ADDENDUM #4

On October 16, 2018, the New Hampshire Department of Health and Human Services published a Request for Proposals, requesting proposals from vendors who are qualified to provide a software system and associated services for the Department to implement a scalable Opioid Crisis Response Management Business Intelligence dashboard.

The Department is publishing this addendum to:

1. **Add Attachment C-2 to the Request for Proposals:**

Vendor Instructions

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 usefullness 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 usefull or potentially usefull 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.

BUSINESS REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
Functional					
B1.1					
B1.2	Design and implementation of data visualization standards via a style guide and example templates specifically leveraging existing toolsets and web portals currently in place at the state to create a consistent way for data to be organized and graphically displayed to meet both user design and user experience requirements.				
B1.3	Create a method to inventory data sources assoicated with the building of the Opioid Crisis dashboard and an ongoing process to add to the inventory of the system and recommend a strategy for future use of data analytics and business intelligence toolsets as well as create a dashboard in which the source is tagged as internal or external (to the Department) and whether the data contains personally identified information (PII) or De-identified information (DII)				
B1.4	Provide professional services to augment internal capabilities associated with the following skill sets: Business analysis, use case development, user persona development, Data and statistical analysis generally, Data and statistical analysis specific to the opioid crisis, Data integration and transformation, Data visualization including geographical information system, Hardware architecture and design, Software configuration and training.				
B1.5	If the proposal is a cloud/hosted solution provide and establish hardware and software and/or cloud services for operation by the State needed to augment the Department's infrastructure.				
B1.6	Implement no later than August 15, 2019 opioid dashboards based on requirements				
B1.7	Provide a detailed description of how you would address charts included in the Introduction section				

B1.8	Provide context sensitive "Help" screens/tips and dashboard instructions				
B1.9	Automated reports/notifications/alerts to users based on subscription or opt in/out functionality				
B1.10	Design, develop and implement a holistic Data Analytics Platform (DAP) that consolidates data from multiple, currently disparate Department, other State of New Hampshire and Federal sources, systems and formats to meet the needs of the state's opioid response and provide the foundation for all other needs of the Department programs.				
B2.1	Include support for the future use of advanced statistical analysis techniques, predictive analytics and machine learning				
B2.2	Be intuitive and easy to learn, understand, navigate and use,				
B2.3	Provide and support average less than 5 seconds with a majority of 1 second query response times, with or without user customization,				
B2.4	Process and load datasets in a fast, smooth, efficient manner to meet no older 24 hour stale data				

B2.5	The selected vendor must leverage (where applicable for the vendor solution) current technologies in place at State of New Hampshire and provide recommendations for alternatives based on proposed strategy to include but not limited to: Oracle databases, Dimensionally modeled data marts, Extract, Transform, Load (ETL) software - Informatica, Statistical analysis tools/software and server - R Programming and RStudio Server/Connect, and Supplementary BI tools leveraging Tableau for dashboards which: Consolidate and arranges numbers, metrics and Department defined scorecards, Key Performance, and other, metrics, Can be tailored for specific roles and display metrics targeted for a single point of view, Includes a customizable interface, Includes the ability to pull real-time data				
B2.6	Design, develop and implement an overarching data model, which: Combines appropriate data elements from various sources, as needed to achieve reporting and alert functions, Includes interfaces, source mapping and user interfaces; required to achieve data consolidation and build the DAP, Identifies current and future state of source systems and processes, Possesses the processing capabilities to provide large dataset analysis, including highly complex numerical analysis of textual, structured, non-structured, spatial and other data sources, Provide metadata tagging of data sources/elements, Allows fast and flexible data integration so that data sources are able to be integrated in the analytical environment and analyzed with limited advanced notice.				

