ATTACHMENT THREE – REVISION ONE
Technical Requirements Traceability Matrix

Request for Proposal Number 6249 Z1

Bidder Name: _____

Bidders must describe in detail how the proposed system meets the conformance specification outlined within each Technical Requirement. It is not sufficient for the Bidder to simply state that it intends to meet the requirements of the RFP. The traceability matrix must indicate how the Bidder intends to comply with each requirement and the effort required to achieve that compliance.

The traceability matrix is used to document and track the project requirements from the proposal through testing to verify that the requirements have been met. The Contractor will be responsible for maintaining the contract set of Baseline Requirements. This traceability matrix will form one of the key artifacts required for testing and validation that each requirement has been complied with (i.e., 100% fulfilled).

The bidder must ensure that the original requirement identifier and requirement description are maintained from the traceability matrix.

How to complete the traceability matrix:

Column Description	Bidder Responsibility
Req #	The unique identifier for the requirement as assigned by DHHS, followed by the specific requirement number. This column is dictated by this RFP and must not be modified by the Bidder.
Requirement	The description of the requirement to which the Bidder must respond. This language is specified in the RFP and must not be modified by the Bidder.
(1) Comply	Bidder must insert an "X" if the system complies with the requirement. Describe in the response how the system meets the requirement. If the system does not comply with the requirement, the Bidder must address the following: 1. Capability does not currently exist in the system, but is planned in the near future (within the next few months) 2. Capability not available, is not planned, or requires extensive source-code design and customization to be considered part of the Bidder's standard capability 3. Capability requires an extensive integration effort of more than 500 hours
(a) Core	Bidder must insert an "X" if the requirement is met by existing capabilities of the core system or with minor modifications or configuration to existing functionality.
(b) Custom	Bidder must insert an "X" if the Bidder proposes to custom develop the capability to meet this requirement. Indicate "custom" for those features that require substantial or "from the ground up" development efforts.
(c) 3rd Party	Bidder must insert an "X" if the Bidder proposed to meet this requirement using a 3rd party component or product (e.g., a COTS vendor or other 3rd party). The Bidder must describe the product, including product name, functionality, and benefits in the response.

TECHNICAL REQUIREMENTS

The following requirements describe what is needed to support DHHS technical project operations.

Each requirement is identified by the following first three characters:

TEC	General Technical Requirements
STN	Standards Requirements
ERR	Error Handling Requirements
DBM	Database/Data Management Requirements
BKP	Backup and System Recovery Requirements
SEC	Security Requirements
DAC	Data Conversion Requirements
PTT	Production, Test and Training Requirements
INT	Interfaces/Imports/Exports Requirements
PER	System Performance Requirements
DOC	System and User Documentation

General Technical Requirements

This section presents the overall technical requirements that apply to the software. Describe in the response how the system meets the requirement.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-1	Provide a description and diagram of the technical architecture. Include all database/web/networking hardware, software, tools, etc. Indicate where the system is hosted. Indicate if any components are needed on the client and/or loaded on servers, etc. Solution will only be server/cloud technology in nature. DHHS envisions one domain to be hosted for all applications. Currently, online renewal applications for individuals and businesses subject to the Uniform Credentialing Act are handled by System Automation. Online initial applications for Nursing and online renewal applications for Long-Term Care are submitted via Nebraska Interactive.				
Response:					
TEC-2	Describe how the system is responsive to mobile technology and works with mobile devices such as smart phones or tablets.				
Response:					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-3	Describe any third party components that are proposed as part of the system, i.e. using Crystal Reports as a reporting tool.				
Response:					
TEC-4	Describe how the system is designed so that business rule parameters and code lookup tables can be easily updated without changing the overall application program logic.				
Response:					
TEC-5	Describe the upgrade and maintenance process for the system. Downtime and impact to the users must be minimized.				
Response:					
TEC-6	Describe any impact on customizations made to the system for upgrades and maintenance processes. Downtime and impact to the users must be minimized.				
Response:					
TEC-7	Describe any redundancy built into the system to limit any downtime.				
Response:					
TEC-8	Describe how the system has the ability to share data securely, including importing and exporting of data to/from other application software tools, such as a Microsoft Excel file, XML, comma separated value (csv) file, etc.				
Response:					
TEC-9	Describe how the system has the ability to archive data and documents per the DHHS' required record retention schedules, which provides different retention periods for different document types. Describe the method and ability to adjust to changes in the retention schedule.				
Response:					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-10	Describe how the system has the ability to provide audit information on all data accessed or changed within the system.				
Response:					
TEC-11	Describe how the system allows multiple users to use the software applications and database concurrently.				
Response:					
TEC-12	Describe how the system is scalable and flexible enough to accommodate any changes required by the DHHS, or by any federal statute, federal mandate, federal decision or federal policy.				
Response:					
TEC-13	Describe how the system is able to scan, attach, and store different document types (pictures, documents, PDF file, etc.) within the system.				
Response:					
TEC-14	Describe how the system has the ability to generate reports and ad hoc queries without performance impact to user access or system response time.				
Response:					
TEC-15	Describe the help desk operations and support that will be provided with the system.				
Response:					

