Security Assessment Report Services RFP
Response to Questions

Q: Can you please provide a copy of the vendor contract for the MARS-E NIST 800-53 Assessment, any amendments, and the RFP response from the winning bidder for YHI's MARS-E V1 assessment?

A: Respondents may email rfp@yourhealthidaho.org for a copy of the contract. The RFP response was proprietary, and as such cannot be made public.

Q: Will YHI provide the breakdown of controls and control families to be assessed in phase 1 vs. phase 2, or is this left to the discretion of the assessing company?

A: YHI has some controls we would like addressed in Phase I based on our observations. Otherwise, we expect the SAR vendor to help form a risk-based approach to the spread of controls tested in Phase 1 versus Phase 2. As a reminder, the new or changed controls from V1 to V2 must be tested in Phase I per CMS requirements. CMS has a recommended roadmap for testing as well to assist vendors.

Q: Will there be more than one location visited for the on-site assessment? (e.g., GI, YHI, and Data Center(s))?

A: The SAR vendor may choose which to perform in person and which to perform remotely. Typically we would expect a new SAR vendor to meet face-to-face once with each partner minimally. YHI and DHW are 3 blocks away from one another. GI is located in Mountain View, CA (we would expect the bulk of the fieldwork to be at GI in person). Data centers should be covered by a SOC report and we would not necessarily expect any travel, unless a particular control needs to be tested not covered by the SOC report.

Q: For reporting on findings from Phase One of the assessment, is it sufficient to include the findings in the weekly status reports as described in the RFP, or does YHI expect a draft SAR report at the end of Phase One that includes all Phase One findings?

A: A running list of exceptions should be provided weekly in Phase One. YHI needs a final list of exceptions at the end of Phase One. There is no expectation for a draft SAR at the end of Phase One.

Q: There are no systems or processes listed on page 6 that are "managed by YHI". However, we believe some systems/processes managed by YHI, such as YHI Customer Support, are normally included in a SAR. Are these types of processes out of scope of the SAR? If not, can you provide a complete list of systems/processes that YHI manages which should be included in the scope of the assessment?

A: YHI's customer support team utilizes GI systems listed in the SAR RFP. Internally, YHI staff uses MS365, a FISMA-compliant system.

Q: Page 6 of the RFP indicates that SSAE16 Type II SOC1, SOC2 (Security and Availability only), and SOC3 documentation may be available from Rackspace. For the SAR, is the assessor only required to review these reports for datacenter related controls or does YHI have an agreement with Rackspace to provide physical access to the datacenters to enable the assessor to test the applicable controls?

A: The vendor should assess the available SOC report(s), map to the MARS-E controls, and test any gaps as appropriate. YHI has a right to audit GI, and as such a right to audit RackSpace if gaps are discovered.

Q: For the remediation recommendations deliverable described on page 8 of the RFP, does YHI expect the remediation recommendations be expressed as milestones in the POA&M document or does YHI wish the assessor's recommendations be expressed in a separate document?

A: A separate document, please.