Exhibit C HELMS Technical Requirements RFI N22787

Section 1: Enterprise, Interfacing Applications

HELMS is intended to be a seamless interface for all business user role functions. It is required that HELMS interface with the following Department- and WA-enterprise systems and solution components.

1. Office 365/Microsoft Office, Outlook.
2. Office of Financial Management Payment Services approved software currently in use: First Data, PayPoint Consumer Payments, Remit Plus, ACH Payment Returns for reconciliation of service payments.
3. OpenText ECM Suite, Department enterprise solution for records management, record storage and other related activities. Record here is defined as physical documents in an electronic format.
4. Secure Access Washington, WA authentication solution.
5. ServiceNow for ITIL service management.
6. Tableau, Department enterprise solution for data visualization.

Section 2: Other Technical Constraints

7. Solution must support OCIO Open Data Policy 187 (http://www.ocio.wa.gov/policy/open-data-planning). Solution must provide large-volume, un-manipulated, raw data in a machine-readable, scheduled data export capabilities.
8. Solution must provide responsive design.
9. Solution must support SAML 2.0 for authentication in order to integrate with Secure Access Washington and ADFS.
10. Solution must include a secondary data store (i.e. reporting database) that is refreshed from the transactional database.
11. Solution must be able to utilize web service APIs for integrations with required enterprise services.

Section 3: Quality of Service Requirements

Performance

Measure	Description	Requirements
Responsiveness	The specific ability of the system to complete any assigned task within a recommended time frame. Example: the system should respond in no less than 3-4 seconds for a query and report load.	Response time of no more than 3-4 seconds for query and report load and 2 seconds for other user interface responses.
Fault-Tolerance	A fault-tolerant system is planned, setup and configured to prevent failure in the event of an unexpected problem or error. In the event of a failure in the system, operating quality should be proportionate to the severity of the failure.	The system will continue to operate and notify the user that the error occurred and log the error.
Availability	The probability that a system will work as required and when required during a predefined period of time.	System is up and functional 99.9% of the time it is required. 8.76 hours in a year of permissible downtime during required uptime. (24 X 7 X 52 = 8,736 total hours in a year; 100% - 99.9% = 0.1% or 0.001; 8,736 X 0.001 = 8.736 hours) Internal core business hours have been determined as 6:00 AM to 6:00 PM Pacific Time Zone Monday through Saturday. For external customers core hours are 24/7. For scheduled data exchanges via system interfaces, the scheduled exchange time is based on agreed upon service level agreements for each data exchange. System must be configured for High Availability.
Reliability	Describes the ability of the system or a component of the system to function under stated conditions (100 users, for example) for a specified period of time.	Able to support concurrent use by 80% of the internal user base during core business hours, defined here as 6:00 AM to 6:00 PM Pacific Time Zone Monday through Saturday. Able to support external customers 90% of the time with 24/7 access.
Scalability	The capacity of a system to be changed in size or scale in order to handle the growing amount of work (or workers) required of the system into the future. Must have the ability to add additional computer memory and storage, but not necessarily in real-time.	Able to support up to 10% growth in overall user base without degradation of performance.
Processing Integrity	System processing is complete, accurate, timely, and authorized.	The system must meet State, Federal and Department auditing standards. Processes are designed in a manner that allows for good recovery and auditability based upon the designated Recovery Time Objective (RTO) and Recovery Point Objective (RPO). For mission critical components, the current required RTO and RPO are both 24 hours. (Possible move to a tiered approach for critical data)

Usability

Measure	Description	Requirements
Accessibility	Providing external users with disabilities with content and interaction that is similar or identical to that provided to external users without disabilities, in a form that produces a similar user experience. (508C Compliance)	System meets OCIO policy 188 on Accessibility (WCAG 2.0) http://www.ocio.wa.gov/policy/accessibility as well as 508C compliance. VPAT is also required.
Usability	The degree to which the system can be used by specified consumers to achieve quantified objectives with effectiveness, efficiency, and satisfaction in a quantified context of use. Consumers of the system, include, for example: internal users, providers and other healthcare professionals entering their application data, students entering requests to secure authorization to test prior to taking examinations, and respondents replying to STIDs and SOCs electronically, and others. Business needs will further define user roles and capabilities to be taken into consideration for system usefulness.	System will undergo 3rd party usability testing for all applicable consumer types and functionality before implementation into production.
Language Support	The user Interface will be made available in prescribed languages determined by the business.	Per Title VI of the Civil Rights Act, provider and facility applicants must read English and therefore, application, renewal and other recurring user interfaces (UI) will be in English; for any external UI, translations must be provided in alternate languages; for internal Department users the UI will be in English. If an additional language needs to be added, the vendor will coordinate with Department in house CLAS SMEs to add the additional language within a timeframe set forth in the SLA.

IT Service Management

Measure	Description	Requirements
Manageability	The ability to effectively coordinate with a vendor as to when preventive maintenance or service on the system should take place. (i.e. incident, change and release management)	System support adheres to ITIL best practices in the maintenance and operations of the software support, incident management, change management, and release management practices. Note: prospective vendors must demonstrate their incident management, change management and release management processes in current deployments
Maintainability	The degree to which system functionality can be repaired, or enhanced.	The system is built in a manner that it can be managed and maintained by the vendor effectively. Changes can be made, tested, deployed and implemented with minimal effort. The system is modular so that if one portion becomes obsolete, the full system will not be compromised.

		Note: Prospective vendors must demonstrate their record for upholding this requirement in current deployments, vendors should provide their software roadmap for existing solutions. in accordance with this requirement vendors will maintain current industry standards to ensure that the system does not become obsolete after a few years.
Interoperability	The ability of different systems and applications to communicate, exchange data, and use the information that has been exchanged.	System supports industry standard practices for data transfers (i.e. bulk data export/import, web/wcf service, api, etc) The system needs to be geared toward the ability to make it easy, fast and accurate to establish data agreements or have near real time updates for the purposes of information sharing or informatics usage.