Appendix I

Hosting Requirements

1. The selected Offeror shall supply all hosting equipment (hardware and software) required for performance of the Contract.

2. The selected Offeror shall provide secure access to all levels of users via the internet.

3. The selected Offeror shall use commercially reasonable resources and efforts to maintain adequate internet connection bandwidth and server capacity.

4. The selected Offeror shall maintain all hosting equipment (hardware and software) and replace as necessary to maintain compliance with the Service Level Agreements (see Appendix M, Service Level Matrix).

5. The selected Offeror shall make available the system and any custom software on a 24 x 7 basis as established by the RFP.

6. The selected Offeror shall perform routine maintenance during the planned weekly maintenance period. Routine maintenance shall include, but is not limited to, server upgrades/patching, software upgrades/patching and hardware maintenance. In order to maintain system availability, the Offeror is expected to rollover to a backup site during maintenance periods.

7. The selected Offeror shall perform non-routine maintenance at a mutually agreeable time with two (2) weeks advance notice to the Commonwealth.

8. From time to time, emergency maintenance may be required to bring down the system. In such situations, if possible, the selected Offeror shall give advance notice, before the system goes down for maintenance, to the Commonwealth. The selected Offeror will limit the emergency maintenance to those situations which require immediate action of bringing down the system that cannot wait for the next scheduled maintenance period. It is expected that the Offeror will rollover to a backup site during any such emergency maintenance.

9. The selected Offeror shall monitor, prevent and deter unauthorized system access. Any and all known attempts must be reported to the Commonwealth within the timeframe set out by the RFP.

10. The selected Offeror shall allow the Commonwealth or its delegate, at times chosen by the Commonwealth, to review the hosted system's location and security architecture.

11. The selected Offeror shall conduct a third party independent security/vulnerability assessment at its own expense and submit the results of such assessment to the Commonwealth within the timeframe set forth in the RFP.

12. The selected Offeror shall comply with Commonwealth directions/resolutions to remediate the results of the security/vulnerability assessment to align with the standards of the

Commonwealth.

13. The selected Offeror shall use industry best practices to protect access to the system with a firewall and firewall rules to prevent access by non-authorized users and block all improper and unauthorized access attempts.

14. The selected Offeror shall use industry best practices to provide system intrusion detection and prevention.

15. The selected Offeror shall use industry best practices to provide virus protection on all servers and network components.

16. The selected Offeror shall use industry best practices to update all systems and third party software security patches to reduce security risk.

17. The selected Offeror shall be solely responsible for all data storage required.

18. The selected Offeror shall take all necessary measures to protect the data including, but not limited to, the backup of the servers on a daily basis in accordance with industry best practices and encryption techniques.

19. The selected Offeror shall employ reasonable disaster recovery procedures to assist in preventing interruption in the use of the system.

20. The selected Offeror support and problem resolution solution shall provide a means to classify problems as to criticality and impact and with appropriate resolution procedures and escalation process for each classification of problem.

21. The selected Offeror staff, directly responsible for day-to-day monitoring and maintenance, shall have industry standard certifications applicable to the environment and system architecture used.

22. The selected Offeror shall limit access to the system and servers and provide access only to those staff that must have access to provide services proposed.

23. The selected Offeror shall locate servers in a climate-controlled environment. Offeror shall house all servers and equipment in an operational environment that meets industry standards including climate control, fire and security hazard detection, electrical needs, and physical security.

24. The selected Offeror shall examine system and error logs daily to minimize and predict system problems and initiate appropriate action.

Appendix I

Hosting Requirements

25. The selected Offeror shall utilize a secured backup solution to prevent loss of data, back up all data every day and store backup media. Storage of backup media offsite is required. Stored media must be kept in an all-hazards protective storage safe at the worksite and when taken offsite. All back up data and media shall be encrypted.

26. The selected Offeror shall completely test and apply patches for all third-party software products before release.