Exhibit B HELMS Security Requirements RFI N22787

Section 1: Washington State Security Requirements

Washington State Office of the Chief Information Officer (OCIO) Security Requirements Policy 141.10, Security Information Technology Assets

NOTE: The Department's Information Security Office can provide assistance in navigating or clarifying this policy.

Section 2: Department Vendor Security Requirements

1. Network architectures must be single tenant or logical single tenant, and assure disaster resiliency. The architecture must provide logical boundaries that separate Internet available systems, internal application/utility systems, data systems, and user activities. Controls must prevent unauthorized connections to the assets within each segment. The architecture must provide continuous monitoring of both internal and external activity for anomalies and identify, report, and defend against security intrusions before the data is compromised. Automated processes, on-line analysis, notification and actions are expected

   Infrastructure must have three separate and fully independent environments/virtual instances: Such as: Development, Quality Assurance (QA) and Production.

2. The vendor must ensure data center security controls meet or exceed those expected by the Federal Information Security Management Act (FISMA) for moderate to high impact systems as described in FIPS 199 and 200, and in the most current release of National Institute of Standards and Technology (NIST) Special Publications SP800- 53.

3. The Vendor must be able to show the data center and all failover facilities are FedRAMP (or FISMA) certified for moderate to high Impact systems and that a recent SOC2 type 2 audit was conducted for the specific data center facility where the service is deployed, and all failover facilities. The audit must address security, integrity, availability and confidentiality.

4. The vendor will certify that all data collected, processed, routed, and/or stored by or through the service, or third party service providers, remains at all times within the United States.

5. The vendor will ensure systematic collection, monitoring, alerting, maintenance, retention, and disposal of security event logs and application audit trails. At a minimum: the logs and audit trails are written to an area inaccessible to system users and are protected from editing. At a minimum the logs and audit trails will provide historical details on all transactions within the system that are necessary to reconstruct activities. Type of event, date, time, account identification and machine identifiers are recorded and collected for each logged transaction. Audit and log files can be analyzed by type in order to find emerging issues or trends. The appearance of severe issues triggers an immediate notification to appropriate system administrators. Logs are secured against unauthorized changes. At a minimum, logs must be retained for a period of 6 months.

The Department expects practices that are consistent with the current version of SP800-92 for moderate to high impact systems.

6. The vendor will have implemented systematic and accountable processes for managing exposures to system and application vulnerabilities and for prevention of malware infections. The processes must assure the infrastructure is hardened against malicious code and maintained at the most current security patch levels. These practices must meet or exceed those described in NIST SP800-40 and SP 800-83.

7. The vendor shall conduct system and application vulnerability assessments at least monthly, and Penetration tests at least quarterly. These tests and assessments must be conducted by an independent accredited firm at least annually

8. The vendor will have successfully implemented application authentication controls that provide a high level of confidence in the identity of individuals, and meet or exceed those described in the most recent version of NIST SP 800-63 for information requiring assurance level 3 or higher.

9. The vendor will ensure the system/service supports single sign on for state government employees, and external users by integrating the system's authentication mechanisms with the Washington State Enterprise Active Directory and the Washington State Secure Authentication Gateways (post listeners are typically used for processing the gateway host headers). Knowledge and experience with SAML 2.0 is required.

10. The vendor will ensure all system and service accounts use Enterprise Active Directory or a similar centralized authentication and authorization mechanism. If authentication methods such as SQL authentication are required, by the system, the vendor must provide documentation showing how the credentials are secured during all transmissions, using encrypted sessions such as TLS or IPSec, and in storage using a secure hash method validated by the National Institute of Standards and Technology (NIST).

11. The vendor will have implemented security controls that require encrypted sessions and strong multifactor authentication for anyone able to remotely access the infrastructure (e.g., vendor employees and contractors). Authentication mechanisms must meet or exceed those described in the most recent version of NIST SP 800-63 for information requiring assurance level 3 or higher. For system administration purposes one of the factors must be provided by a device separate from the computer gaining access.

12. The vendor will ensure the data are encrypted, when transmitted across open untrusted networks (using key lengths of 128 bits or greater), and when at rest, (using key lengths of 256 bits or greater). Algorithm modules validated by the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) are required: http://csrc.nist.gov/groups/STM/cavp/validation.html, http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.

13. The vendor shall ensure application controls provide for sessions that terminate or re-authenticate after an inactivity period of 20 minutes or less.

14. The vendor shall ensure administrator and user roles sufficiently restrict privileges and access rights based upon the concepts of least privilege and need to know.

15. The vendor will have implemented application/system development practices consistent with the current version of NIST SP800-64 for moderate to high impact systems.

16. The vendor will assure the software does not contain any of the Open Web Application Security project (OWASP) top 10 vulnerabilities - https://www.owasp.org/index.php/Main_Page.

17. The vendor's operational security controls must meet or exceed those described in the most current version of National Institute of Security and Technology (NIST) special publication: SP800-53. Where applicable all controls must be consistent with those described for moderate to high impact systems.

18. The vendor must be able to show a recent SOC2 type 2 audit of their development and operational practices was conducted, or that a SOC2 type 2 audit will be completed within 6 months after contract execution. This audit must address security, integrity, availability and confidentiality.

19. The vendor must have implemented cyber security incident response practices consistent with NIST SP 800-61.

    The vendor will provide the Department a copy of their incident response practices prior to contract award.

20. The vendor will document, test and maintain a disaster recovery plan and alternate facility to assure the system/service is recovered within the recovery time objective set by the program.