B2.7	Vendors must include a proposed architecture for the DAP, which integrates data from source systems and meets, or exceeds, the following minimal requirements:				
B2.8	Provides a framework for organization of data, information management and technology systems required to build and implement the system,				
B2.9	Allows for data components of the architecture to include internal and external sources of structured and unstructured data users require to analyze the opioid crisis,				
B2.10	Includes data integration, data cleansing and the development and implementation of data dimensional rules,				
Technical					
B3.1	Describes the conceptual and logical technology components required to present information to users and enable them to analyze the data and its impacts,				
B3.2	Allows for the ability to drill down on report data by varying levels of geographic, provider, program, service and client demographic details				
B3.3	Allow for the extraction of patterns and knowledge from large amounts of data,				
B3.4	Provide predictive or statistical analysis model, based upon data type and attributes				
B3.5	Provides browser-based solution to support all major browsers.				
B3.6	Internal multi-tenant sandbox to provide statistical analysis areas to look at data with access to the dimensional based data to design and develop visualizations on an ad-doc development based methodology				
B3.7	Internal role based authentication to provide view, modify and delete as well as external facing role based solution with ability to define group or user defined access				
B3.8	Provide a methodology to track web traffic and report on number of viewers, number of this and/or other measures.				
B3.9	State Sizing and Growth Assumptions				

B3.10	Develop capacity to make data and information available in meeting the Department's Federal Reporting requirements and necessary for Federal grant applications				
SUBHEAD					
B4.1	The new System must accommodate the anticipated number of users and workstations at each location. In order to support initial sizing expectations, prior to completion of capacity planning as part of this project, the State has estimated the first phase system must accommodate approximately 2,000 internal users (25% active users, 5% concurrent) in and for future use, 250,000 external users (10% active users, 2% concurrent) at this time, and all of these users are expected to have a workstation that will access the System. These initial estimates will be replaced with the finale user sizing in the Capacity Plan deliverable as part of the design phase. Workstations, network, servers, storage and WAN connectivity will be recommended by the vendor to ensure sizing to access and utilize the system.				
B4.2	The new shared infrastructure and functional capabilities need be designed to be operational 24 hours per day (hours to be determined by the state), 7 days per week, and 52 weeks per year. The centralized servers and resources and public facing web site will be designed to be operational 7 days per week and 24 hours per day. No single disruption is anticipated to last longer than 8 hours. The System as a whole will be available for use 99 percent of the timeless mutually agreed and scheduled service/maintenance intervals.				
B4.3	The new System must support transparent failover capabilities using high-availability architectural elements.				
B4.4	Specify all equipment (if any) required for the development and operations of the solutions and requirements defined in this RFP. The equipment will be comprised of industry standard and readily available components.				
B4.5	Creating/viewing population-based or individual-based alerts and notifications				
B4.6	Subscribing/Un-subscribing to alerts/notifications of interest				
B4.7	Sending notifications through preferred notification method				

B4.8	Scheduling of distribution of reports and notifications based on user input via an "opt in" model				
B4.9	Describe the proposed solution to meet 508 compliance and DoIT compliance requirements. The authentication and authorization solution must be ADA compliant.				
B4.10	Determining who originates and approves DAP investment proposals.				
B4.11	Determining the approved technologies and products developers must use to build services.				
B4.12	Defining the procedure for requesting permission to use a service.				
B4.13	Identifying (and executing) what service and system testing is required before deploying a service enhancement.				
B4.14	Promulgate policies, standards, and guidelines				
B4.15	Facilitation of processes				
B4.16	Collection, analysis and visualization of metrics				
B4.17	Administer the integration metadata - for example, DAP metadata (such as Web Services Description Language) or business-to-business metadata (such as electronic data interchange/XML document standards).				
B4.18	Monitor the associated governance procedures, through one or more repositories.				
B4.19	Role-based Access and User Provisioning - Technology component that enables what information a particular user is authorized to access.				
B4.20	Users' access rights shall be based on what roles they play in the enterprise (State and Counties) and/or what groups they belong to for external entities.				
B4.21	Role-Based Access shall include the capability to enforce who can update data versus access and view only. Further, the update authority should be defined at the field level within a panel.				