Standards Requirements

DHHS currently operates its computer system in compliance with many technology and operational standards. These standards originate from internal development, industry best practices and governmental mandates. The Bidder must describe how all applications operate in compliance with these standards and practices.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
STN-1	If web-based system applications are required, describe what industry standard browsers are supported by the system. If the system requires additional components, describe the technical details of those components.				
Response:					
STN-2	The system must store data in federally compliant data centers residing within the continental United States of America.				
Response:					
STN-3	All data is the property of DHHS, and DHHS will retain the exclusive rights of use now and in perpetuity.				
Response:					
STN-4	The system must comply with accessibility requirements described in 45 CFR 85 and with State of Nebraska accessibility requirements located at: https://nitc.nebraska.gov/standards/2-101.pdf.				
Response:					
STN-5	The system must comply with the sub-parts of Section 508 of the Americans with Disabilities Act (ADA), and any other applicable State or federal disability legislation. Refer to http://www.ada.gov/508/.				
Response:					
STN-6	Describe how the system complies with digital signature requirements described in the Nebraska Digital Signatures Act, and all other applicable legal requirements in Nebraska for digital signatures. Refer to http://www.sos.ne.gov/rules-and-regs/regsearch/Rules/Secretary_of_State/Title-437.pdf for definition and standards in Nebraska.				
Response:					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
STN-7	The system must comply with all HIPAA and other statutory, regulatory, and policy requirements for protected health information. Refer to http://dhhs.ne.gov/ITSecurity.				
Response:					
STN-8	If the system requires client software to be installed, describe how the system ensures that all software used for the system can be distributed, installed and configured in an unattended "silent" manner.				
Response:					
STN-9	Current DHHS policies prevent users from making administrative changes and downloading software locally to their PC. Describe how the system supports this policy.				
Response:					
STN-10	Current DHHS policies recommend not storing any data locally in the event that a user's desktop PC needs to be reimaged (which deletes locally stored data). Describe how the system supports this policy.				
Response:					
STN-11	Describe the report design tools and output formats.				
Response:					
STN-12	Describe how the system maintains licensed software, including all third-party software, no more than two supported versions behind the latest release, and updated with latest security patches.				
Response:					

Error Handling Requirements

The management of the system requires that all occurrences of errors be logged for review and that critical errors be accompanied by appropriate alerts. Authorized users need to be able to query and review the error log and configure the alerts.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
ERR-1	Describe the error handling functionality.				
Response:					
ERR-2	Describe how the system provides a comprehensive set of edits at the point of data entry to minimize data errors and provide immediate feedback in order for incorrect data to be corrected before further processing (e.g., spell check, zip codes, etc.).				
Response:					
ERR-3	Describe how the system ensures all errors are written and categorized to an error log. Describe how the system allows for a user to view, filter, sort, and search the error log.				
Response:					
ERR-4	Describe how the system allows for user-defined alerts of errors, including those to external communication mechanisms (e.g., e-mail and text messaging).				
Response:					
ERR-5	Describe how the system provides for the generation of standard and customizable error reports.				
Response:					
ERR-6	Describe how the system includes a comprehensive list of error messages with unique message identifiers.				
Response:					
ERR-7	Describe how the system displays errors to the user/operator in real-time whenever an error is encountered.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response:					
ERR-8	Describe how the system has the ability to suppress error messages based upon user-defined criteria.				
Response:					

