports the fact that Identification and Authentication testing has been recently accomplished; supports obtaining information about those parties attempting to log onto a system or application for security purposes and the validation of users.	M			
T1.4	Test for Access Control; supports the management of permissions for logging onto a computer or network.	M			
T1.5	Test for encryption; supports the encoding of data for security purposes, and for the ability to access the data in a decrypted format from required tools.	M			
T1.6	Test the Intrusion Detection; supports the detection of illegal entrance into a computer system.	M			
T1.7	Test the Verification feature; supports the confirmation of authority to enter a computer system, application or network.	M			
T1.8	Test the User Management feature; supports the administration of computer, application and network accounts within an organization.	M			
T1.9	Test Role/Privilege Management; supports the granting of abilities to users or groups of users of a computer, application or network.	M			

T1.10	Test Audit Trail Capture and Analysis; supports the identification and monitoring of activities within an application or system.	M			
T1.11	Test Input Validation; ensures the application is protected from buffer overflow, cross-site scripting, SQL injection, and unauthorized access of files and/or directories on the server.	M			
T.1.12	For web applications, ensure the application has been tested and hardened to prevent critical application security flaws. (At a minimum, the application shall be tested against all flaws outlined in the Open Web Application Security Project (OWASP) Top Ten (http://www.owasp.org/index.php/OWASP_Top_Ten_Project).	M			
T1.13	Provide the State with validation of 3rd party security reviews performed on the application and system environment. The review may include a combination of vulnerability scanning, penetration testing, static analysis of the source code, and expert code review (please specify proposed methodology in the comments field).	M			
T1.14	Prior to the System being moved into production, the Vendor shall provide results of all security testing to the Department of Information Technology for review and acceptance.	M			
T1.15	Vendor shall provide documented procedure for migrating application modifications from the User Acceptance Test Environment to the Production Environment.	M			
NDARD TESTING					
T2.1	The Vendor must test the software and the system using an industry standard and State approved testing methodology.	M			
T2.2	The Vendor must perform application stress testing and tuning.	M			
T2.3	The Vendor must provide documented procedure for how to sync Production with a specific testing environment.	M			
T2.4	The vendor must define and test disaster recovery procedures.	M			

HOSTING-CLOUD REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
OPERATIONS					
H1.1	Vendor shall provide an ANSI/TIA-942 Tier 3 Data Center or equivalent. A tier 3 data center requires 1) Multiple independent distribution paths serving the IT equipment, 2) All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture and 3)Concurrently maintainable site infrastructure with expected availability of 99.982%.	M			
H1.2	Vendor shall maintain a secure hosting environment providing all necessary hardware, software, and Internet bandwidth to manage the application and support users with permission based logins.	M			
H1.3	The Data Center must be physically secured – restricted access to the site to personnel with controls such as biometric, badge, and others security solutions. Policies for granting access must be in place and followed. Access shall only be granted to those with a need to perform tasks in the Data Center.	M			
H1.4	Vendor shall install and update all server patches, updates, and other utilities within 60 days of release from the manufacturer.	M			
H1.5	Vendor shall monitor System, security, and application logs.	M			
H1.6	Vendor shall manage the sharing of data resources.	M			
H1.7	Vendor shall manage daily backups, off-site data storage, and restore operations.	M			
H1.8	The Vendor shall monitor physical hardware.	M			

H1.9	Remote access shall be customized to the State's business application. In instances where the State requires access to the application or server resources not in the DMZ, the Vendor shall provide remote desktop connection to the server through secure protocols such as a Virtual Private Network (VPN).	M			
H1.10	The Vendor shall report any breach in security in conformance with State of NH RSA 359-C:20. Any person engaged in trade or commerce that is subject to RSA 358-A:3, I shall also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons shall notify the New Hampshire attorney general's office.	M			
DISASTER RECOVERY					
H2.1	Vendor shall have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems shall be architected to meet the defined recovery needs.	M			
H2.2	The disaster recovery plan shall identify appropriate methods for procuring additional hardware in the event of a component failure. In most instances, systems shall offer a level of redundancy so the loss of a drive or power supply will not be sufficient to terminate services however, these failed components will have to be replaced.	M			
H2.3	Vendor shall adhere to a defined and documented back-up schedule and procedure.	M			
H2.4	Back-up copies of data are made for the purpose of facilitating a restore of the data in the event of data loss or System failure.	M			
H2.5	Scheduled backups of all servers must be completed regularly. The minimum acceptable frequency is differential backup daily, and complete backup weekly.	M			
H2.6	Tapes or other back-up media tapes must be securely transferred from the site to another secure location to avoid complete data loss with the loss of a facility.	M			

