

RFP Feedback

The purpose of this document is to provide limited feedback to the HIE team regarding the RFC.

Table of Content

RFP Feedback	1
Table of Content	1
Overall	2
Core Services	2
Across all Areas	2
Privacy and Security	2
Legal Hold	2
Data at Rest	2
Audit Logging	2
System Environments	3
Scalability	3
Recovery and Availability	3
Configuration Management	3
System Security	4
System Health	4
Training	4
Resources	4
Help Desk	4
Hosting	4
Value Added Services	5
Across all Areas	5

Overall

Should we ask the vendor to provide any kind of particular model of cost recovery? Are we asking them to give us something to consume as a whole or on a per transaction basis?

Core Services

Across all Areas

Should the team define key metrics for each of the core services?

Should the team consider publishing estimates regarding service usage in the Core Services such that the RFP provider may understand the scope and scale of the environment?

The ability to report the usage of the particular core service in user defined periods of time.

The ability to provide analytics of the usage of the core services over time.

Privacy and Security

Legal Hold

Does the concept of legal hold apply to the HIE and should we ask that the responding vendors describe how legal hold requests would be addressed in the proposal?

Additional detail found at http://en.wikipedia.org/wiki/Legal_hold

Data at Rest

Should we ask the responding vendor to address how “data at rest” is protected from accidental leakage and accidental disclosure. Data at rest includes end user devices, disks in storage arrays, backup media (usually tape) and end user devices (inside and outside the hosting data center). Item 17 refers to section 13402(h)(2) of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5); however, it is only prescriptive of what should happen if a breach occurs, not how to reduce the risk of a breach?

Audit Logging

Can we ask the responders to describe how audit and logging data is managed. More specifically, how can audit and logging data be searched, archived and restored when necessary.

System Environments

Scalability

Can we ask the vendor to demonstrate (and report) that the system will scale to appropriate workload levels for North Carolina using load testing techniques?

Can we ask the vendor to provide the ability to perform (and report) automated functional tests and the results of that testing prior to significant change to the system.

Recovery and Availability

Should the workgroup define the goals for:

- RTO – Recovery Time Objective, when the system needs to be back up and running in the event of an event that diminishes or stops the system?
- RPO – Recovery Point Objective, how much data can be lost (tolerated) in the event that a data restoration is necessary.

Both of these definitions (and ultimately requirements) would help the vendors understand the business criticality of these systems.

Should the workgroup define the goals of [availability](#) of the proposed solution? In turn, can the vendor describe how the system will support the availability required by the business.

Should we ask the vendors to execute and report the results of periodic Disaster Recovery exercises that would demonstrate the vendor's ability to actually recover the "system."

If a hot site is necessary to support the appropriate RTO/RPO objectives, should we ask the vendor to periodically execute the failover?

Should we ask the vendor to periodically recover data from the production environment to a non production environment to validate recovery capabilities?

In the event of a data recovery, describe how recovered data and transactions will be reconciled and how potentially unrecovered data or transactions would be identified.

Can the vendor describe the technical resources required to consume the system outside the data center (at the endpoint for the end user). Minimum requirements for the technical resources required to consume the system (i.e., workstation, network (bandwidth and latency)).

Configuration Management

Can we ask the vendors to describe their configuration management processes and policies? This may be important to determine the vendors ability to maintain the proper configuration of computing resources and services. Can the vendor identify computing resources that are no longer in compliance with the proposed configuration (i.e., what

systems are not patched appropriately or what firewalls have ports open that are not identified in the configuration management system)?

Can the vendor describe how non-production environments will be configured and updated over time to ensure that the non-production environment represent an appropriate similarity to the production environment specifically as it relates to user test environments?

System Security

Could we ask the vendors to describe the security posture of the system and how they incorporate the concept of [defense in depth](#) in regard the system?

Can we ask the vendor to conduct periodic security analysis, testing and reporting to validate the implementation of the HIE and to identify any security gaps? Consideration for a third party to validate the security of the HIE as a system (people, process and technology – system).

System Health

Could we ask the vendors to describe how we will be able to determine the health of the overall system in relationship to the business functions supported by the computing resources? How we can identify and plan for appropriate increases in capacity for computing resources using the tools and processes proposed?

Training

Resources

Should the vendor provide a training environment (computing systems) for the duration of the HIE?

Help Desk

Should we ask that root cause reports be published for an event that violates SLA agreements. Root cause results should be retained and available online the vendor and the HIE.

Hosting

The hosting tab indicates in many places that the vendor should have the “ability to”. Should we also ask the vendors to report on historic performance for each area (i.e., Item Number 30 – Ability to report on system and network performance matrix, can they show representative examples of these artifacts in existing systems or a proposed representation). The [ability](#) to provide a level of service is occasionally distinct from the [historic performance](#) of the service.

Should we ask the vendor to describe any significant restrictions in their ability to scale the hosting solution for the HIE in the next five years. A significant restriction is one that would impose an unplanned financial or time impact on the planned deployment of the system. (i.e., do you have adequate floor space, power, UPS capacity to scale the hosting system?)

Describe how hosting resources and assets will be refreshed in the proposal. Describe the planned software upgrade methodology.

Please describe the Data Center Classification of any data center that participates in the solution (As defined by the Uptime Institute).

Describe the level of support from OLA and SLA providers of your solutions as well as the underpinning contracts used to provide your hosting solution.

Describe the physical security of any and all data centers supporting the proposed solution.

Value Added Services

Across all Areas

The team should define key metrics for each of the Value Add services.

The team should consider publishing estimates regarding service usage in the Value Add Services such that the RFP provider may understand the scope and scale of the environment.

The ability to report the usage of the particular Value Add services in user defined periods of time.

The ability to provide analytics of the usage of the Value Add services over time.