B4.22	Authentication of user identities - Technology component that verifies the identities of those seeking to access client data. Shall include strong authentication supported by an appropriate infrastructure for identity and access management.				
B4.23	The solution must have a mechanism for Annual Reconciliation of users to determine if access is still needed.				
B4.24	Configure, install and train on the existing Tableau environment to allow for the usage of R Programming				
B4.25	Logging of activity - For financial, operational, and legal reasons, the solution must record all activities in a log, which must be searchable to allow administrators to identify any abnormal pattern of activity.				
B4.26	The solution must include the capability to monitor activity continually according to a set of pre-defined rules, and to notify administrators when abnormal activity is detected				
B4.27	Authorization - Authorization shall provide access control through enforcement, and be used to determine the specific scope of access to grant to an identity. It must provide real-time access policy decisions and enforcement (based on identities, attributes, roles, rules, entitlements and so on). Users must be able to access only what their job functions allow them to access. For instance, if a person is a "manager," then he or she is granted the access necessary to create or edit a performance review; however, if a person is not a manager, then he or she should be able to review only his or her own performance review, and only at a specific stage of the review cycle. Web access management (WAM), externalized authorization management, identity-aware networks and digital rights management tools are examples of authorization technologies.				

B4.28	Administration - Administration shall offer a means of performing identity-related tasks (for instance, adding a user account to a specific system). Administration tools must provide an automated means of performing identity-related work that would otherwise be performed by a human; examples include tasks such as creating, updating or deleting identities (including credentials and attributes), and administering access policies (rules and entitlements). User provisioning shall be considered a part of administration technology. Helpdesk agents shall have override capabilities to correct data and account errors.				
B4.29	Establishment of an agile State enterprise technology platform based on an DAP architecture				
B4.30	The selected vendor must work with Department to ensure strategic alignment between the deployed technology and the future-state business processes and operational model. This collaboration is to occur, at a minimum, through the following activities:				
B4.31	Work with Department Executive Leadership and OIS to refine the overall vision for the project and to develop a strategic plan for managing change;				
B4.32	Cultivate ownership and teamwork among stakeholders at executive levels				
B4.33	Define a change control process for considering and accepting or denying changes (policy, planning, design, processes, etc.) throughout the project				
Training					
	Work with the Department to develop and deliver training as appropriate to State users				

	The System training, in addition to focusing on the navigation and use of the System, must also focus on how the System is integrated into the day-to-day work of end users including access level, new business processes and/or workflows that the System will support. Additionally, training for the usage of the back-end environment, informatica and database dimensional design will be provided to a team consisting of State of New Hamshire database administrators, system administrators and business analysts responsible for the on-going maintenance and support of the system (outlined further in the Technical training section).				
	The selected vendor must provide the State Project Manager with documented evidence of each trainee's competence to operate the System and integrate its support in to their day-to-day work. Training must be of sufficient length to ensure adequate comprehension. Training must be provided "just in time" prior to deployment and must comprehensively address all System operations as well as security considerations.				
	The selected vendor must organize and provide formal orientation and training before System deployment, to the State development and operations staff so that they are enabled to manage and maintain the System.				
	The Contractor will also involve the State's technical staff in any enhancements to the System to enable the staff to become familiar with the process.				

	Effective training that will provide the required skills to use this new automated tool is critical to the successful implementation and use of the new System. The selected vendor must develop user training curricula, schedules, training materials and training evaluation materials. The selected vendor must maintain an online training environment that allows trainees to access the new System. The selected vendor must conduct face-to-face, hands-on, user training in logical groupings at regional locations determined by the State, and for managing all training planning and logistics.				
Inventory and Migration					
	The selected vendor shall develop a prioritized list of data sources to integrate and migrate into the Enterprise Data Warehouse. The selected vendor must identify and prioritize data sources required to support each implementation phase. Additionally, the selected vendor is required to integrate each respective data source into the Enterprise Data Warehouse. The following are the initial list of data sources to be migrated into the EDV and utilized to create the Opioid Crisis dashboard:				
	Medicaid and Comprehensive Health Care Information System (CHIS): Pharmacy, physical, behavioral health care claims for all NH Medicaid services and for most commercially insured population in New Hampshire. Medicaid member data will be integrated into the EBI warehouse under a separate effort by Spring 2019.)				
	Child protection investigations and findings including whether opioid or other substance use is possible factor in the case. Child Welfare System/DCYF Cases				