H2.7	Data recovery – In the event that recovery back to the last backup is not sufficient to recover State Data, the Vendor shall employ the use of database logs in addition to backup media in the restoration of the database(s) to afford a much closer to real-time recovery. To do this, logs must be moved off the volume containing the database with a frequency to match the business needs.	M			
HOSTING SECURITY					
H3.1	The Vendor shall employ security measures ensure that the State's application and data is protected.	M			
H3.2	If State data is hosted on multiple servers, data exchanges between and among servers must be encrypted.	M			
H3.3	All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, shall have aggressive intrusion-detection and firewall protection.	M			
H3.4	All components of the infrastructure shall be reviewed and tested to ensure they protect the State's hardware, software, and its related data assets. Tests shall focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide confidentiality, integrity and availability.	M			
H3.5	The Vendor shall ensure its complete cooperation with the State's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.	M			
H3.6	The Vendor shall authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Vendor' hosting infrastructure and/or the application upon request.	M			
H3.7	All servers and devices must have event logging enabled. Logs must be protected with access limited to only authorized administrators. Logs shall include System, Application, Web and Database logs.	M			

H3.8	Operating Systems (OS) and Databases (DB) shall be built and hardened in accordance with guidelines set forth by CIS, NIST or NSA.	M			
H3.9	The Vendor shall notify the State's Project Manager of any security breaches within two (2) hours of the time that the Vendor learns of their occurrence.	M			
H3.10	The Vendor shall be solely liable for costs associated with any breach of State data housed at their location(s) including but not limited to notification and any damages assessed by the courts.	M			
SERVICE LEVEL AGREEMENT					
H4.1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M			
H4.2	The vendor shall maintain the hardware and Software in accordance with the specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M			
H4.3	The vendor shall repair or replace the hardware or software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M			
H4.4	All hardware and software components of the Vendor hosting infrastructure shall be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc., shall be applied within sixty (60) days of release by their respective manufacturers.				
H4.5	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 8:30am to 5:00pm- Monday through Friday EST.	M			

H4.6	The Vendor shall conform to the specific deficiency class as described: o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.	M			
H4.7	As part of the maintenance agreement, ongoing support issues shall be responded to according to the following: a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies –The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract.	M			

H4.8	The hosting server for the State shall be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	M			
H4.9	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M			
H4.10	If The Vendor is unable to meet the uptime requirement, The Vendor shall credit State's account in an amount based upon the following formula: (Total Contract Item Price/365) x Number of Days Contract Item Not Provided. The State must request this credit in writing.	M			
H4.11	The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M			
H4.12	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M			
H4.13	The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: Server up-time; All change requests implemented, including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M			
H4.14	The Vendor will give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M			

SUPPORT & MAINTENANCE REQUIREMENTS

State Requirements			Vendor		
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
SUPPORT & MAINTENANCE REQUIREMENTS					

S1.1	The Vendor's System support and maintenance shall commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M			
S1.2	Maintain the hardware and Software in accordance with the Specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M			
S1.3	Repair Software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M			
S1.4	The State shall have unlimited access, via phone or Email, to the Vendor technical support staff between the hours of 8:30am to 5:00pm- Monday through Friday EST.	M			
S1.5	The Vendor response time for support shall conform to the specific deficiency class as described below or as agreed to by the parties: o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.	M			

