APPLICATION REQUIREMENTS				
State Requirements				
Req #	**Requirement Description**	**Criticality**	**Response**	**Example Response**
GENERAL SPECIFICATIONS				
A1.1	Ability to access data using open standards access protocol.	M		The solution being proposed will use a commercial off the shelf (COTS) software that utilizes XML, HTML and SQL all of which leverage open standards to allow for interoperability and continued quality.
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		As represented in A1.1 by utilizing open standards our solution is compliant with this requirement.
A1.3	Web-based compatible and in conformance with the following W3C standards: HTML5, CSS 2.1, XML 1.1	M		The web based component of this solution conforms to w3c standards in our case specifically leveraging HTML5, XML and SOAP
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		Utilizing our COTS solution will require the user to validate their identify through a user name and password provided after information is obtained to create the users account.
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		Based on the role based access controls within the COTS solution we will ensure the users have access only to the data that the State authorizes.
A2.3	Enforce unique user names.	M		The COTS solution combined with our logical access procedure to create user accounts ensures the unique user name.
A2.4	Comply with the Department's Password Standard and DoIT's statewide User Account and Password Policy when developing, establishing, and enforcing system Administrative (privileged) and End User (non-privileged) accounts. Should a requirement conflict reside between the two documents the more restrictive requirement must be followed.	M		The COTS solution will comply with the requirements as listed in the Department's Password Standard and NH DoIT's Password Policy.
A2.8	Provide the ability to limit the number of people that can grant or change authorizations.	M		Based on State approval the system will allow for up to 3 administrators to support granting or changing permissions.
A2.10	The application shall not store authentication credentials or sensitive data in its code.	M		All authentication credentials are encrypted utilizing the Advanced Encryption Standard (AES)
A2.11	Log all attempted accesses that fail identification, authentication and authorization requirements.	M		The system in compliance with failed attempt policy automatically logs all failed attempts to result in a lockout. See A2.4

A2.13	All logs must be kept for one (1) year, unless protected health information is entered into/stored in the system or product, then all audit logs must be kept for six (6) years for HIPPA compliance.	M		The COTS solution will maintain logs for 1 years
A2.14	The application must allow a human user to explicitly terminate a session. No remnants of the prior session should then remain.	M		The COTS solution allows for the termination of the user account which will result in the termination of access.
A2.15	Do not use Software and System Services for anything other than they are designed for.	M		The solution will be implemented at the direction of the department to meet the requirements of the contract.
A2.16	The application Data shall be protected from unauthorized use when at rest.	M		The COTS solution will encrypt data in transit and at rest coupled with role based access permissions the application data will be protected at rest
A2.17	The application shall keep any sensitive Data or communications private from unauthorized individuals and programs.	M		See A2.16
A2.18	Subsequent application enhancements or upgrades shall not remove or degrade security requirements.	M		The COTS solution and subsequent upgrades will maintain or enhance security requirements in partnership and communication with the State.
A2.19	Utilize change management documentation and procedures.	M		The COTS solution will follow industry best practices for change management and the configuration administrators will document all changes made to production after final user acceptance of the changes.
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		The COTS solution will not utilize web services to interface with the State's data systems; however the solution will be able to export the information into CSV, Excel or similar functions and provide the information to the State for ingestion.
A2.21	Logs must be configured using "fail-safe" configuration. Audit logs must contain the following minimum information: 1. User lDs (of all users who have access to the system) 2. Date and time stamps 3. Changes made to system configurations 4. Addition of new users 5. New users level of access 6. Files accessed (including users) 7. Access to systems, applications and data 8. Access trail to systems and applications (successful and unsuccessful attempts) 9. Security events	M		The COTS solution will be able to maintain the following information either in a log or separate documentation: 1. User lDs (of all users who have access to the system) 2. Date and time stamps 3. Changes made to system configurations 4. Addition of new users 5. New users level of access 6. Files accessed (including users) 7. Access to systems, applications and data 8. Access trail to systems and applications (successful and unsuccessful attempts) 9. Security events