	Automated Hospital Emergency Department Data (AHEDD): State-wide surveillance system collects real-time data from all 26 New Hampshire acute care hospital emergency departments to detect clusters or monitor potential health threats in the population such as respiratory illness during influenza season, injuries during snow storms, and drug overdoses during the current opioid crisis.)				
	Vital Records Data: Real time birth and mortality records certificates. Data collected by the NH Division of Vital Records for NH residents and births or deaths occurring in NH. NH resident out-of-state births are reported to NH through an interstate exchange agreement.				
	Drug overdose deaths data by Fentanyl (no other drugs), Fentanyl and Other Drugs (excluding heroin), Heroin (no other drugs), Heroin and Other Drugs (excluding fentanyl), Heroin and Fentanyl, Unknown Opioids, Other Opiates/Opioids determined by the Medical Examiner.Medical Examiner Report				
	Emergency Medical Services (EMS) Trauma Emergency Medical Services Information System (TEMSIS): medical responses on Naloxone administration incidents data. A data collection and analysis capability system that provides for the evaluation of the emergency medical and trauma services system (TEMSIS).				
	Grant/State BDAS Treatment Services: Medication assisted treatment with Opioid/opiate, methamphetamine, & cocaine/crack admissions to state funded facilities. An array of levels of care including outpatient, intensive outpatient, partial hospitalization, residential, withdrawal management, and peer and non-peer recovery support services.				
	Population Data: Base data used for calculation of population based rates.				

	NH Health WISDOM: Data access for public health indicators via interactive dashboards and community profiles. Customize and display data in maps, graphs, and tables related to the NH State Health Improvement Plan, NH Environmental Public Health Tracking Program, and the NH Occupational Health Surveillance Program.				
	To help ensure that the selected vendor and the State Project team fully understand the extent of the work needed for data conversion, a detailed study of conversion issues and requirements will be required of the selected vendor.				
	Conducting selected data source analysis to determine conversion requirements				
	Reviewing conversion analysis with the State Project team, prepare detailed data conversion plan (addressing manual and electronic data)				
	Defining strategies for verifying and/or correcting existing data				
	Developing data conversion scripts and test data conversion scripts				
	In this task the selected vendor must address data migration issues and a plan must be in place to ensure the validation of all conversion routines and the accuracy and completeness of all data.				
Data Governance					
	Design and Implementation of a data governance strategy				
	A DAP initiative requires an infrastructure reference model that provides guidance for selecting technologies and products when implementing and deploying services. The Vendor must design and implement a DAP governance system that addresses the following requirements (at a minimum):				
	Defining methods to ensure that the services infrastructure supports robust, secure, scalable, and interoperable operations.				
	Identifying what are the approved or standard technologies and products for service development and deployment.				

	Designing and implementing methods, patterns, and technologies that will be used to support security, reliability, transaction, and instrumentation requirements.				
	Determining who determines which technologies and products go onto the standards list.				
	Defining who needs to approve future technology and product decisions as standards evolve in the future.				
	Service Design and Development				
	Service design and development precepts delegate decisions about services to the appropriate architects and developers. The Vendor must design and implement a DAP governance system that addresses the following requirements (at a minimum):				
	Defining a method(ology) to ensure that services are built the right way.				
	Determining the appropriate types of models that must be implemented.				
	Identifying sign off or approval requirements for service models.				
	Determining the design patterns that should be used to support DAP principles.				
	Identifying sign off or approval requirements system or service design decisions.				
	Establishing technology standards for a future project.				
	Determining technology selection sign off or approval requirements.				
	Establishing standard designs for message formats.				
	Determining interface sign off or approval procedures.				
	Defining the required testing for DAP projects.				
	Establishing completed project acceptance requirements and procedures.				
	Creating a "prototyping or early experience" capability to experiment with and design enhancements to rules-engines by the program group for review and approval prior to entering a more formal development, testing and release process.				