S1.6	The Vendor shall make available to the State the latest program updates, general maintenance releases, selected functionality releases, patches, and Documentation that are generally offered to its customers, at no additional cost.	M			
S1.7	For all maintenance Services calls, The Vendor shall ensure the following information will be collected and maintained: 1) nature of the Deficiency; 2) current status of the Deficiency; 3) action plans, dates, and times; 4) expected and actual completion time; 5) Deficiency resolution information, 6) Resolved by, 7) Identifying number i.e. work order number, 8) Issue identified by;	P			
S1.8	The Vendor must work with the State to identify and troubleshoot potentially large-scale System failures or Deficiencies by collecting the following information: 1) mean time between reported Deficiencies with the Software; 2) diagnosis of the root cause of the problem; and 3) identification of repeat calls or repeat Software problems.	P			
S1.9	As part of the Software maintenance agreement, ongoing software maintenance and support issues, shall be responded to according to the following or as agreed to by the parties: a. Class A Deficiencies - The Vendor shall have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies –The State shall notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor shall repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract; or as agreed between the parties.	M			

S1.10	The Vendor shall use a change management policy for notification and tracking of change requests as well as critical outages.	M			
S1.11	A critical outage will be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M			
S1.12	The Vendor shall maintain a record of the activities related to repair or maintenance activities performed for the State and shall report quarterly on the following: All change requests implemented; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M			
S1.13	A regularly scheduled maintenance window shall be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M			
S1.14	The Vendor shall give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M			
S1.15	The State shall provide the Vendor with a personal secure FTP site to be used by the State for uploading and downloading files if applicable.	M			
PROJECT MANAGEMENT					
State Requirements			**Vendor**		
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
PROJECT MANAGEMENT					
P1.1	Vendor shall participate in an initial kick-off meeting to initiate the Project.	M			
P1.2	Vendor shall provide Project Staff as specified in the RFP.	M			

P1.3	Vendor shall submit a finalized Work Plan within ten (10) days after Contract award and approval by Governor and Council. The Work Plan shall include, without limitation, a detailed description of the Schedule, tasks, Deliverables, milestones/critical events, task dependencies, and payment Schedule. The plan shall be updated no less than <every two weeks.>	M			
P1.4	Vendor shall provide detailed <bi-weekly or monthly> status reports on the progress of the Project, which will include expenses incurred year to date.	M			
P1.5	All user, technical, and System Documentation as well as Project Schedules, plans, status reports, and correspondence must be maintained as project documentation. (Define how- WORD format- on-Line, in a common library or on paper).	M			

ACTIVITY / DELIVERABLES / MILESTONES PRICING WORKSHEET				
ACTIVITY, DELIVERABLE, OR MILESTONE		**DELIVERABLE TYPE**	**PROJECTED DELIVERY DATE**	**MILESTONE PAYMENT**
PLANNING AND PROJECT MANAGEMENT				
1	Conduct Project Kickoff Meeting	Non-Software		
2	Work Plan	Written		
3	Project Status Reports	Written		
4	Infrastructure Plan, including Desktop and Network Configuration Requirements	Written		
5	Security Plan	Written		
6	Communications and Change Management Plan	Written		
7	Software Configuration Plan	Written		
8	Systems Interface Plan and Design/Capability	Written		
9	Testing Plan	Written		
10	Data Conversion Plan and Design	Written		
11	Deployment Plan	Written		
12	Comprehensive Training Plan and Curriculum	Written		
13	End User Support Plan	Written		
14	Business Continuity Plan	Written		
15	Documentation of Operational Procedures	Written		
INSTALLATION				
16	Provide Software Licenses (if needed)	Written		
17	Provide Fully Tested Data Conversion Software	Software		
18	Provide Software Installed, Configured, and Operational to Satisfy State Requirements	Software		
TESTING				
19	Conduct Integration Testing	Non-Software		
20	Conduct User Acceptance Testing	Non-Software		
21	Perform Production Tests	Non-Software		
22	Test In-Bound and Out-Bound Interfaces	Software		
23	Conduct System Performance (Load/Stress) Testing	Non-Software		
24	Certification of 3rd Party Pen Testing and Application Vulnerability Scanning.	Non-Software		
SYSTEM DEPLOYMENT				
25	Converted Data Loaded into Production Environment	Software		
26	Provide Tools for Backup and Recovery of all Applications and Data	Software		
27	Conduct Training	Non-Software		

28	Cutover to New Software	Non-Software		
29	Provide Documentation	Written		
30	Execute Security Plan	Non-Software		
OPERATIONS				
31	Ongoing Hosting Support	Non-Software		
32	Ongoing Support & Maintenance	Software		
33	Conduct Project Exit Meeting	Non-Software		
			TOTAL COST	