Database/Data Management Requirements

DHHS requires the benefits inherent with a relational database management system (RDBMS). The accessibility, flexibility and maintainability achieved through normalized data structures are essential to achieving the business objectives outlined in this RFP.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DBM-1	Describe the database architecture, including the database software that is supported by the system.				
Response:					
DBM-2	Describe how the system allows changes to be made available immediately on-line.				
Response:					
DBM-3	Describe how the system facilitates data structure changes to accommodate expanding scope, new services, changing requirements and legislative mandates.				
Response:					
DBM-4	Describe the standard software development life cycle (SDLC) for deploying software. Describe the process for planning, creating, testing and deploying the system.				
Response:					
DBM-5	Describe how the system provides the flexibility to extract and load data into standard non-proprietary software formats.				
Response:					
DBM-6	Describe how the system maintains an automated history of all transactions, including, but not limited to: date and time of change, "before" and "after" data field contents, and operator identifier or source of the update.				
Response:					
DBM-7	Describe how the software database conforms to the Open Database Connectivity Standard (ODBC).				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response:					
DBM-8	Describe how the system provides utilities or other tools for administrative users to evaluate data relationships between tables.				
Response:					
DBM-9	Describe how the system prevents corruption or loss of data already entered into the system in the event of failure.				
Response:					

Backup and System Recovery Requirements

The system must create backup copies of the software and restore and use those backup copies for the basic protection against system problems and data loss. This requirement refers to all application system files, data files, and database data files. The system must provide a comprehensive and easily manageable backup and recovery process.

The system must have a recovery plan that ensures component failures do not disrupt services. The plan must be completed, implemented, and tested prior to system implementation.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
BKP-1	Describe the Backup and System Recovery plan and readiness. Describe the service level agreement on returning the system to service from a backup. Describe the backup retention schedules – daily, weekly, monthly, quarterly, etc.				
Response:					
BKP-2	Describe all needed hardware, software, and tools, and define all roles, responsibilities, processes, and procedures. The system must be sufficiently flexible to integrate with existing DHHS capabilities and accommodate future changes.				
Response:					
BKP-3	Describe the Disaster Recovery Plan. Describe the service level agreement on returning the system back to operational service.				
Response:					
BKP-4	Describe how backups of the system are able to be scheduled without user intervention and without interruption to the system.				
Response:					
BKP-5	Describe how the system provides testing and validation processes for all of the backup requirements listed previously (BKP-1, BKP-2, BKP-3 and BKP-4).				
Response:					
BKP-6	If there is a backup failure or downtime, describe the method and timing of communication to DHHS.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response:					