TESTING REQUIREMENTS				
State Requirements				
Req #	**Requirement Description**	**Criticality**	**Response**	**Example Response**
APPLICATION SECURITY TESTING				
T1.1	All components of the Software shall be reviewed and tested to ensure they protect the Department and State's web site and its related Data assets.	M		As this is a COTS solution the components of the software that will be reviewed and tested will focus on the configuration of the system to meet the business and technical requirements of the solution.
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		The COTS solution has published documentation to address the technical, administrative and physical security controls available upon request.
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		This is addressed via logs associated with login attempts
T1.4	Test for Access Control; supports the management of permissions for logging onto a computer or network.	M		See A2.4
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		See A2.4 and A2.16
T1.6	Test the Intrusion Detection; supports the detection of illegal entrance into a computer system.	M		See T1.2
T1.8	Test the User Management feature; supports the administration of computer, application and network accounts within an organization.	M		See A2.4, this process is tested each time an account is activated or de-activated
T1.9	Test Role/Privilege Management; supports the granting of abilities to users or groups of users of a computer, application or network.	M		This will be accomplished after final configuration and account creation has been completed and validated by the department
T1.10	Test Audit Trail Capture and Analysis; supports the identification and monitoring of activities within an application or system.	M		The COTS solution has an internal testing plan for ensuring the audit trail logs are in place.
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		The COTS solution has an internal testing plan and is covered contractually to protect against the items listed

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		The COTS solution has an internal testing plan for ensuring the audit trail logs are in place.
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		The 3rd party scans can be provided upon request. These reports are a sub-contract component with the COTS solution being employed on this solution.
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		As the COTS solution maintains FedRamp Moderate certification all testing was completed in order to maintain compliance. It is anticipated that testing of the configuration will be accomplished prior to production use.
T1.15	Vendor shall provide documented procedure for migrating application modifications from the User Acceptance Test Environment to the Production Environment.	M		All configurations will be accomplished in a single environment and approved to be implemented on demand. No migration will be performed for this COTS solution.
STANDARD TESTING				
T2.1	The Vendor must test the software and the system using an industry standard and State approved testing methodology.	M		See T1.14
T2.2	The Vendor must perform application stress testing and tuning.	M		See T1.14
T2.3	The Vendor must provide documented procedure for how to sync Production with a specific testing environment.	M		See T1.14
T2.4	The vendor must define and test disaster recovery procedures.	M		See T1.14

HOSTING-CLOUD REQUIREMENTS

State Requirements

Req #	Requirement Description	Criticality	Response	Example Response
			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		See T1.14
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		See T1.14
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		See T1.14
H1.4	Vendor shall install and update all server patches, updates, and other utilities within 60 days of release from the manufacturer.	M		See T1.14
H1.5	Vendor shall monitor System, security, and application logs.	M		See T1.14
H1.6	Vendor shall manage the sharing of data resources.	M		See T1.14
H1.7	Vendor shall manage daily backups, off-site data storage, and restore operations.	M		Daily backups will be performed nightly per sub-contract with COTS solution
H1.8	The Vendor shall monitor physical hardware.	M		See T1.14
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		The COTS solution will be a cloud based solution accessible based on the role based access permissions configured as part of the project based on the State's requirements.
			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		See T1.14
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		See T1.14

H2.3	Vendor shall adhere to a defined and documented back-up schedule and procedure.	M		See H1.7
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		See H1.7
H2.5	Scheduled backups of all servers must be completed regularly. The minimum acceptable frequency is differential backup daily, and complete backup weekly.	M		See H1.7
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		See H1.7
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		All data recovery is managed via the backup and restore process
	HOSTING SECURITY			
H3.2	If State data is hosted on multiple servers, data exchanges between and among servers must be encrypted.	M		All data is encrypted and at rest regardless of number of servers.
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		All security controls are tested and addressed via the item T1.14
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		All security controls are tested and addressed via the item T1.14
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		All security controls are tested and addressed via the item T1.14
	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		The COTS solution will be maintained, operated and supported per the contract terms.
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		The COTS configuration may be changed as needed to meet the State's requirements.