	Configuration and release management				
	Configuration management precepts establish which developers or administrators are responsible for configuring a service and preparing it for production deployment. The Vendor must build on and extend New Hampshire's release management processes, or develop one if the existing process is mutually determined to be not suitable. Requirements in this area are to include the following:				
	Establishing objective criterion to ensure that services are stable upon production release.				
	Defining entire deployable units including its dependencies.				
	Defining who is responsible for creating and version managing configuration files and deployment packages.				
	Establishing clear responsibilities and requirements for system testing, performance testing, and capacity planning.				
	Defining the service staging and promotion process.				
	Defining and implementing services registration procedures.				
	Defining what information must be captured pertaining to a service.				
	Defining service provision and instrumentation requirements.				
	Establishing signs off or approvals required to migrate a service into production.				
	Contract management				
	Contract management precepts shall define the policies and processes that potential service consumers use to obtain permission to access a service. The proposed DAP governance solution may extend the existing provisioning governance system if suitable, or build a new one as appropriate. The Vendor must design and implement precepts in the following areas:				
	Ensuring that new consumers don't crash the system through use, operation or load.				
	Establishing the procedures for requesting permission to use a service.				

	Identifying required information to request permission to use a service.				
	Establishing an impact analysis to be performed before granting permission to new consumers.				
	Determining appropriate sign offs or approvals to granting permissions to access the system.				
	Establishing a framework to negotiate service level agreements (SLAs) for use of the system.				
	Defining and implementing SLAs be reported and enforced.				
	Establishing processes to address modifications or additional resources that may be required to support the SLAs.				
	Defining appropriate testing practices and procedures that are required before a new consumer can be provisioned.				
	Establishing a process to provision new consumers				
	Service monitoring and control				
	Service monitoring and control precepts must be designed and implemented in such a manner as to define responsibilities for issues related to operating a service. The Vendor may build on and extend or develop new service management and operations governance by defining and implementing precepts that address the following:				
	Establishing controls and reporting to ensure that services behave as expected.				
	Defining instrumentation and reporting to track service consumption and utilization.				
	Establishing methods and reporting procedures to detect, eliminate and prevent against unauthorized service access.				
	Create tracking and reporting for service SLA compliance and violations.				
	Identification of notifications and escalation contacts and procedures for service issues and outages				
	Service monitoring and control capabilities must be built into the DAP runtime infrastructure. DAP governance standards must define where and how to use, report on and enhance SLAs.				
	Incident management				

	Incident management precepts shall define and implement responsibilities for monitoring and managing problems and issues that arise during the operation of the service. The Vendor must build on and extend or develop new incident management governance by implementing precepts that cover the following (at a minimum):				
	Design and implementation of processes and procedures to manage incidents and failures				
	Definition/Identification of responsibilities for end-to-end service exception and fault tracking				
	Definition/Identification of responsibilities for end-to-end service error identification and resolution.				
	Definition of the escalation path for SLA violations.				
	Change management				
	Change control management precepts shall define and implement responsibilities for managing system enhancement requests and service versioning. The Vendor must build on and extend or develop and implement new change management governance by defining precepts that cover (at a minimum):				
	Implement a process to manage change requests and to ensure that enhancements don't introduce defects in the system.				
	Design and implement procedures for requesting service enhancements.				
	Define what information is required when requesting a service enhancement.				
	Design an impact analysis process to be performed before a service enhancement request is accepted.				
	Define sign off or approval requirements for service enhancement requests.				
	Define roles, responsibilities and sequence of events pertaining to the implementation of an enhancement.				
	Develop guidelines to assist the State in paying for or funding an enhancement.				

	Define recommended methods and a process for addressing enhancement requests associated with regulatory requirements.				
	Define methods to enable service versioning and version control/migration.				
	Establish guidelines on how long should a previous version(s) of the service be maintained and subsequently retired.				
	Define what degree of service and system testing is required before deploying a service enhancement.				
	Establish leading practices to mitigate current consumer disruption when deploying an enhancement.				
	Develop procedures to notify consumers of the enhancement or changes to the system.				
	Develop and implement processes to fall back to a system previous version upon discovery of a critical defect.				
	Data Management				
	Design and Implementation of a data management strategy including data warehousing, data quality, and data integration capabilities. The strategy will incorporate current practices and the vendor will work with the current teams.				