Security and Audit Requirements

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-1	Describe the security safeguards integrated into their application and how these safeguards address DHHS security. Refer, for example, to DHHS Information Technology (IT) Access Control Standard ((DHHS-IT-2018-001B) for specific requirements: http://dhhs.ne.gov/ITSecurity				
Response:					
SEC-2	The system must comply with Federal, State, and division-specific security requirements including but not limited to: 1. Health Insurance Portability and Accountability Act (HIPAA) of 1996 2. Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 3. Nebraska Electronic Signature Statute http://www.nebraskalegislature.gov/laws/statutes.php?statute=86-611 4. Privacy Act of 1974 5. 45 CFR 164 Security standards for PHI Refer to the Nebraska DHHS Information Systems and Technology Security Policies and Standards for more information (http://dhhs.ne.gov/ITSecurity) Due to PHI, DHHS will not give access or demonstrate the current system. Our current data systems include System Automation's License 2000 and the federal government's Aspen Central Office.				
Response:					
SEC-3	Describe how the system meets the DHHS requirements for unique user ID access. Include: 1. Specification on configuration of the unique user ID. 2. How the unique user ID is assigned and managed. 3. How the unique user ID is used to log system activity. 4. How the system handles the creation of duplicate user ID accounts.				
Response:					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-4	Describe how the system meets the DHHS standard for administering passwords: 1. Initial Password assignment. 2. Strong Password Requirements. 3. Password reset process. 4. Password expiration policy. 5. Password controls for automatic lockout access to any user or user group after an administrator-defined number of unsuccessful log-on attempts.				
Response:					
SEC-5	Describe how the system meets the requirements for unique system administration access. Include: 1. Specification on configuration of the unique system administration ID, (approximately 30 with ability to access and manage the applications across all license types). 2. How the unique system administration ID is assigned and managed. 3. How the unique system administration ID is used to log system activity.				
Response:					
SEC-6	Describe how the system meets the requirements for unique database administration access. Include: 1. Specification on configuration of the unique database administration ID. 2. How the unique database administration ID is assigned and managed. 3. How the unique database administration ID is used to log system activity.				
Response:					
SEC-7	Describe how the system supports the use of multi-factor authentication.				
Response:					
SEC-8	Describe any security processes for managing security updates, and integrated components subject to vulnerability, including anti-virus.				
Response:					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-9	Describe how the system provides the ability to maintain a directory of all personnel who currently use or access the system.				
Response:					
SEC-10	The State of Nebraska requires authentication and authorization of users through an enterprise directory known as the Nebraska Directory Services (NDS) to access web-based applications. Describe how the system will integrate NDS authentication. Refer to the Nebraska Information Technology Commission Security Architecture – Authentication and Authorization – Identity and Access Management Standard for State Government Agencies (8-303) for specific requirements: https://nitc.nebraska.gov/standards/8-303.pdf				
Response:					
SEC-11	Describe how the system provides rule-based security and allows restricted access to system features, function, screens, fields, database, etc. Role authentication may occur at the directory level, application level, or database level (depending on database system). Describe the security administration functions integrated into the system that manage role-based access to system functions, features, and data. Include a description of: 1. How and where the system stores security attributes or roles (e.g., LDAP attributes, database tables, files). 2. The interface between the LDAP and the application, if roles are assigned in an LDAP directory. 3. How roles are created and security is applied to the role based on how and where security attributes are stored (if multiple options describe each). 4. How groups are defined and how roles and security are applied to each group. 5. How access limits are applied to screens and data on screens by role or group. 6. How users are created and assigned to one or more roles or groups. 7. How role and group creation and assignment activity is logged.				
Response:					
SEC-12	The system must automatically disconnect based upon inactivity, as required by DHHS Security Policies and Standards. Describe how the feature is administered and what effect disconnect has on any activity or transaction in process at the time of disconnection. Refer to DHHS Securing Hardware and Software Standard (DHHS-IT-2018-001A) for specific requirements: http://dhhs.ne.gov/ITSecurity				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response:					
SEC-13	The system must protect confidential and highly restricted data from unauthorized access during transmission. Describe transmission safeguards that are integrated into the proposed system to protect data during transmission, including any encryption technology. Refer to DHHS Information Technology (IT) Security Policy (DHHS-IT-2018-001) for specific requirements: http://dhhs.ne.gov/ITSecurity				
Response:					
SEC-14	The system must provide auditing functions for all data fields, including but not limited to: 1. The user ID of the person who made the change. 2. The date and time of the change. 3. The physical, software/hardware and/or network location of the person while making the change. 4. The information that was changed. 5. The outcome of the event. 6. The data before and after it was changed, and which screens were accessed and used. Refer to DHHS Information Technology (IT) Audit Standard (DHHS-IT-2018-001F DHHS IT Audit Standard) for specific audit requirements: http://dhhs.ne.gov/ITSecurity				
Response:					
SEC-15	The system must provide auditing functions for confidential and highly restricted data that is accessed and viewed, regardless of whether the data was changed. Describe the auditing functions which must include but not be limited to: 1. The user ID of the person who viewed the data. 2. The date and time of the viewed data. 3. The physical, software/hardware and/or network location of the person viewing the data. 4. The information that was viewed. Refer to DHHS Information Technology (IT) Audit Standard (DHHS-IT-2018-001F DHHS IT Audit Standard) for specific audit requirements: http://dhhs.ne.gov/ITSecurity				
Response:					
SEC-16	If the system has the ability to override edits, describe how the system audits all overridden edits and identifies information including, but not limited to, the login ID, date, and time.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response:					
SEC-17	Describe how the system produces daily audit trail reports and allows inquiries, showing updates applied to the data.				
Response:					
SEC-18	Describe how the system provides an auto archive/purge of the log files to prevent uncontrolled growth of the log and historical records storage using administrator-set parameters.				
Response:					
SEC-19	Describe how the system supports encryption of data at rest or an equivalent alternative protection mechanism. Describe the proposed encryption of data. If data is not encrypted, describe in detail compensating controls.				
Response:					
SEC-20	Describe how the system adheres to the principle of "Fail Safe" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks.				
Response:					
SEC-21	Describe how the system is configurable to prevent corruption or loss of data already entered into the system in the event of failure.				
Response:					
SEC-22	Describe how the system, upon access, displays a message banner indicating that this application is only to be accessed by those individuals who are authorized to use the system.				
Response:					
SEC-23	Describe how the system, prior to access of any confidential or highly restricted data, displays a configurable warning or login banner (e.g. "The system must only be accessed by authorized users"). In the event that the				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
	system does not support pre-login capabilities, describe how the system displays the banner immediately following authorization.				
Response:					
SEC-24	Describe how the system recognizes confidential and highly restricted data in screens, reports, and views (i.e. PHI and SSN), and restricts distribution and access based upon system security settings and roles. Include warnings on printed and viewed reports.				
Response:					
SEC-25	The system or Contractor must alert DHHS of potential violations of security and privacy safeguards. Incidents that involve or could potentially involve confidential or highly restricted data must be reported immediately as defined in DHHS Policy DHHS-2018-IT-001E DHHS IT Incident Management Standard.				
Response:					
SEC-26	Describe how the system provides the capability to monitor events on the information system, detects attacks, and provides identification of unauthorized use of the system.				
Response:					
SEC-27	The system must provide a process for archiving or destroying data and sanitizing storage media in conformance with DHHS and Division data governance policies and subject to applicable HIPAA, and federal (e.g., Federal Information Processing Standards (FIPS), National Institutes of Standards and Technology (NIST), and State laws.				
Response:					
SEC-28	Describe how the system provides the capability to identify and report on unauthorized attempts to access information in the system, based on user-defined criteria.				
Response:					
SEC-29	Describe how the system has defined and deployed strong controls (including access and query rights) to prevent any data misuse, such as fraud, marketing or other purposes.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response:					
SEC-30	The system must be able to export audit logs that can be used with a third party Log Management & Analysis tool. Describe how the system exports logs in such a manner as to allow correlation based on time (e.g. Universal Time Coordinate (UTC) synchronization.				
Response:					
SEC-31	Describe how the system supports removal of a user's privileges without deleting the user from the system to ensure a history of user's identity and actions.				
Response:					