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		Since the solution is dependent upon the COTS solution proposed any replacement of the software would require a change order and amendment to the contract.
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.	M		This will follow the COTS solutions roadmaps for patches in alignment with item T1.14
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		The proposal will include technical support for the State between 8:30am and 5:00pm EST Monday through Friday.
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		The proposed solution will be a COTS solution and thus the solution will be able to comply with the following: Class A Deficiency - system is not available or is not performing the function agreed upon during production go live Class B Deficiency - COTS configuration issue with a workaround not impacting system utilization, but requires attention to resolve manual workaround. Class C Deficiency - COTS configuration that has minimum impact on the function. Would be de prioritized to complete remediation on Class B and Class A deficiencies.
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		The proposed solution will be able to provide response times as described herein.

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		The COTS solution will be available 24 hours a day and 7 days a week; however support will be available as described in H4.5
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		The COTS solution has full failover functionality allowing for maintenance to occur without impact to the business functionality.
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		Agreed for any uptime requirement not met for the COTS solution included in the proposal.
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		The COTS solution will not be able to provide the details identified herein. The proposed solution will be able upon request to provide documentation surrounding configurations changes that were completed in production through the change management process, see A2.19.
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		Following the change management process see item A2.19 notification will be provided prior to implementation in production and training shall be performed either via in-person, video computer based training, and/or in documentation.

SUPPORT & MAINTENANCE REQUIREMENTS

State Requirements

Req #	Requirement Description	Criticality	Response	Example Response
	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		Agreed
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		Based on assigned deficiencies the support team will resolve the issue and obtain acceptance following standard change management practices.
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		These documents will be provided based on their availability from the third-party COTS solution.
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;	M		Agreed
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.	M		The proposed solution and support will be able to diagnose root cause as needed as well as problem management to address repeat calls or configuration issues.
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		agreed
S1.16	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		See H4.8

PROJECT MANAGEMENT				
State Requirements				
Req #	**Requirement Description**	**Criticality**	**Response**	**Example Response**
PROJECT MANAGEMENT				
P1.1	Vendor shall participate in an initial kick-off meeting to initiate the Project.	M		Agreed
P1.2	Vendor shall provide Project Staff as specified in the RFA.	M		Agreed
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, vendors and state resources required and payment Schedule. The plan shall be updated no less than every two weeks.	M		Agreed
P1.4	Vendor shall provide detailed bi-weekly status reports on the progress of the Project, which will include expenses incurred year to date.	M		This proposal includes a weekly update for status reports that will include risks, actions, decisions. A monthly financial expense report will be provided.
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		This proposal includes standard project management principles and deliverables to include schedules, plans, reports, risks, actions, issues, decisions and financials and we can support utilizing the State project management solution or provide our own at the State's direction.
P1.6	Vendor shall provide a full time Project Manager assigned to the project.	M		Agreed
P1.7	The Vendor Project Manager, and relevant key staff, shall every three (3) months, beginning in the first month of the Contract, travel to Concord, NH to meet with project representatives from DHHS and the NHID to review past quarter performance and upcoming quarter Plan of Operations. Virtual meetings may be permitted if approved by DHHS.	M		All staff will be work remotely for the duration of this contract
P1.8	The Vendor's project manager is also expected to host other important meetings, assign contractor staff to those meetings as appropriate and provide an agenda for each meeting.	M		Agreed
P1.9	Meeting minutes will be documented and maintained electronically by the contractor and distributed within 24 hours after the meeting. Key decisions along with Closed, Active and Pending issues will be included in this document as well.	M		Agreed