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 for internal facing solution	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			

Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
A2.13	All logs must be kept for (6 **months**)	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		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			

TESTING					
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			
STANDARD 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 and how the system will meet all Federal and State requirements currently in law and rules protecting sensitive personal health information, as outlined in the Health Insurance Portability and Accountability Act (HIPAA) and the more stringent Title 42 Code of Federal Regulations (CFR) Part 2: (Confidentiality of Substance Use Disorder Patient Records regulation), as outlined by the Federal Substance Abuse Mental Health Services Administration (SAMHSA) and the Office of the National Coordinator for Health Information Technology (ONC)	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 hardend 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			
H3.11	The cloud services if used will be FEDRAMP compliant	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			

Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
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			

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, 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			
P1.6	The selected vendor must define an integrated project management plan, which;				
P1.7	Includes cost estimates for specific work to be performed,				
P1.8	Defines Department Training as a component of the implementation plan,				
P1.9	Clearly defines the approach and methodology to be used in each phase of the project,				
P1.10	Includes a discovery, detailed requirements and prioritization component phase of the project,				

P1.11	The Department has historically followed a waterfall approach to enacting changes. This is usually accomplished by having requirements meetings, followed by vendor design based on the requirements, with a development, unit test, integration test, system test and regression testing. Finally ending up with a migration to production and training and post-production review. With this RFP the goal will be to adjust to a more agile approach, allowing the organization to adapt and change as needed more efficiently and effectively in order to meet the business needs. The goals will be to provide a bi-weekly demonstration of work for review and planning for next steps. The new process will be based on the following scope as a baseline to the strategy:				
P1.12	Team Formation: the Department in concert with the awarded vendor will identify the required team members for the duration of the product delivery. The team will consist of a product owner, scrum master, and other team members. There will be several teams based on the amount of features being worked on at any given time. Additionally, there will be operational teams to commit to and complete features associated with user stories and tasks to keep the system running as well as product enhancement teams to commit and complete features associated with user stories and tasks to meet the changes required by the business.				
P1.13	Process: The awarded vendor will plan and implement a process similar to the following:				
P1.14	Backlog Creation and refinement: The Product Owner working with team members and the business will create a prioritized backlog of work in the form of high level features. This will be an on-going process that must be completed prior to each Sprint Planning Meeting. Additionally, the Product Owner(s) will breakdown the features into prioritized user stories related to the originating features for use in the Sprint Planning meeting.				

P1.15	Sprint Planning Meeting: This meeting will minimally consist of all team members facilitated by the Scrum Master and will be focused on clarifying the details of the prioritized backlog items, re-prioritizing as needed and obtaining commitment from the team to complete user stories from the backlog in the proposed sprint not to exceed 4 weeks with a preferred cadence of 2 weeks. Additionally the team will then create detailed tasks and commit to the items individually. The commitments will be managed using a KanBan tool to be provided by the vendor and agreed to by both parties for the teams use throughout the contract period.				
P1.16	Sprint: The sprint will consist of daily standup meetings (not to exceed 10 minutes) to discuss roadblocks, any clarification needs associated with work accomplished the previous day or planned for the current day, or other important items to the team. The team will work in concert with each other preferably within the same location and will require a meeting room provided by the awarded vendor for impromptu meetings to move tasks forward.				
P1.17	Sprint Review Meeting: Demonstrate working product associated with commitments from the sprint planning meeting. Communicate items to focus on in the next sprint.				
P1.18	Daily Meeting: Consist of the team members that have committed to completing tasks in the sprint and will be no longer than 10 minutes answering the following questions:				
P1.19	What did I complete yesterday?				
P1.20	What am I doing today?				
P1.21	Are there any roadblocks keeping me from completing my commitments?				
	Develop and obtain buy-in for a stakeholder and communication management plan and work with the Department to craft appropriate communication messages throughout the project				

Conduct organizational assessments and gap analyses for the affected divisions and programs and facilitate the development of appropriate organizational structures and job descriptions
Work with the Department to define business processes, including use cases, workflows, and business rules

The project must utilize agile-like software development principles and practices

Will not meet
Will partially meet
Wholly meet