Data Conversion Requirements

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DAC-1	Describe the process for converting all historical data from the Department's existing systems, spreadsheets, and other supporting applications that are required for ongoing operations of the system and the historical reporting needs of the department. System Automation's License 2000 (Oracle) currently contains approximately 655 tables and 50 million records. DHHS also has approximately twelve (12) Access/Excel databases. Some information in these databases does not tie to license information in L2K. DHHS also uses the federal government's Aspen Central Office to import licensure data on a daily basis.				
Response:					
DAC-2	Describe the data conversion plan which includes data element mapping crosswalks, data cleansing, data synchronization for initial and interim conversion activities leading up to the final data conversion, and frequency of interim conversion events and final conversion execution. Contractor will be responsible for all data standardization and cleansing. It is acceptable to migrate data and go live with license applications in incremental steps. For individual licensees, SSN is included in L2K. There is also an identifier called "Person ID" in L2K. For establishments in L2K, there are unique license numbers by license type, and unique applicant numbers. In ACO, establishments have unique license numbers by license type.				
Response:					

Production, Test and Training Requirements

DHHS requires three separate environments (Production, Test, and Training) in order to operate and maintain the new software on an ongoing basis:

Test Environment – A test environment is required that mirrors the live production environment, including hardware and software. This test environment will be used to test application changes before deployed to production. This step is an important part of quality assurance, where all changes are tested to minimize the risk of adverse reactions in the production environment. While it is necessary to mirror all of the functions of the production environment, it is not necessary to maintain the same load capacity.

Training Environment – A training environment is also required that allows DHHS to provide hands-on training to users. This environment would allow DHHS to maintain unique data for use in training and conduct training without interference with the test or production environments. This environment will have occasional use.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PTT-1	Describe how the system supports several environments, i.e., production environment, test environment, and training environment.				
Response:					
PTT-2	Describe how the system supports non-production environments such as testing and training environments. Training environment must contain de-identified data and not include confidential or highly restricted data.				
Response:					
PTT-3	Describe how the system provides the ability to refresh any testing or training environment at the request of DHHS. Describe the refresh process and whether the refresh process can be completed using DHHS resources, or whether the process requires professional services from the Contractor.				
Response:					
PTT-4	Describe the test procedures for any changes to the system. Describe user test planning including unit testing, end-to-end testing, stress testing, and readiness testing prior to “go live” date.				
Response:					
PTT-5	Describe how the system allows changes to be tested before implementation in the production database. Examples include changing licensure requirements, license type name changes, and scripts to replace data.				
Response:					

Interfaces/Imports/Exports Requirements

The system is required to be able to interface with other computer systems as necessary.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
INT-1	Describe the automated approach to managing interfaces. HL7 standards are available at www.hl7.org				
Response:					
INT-2	Describe how the system interfaces secure and protect the data and the associated infrastructure from a confidentiality, integrity and availability perspective.				
Response:					
INT-3	Describe how the system has the capability to notify system administrators/ system support staff if an interface is not available for any reason.				
Response:					
INT-4	Describe how the system provides necessary application program interfaces and/or web services to allow DHHS to create interfaces to and from the system. Exact number of imports/exports required. DHHS anticipates disciplinary databanks, compacts, schools, exam companies, and employers may interact with the system.				
Response:					
INT-5	Describe how the system supports data exchanges between components in real time so that data is always synchronous across the entire system, including any third-party components.				
Response:					
INT-6	Describe how the system has the ability to expand data access to additional systems that are consistent with current data standards.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response:					
INT-7	Describe how the system conducts end-to-end testing with interface partners, both external and internal, to ensure requirements are met.				
Response:					

System Performance Requirements

This section describes requirements related to the systems' on-line performance, response times, and sizing from a system architecture standpoint.

NOTE: If your system has specific high availability or redundancy requirements, the requirements must be defined below (see PER-5).

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PER-1	Describe the system performance functionality and monitoring tools.				
Response:					
PER-2	Describe the minimum response times for the following functions, even at peak load. For example, expected response time will be within two (2) seconds 95% of the time, and under five (5) seconds for 100% of the time. 1. Record Search Time 2. Record Retrieval Time 3. Transaction Response Time 4. Print Initiation Time 5. Subsequent Page Display Response Time 6. Document Availability Note: These response times do not include network latency, which will be measured and reported by DHHS.				
Response:					
PER-3	Describe how the system captures system downtimes, along with the causes of the downtimes where applicable. Describe the method and timing of communication to DHHS on downtimes.				
Response:					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PER-4	Describe how the system supports concurrent users with minimal impact to response time, with the ability to increase the demand on the system by 50% without modification to the software or degradation in performance.				
Response:					
PER-5	Describe how the system is available online 24 hours a day and 7 days a week. Describe any known timeframes where the system will be unavailable for use.				
Response:					
PER-6	Describe how the system provides application performance monitoring and management capabilities, including any key performance indicators (KPI) or other metrics to measure and report system performance for the proposed system.				
Response:					

System and User Documentation Requirements

DHHS requires the Contractor to develop, electronically store and distribute system documentation to include, at a minimum:

1. Reference Materials
2. System Documentation
3. A complete Data Dictionary

The Contractor must provide a complete Data Dictionary. The Data Dictionary is to include definitions of all data elements and tables where they reside.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DOC-1	Describe how the system provides on-line help for all features, functions, and data element fields, as well as descriptions and resolutions for error messages, using help features including indexing, searching, tool tips, and context-sensitive help topics. Provide a sample copy of five (5) screen shots with on-line help.				
Response:					
DOC-2	Describe how the system provides on-line user reference materials with a printable version available. The documentation must include full mock-ups of all screens/windows and provide narratives of the navigation features for each window/screen. Provide a sample copy of five (5) pages of the user reference materials.				
Response:					
DOC-3	Describe how the system will have on-line reporting reference materials with a printable version available that includes descriptions, definitions, and layouts for each standard report. Include definitions of all selection criteria parameters and each report item/data element, all field calculations defined in detail, and field and report titles. Provide a sample copy of five (5) pages of the reporting reference materials.				
Response:					
DOC-4	Describe how the system provides an entity-relationship model, class diagram, and a table of contents with data dictionary for report creation by the State that is regularly updated and includes table, field, and relationships.				
Response:					
DOC-5	Describe how the system provides a data dictionary which includes user-defined fields and tables which can be viewed online and kept updated for each modification.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response:					