Links to watch the 8/13 Marketplace Committee meeting, currently scheduled at 8:00 AM MST:
http://www.idahoptv.org/insession/
http://www.yourhealthidaho.org/about-us/board-of-directors/board-meeting-details/
Either link above should provide a link to stream the audio and video of the Marketplace Committee.

Question #	Question	Answer
1	Will documentation be available to review offsite?	GI, Rackspace, and YHI documentation will be available for offsite review via secure portal.
2	Will full cooperation and access required to perform the SAR services be provided by other service providers with potential information required, (GetInsured, Accenture and First Data) without additional agreements between the SAR Vendor awardee and said service providers?	YHI is the contractual owner of all relevant parties and documentation.
3	In Attachment C, Independent Contractor Agreement for SAR Services, section K states that "the contractor will at its expense conduct a background check of its personnel prior to their commencement of work on the services" versus the RFP which states on page 12, "The successful Respondent will be required to pass a background check conducted by YHI" Are both background checks required?	YHI is reserving the right to check on the Respondent (the entity) as we determine. We are also expecting that the Respondent will do an appropriate background check on its personnel - two different concepts even though they used the same terms.
4	Does YHI require MARS-E (NIST 800-53 rev 3), or will the SAR Vendor be able to use the most recent rev 4?	YHI requires that the vendor uses MARS-E NIST 800-53 rev 3.
5	The RFP states: The SAR Vendor is not authorized to act on behalf of or commit YHI, but will manage the process to meet the deadlines of YHI and CMS. How will YHI handle resistance by other parties, to the SAR Vendor's requests for documentation and visibility into the system?	YHI is the contractual owner of all relevant parties and documentation.
6	YHI has provided CMS requirements for testing, which includes: • Security Control Technical Testing • Network and Component Scanning • Configuration Assessment • Documentation Review • Personnel Interviews • Observations	See Attachment A.
7	Are all the CMS requirements required for this project, as they are not specifically asked for in the RFP?	All of the CMS requirements are in scope for this project except for FTI related controls/control requirements.
8	Is there flexibility in the timeframe in which the project needs to occur?	No, the project is under a strict timeline.
9	Does the scope of this project include penetration and vulnerability testing? If this testing is within the scope of the project will remote users be included or excluded?	Please provide your proposal based on best practices and experience, keeping in mind the timeframe.
10	Revision 3 is referenced in the RFP, can we obtain a copy of NIST Special Publications 800-53 Revision 3 as the NIST website only offers Revision 4?	No.
11	Are physical site surveys a part of the risk assessment (designed to provide a snapshot of facility physical security posture and practices)?	Yes.
11.1	If so, how many facilities will be included in the assessment?	3 Locations(YHI-Boise, ID, GI-Mountain view, CA, & the main Rackspace data center-Ashburn, VA).
11.2	Does the Risk Assessment include any facilities or support agencies not located within 15 miles of the primary location?	Yes.
11.3	Does the scope of the project also include physical site surveys of the Rackspace locations in Chicago, IL and Ashburn, VA?	The primary data center in Ashburn, VA will be in scope for the project.
11.4	The RFP mentions "Interfaces: Between GI and DHW Between GI and Dept. of Insurance (DOI)." Is the Department of Insurance a separate entity from YHI? The RFP mentions "Interfaces: Between GI and DHW Between GI and Dept. of Insurance." Is the Department of Insurance a separate entity from YHI? If the Dept. of Insurance is a separate entity, does the scope of the project include a physical site survey of it?	DHW and DOI are separate entities and are not in scope, but we would like the respondents to look at the interfaces.
12	How many security-related policies/procedures have been developed?	Policies and procedures will be in place for all NIST 800-53 Rev 3 controls.
13	We conduct interviews with 3 groups (management, operational, technical). Would multiple interview sessions per group be involved?	The number of interview sessions with each party involved will vary based on the number of MARS-E controls that are applicable for each party.
14	Will the project include a need for scans performed internally, externally or both?	Both.
14.1	If so, how many internal IP addresses will be scanned?	12(GI) 1(YHI)
14.2	How many external IP addresses will be scanned?	0(YHI)
14.3	Will the internal scan be performed using administrator credentials or without credentials?	No.
15	In addition to assessing vulnerabilities, will we be asked to penetrate the vulnerabilities (external, internal, or both)?	No, do we not want the respondents to exploit vulnerabilities.
15.1	If so, how many physical locations or data centers will be involved in the vulnerability scan?	N/A
16	Are network assets involved in the security assessment accessible from a single location?	No, the project will include network assets located in the Rackspace Data center, YHI Server site, etc.
17	How many (approximate) IP addresses and systems are in each location?	12(GI), 1(YHI)

18	Will Web application assessments be included in the scope of this assessment?	Yes.
19	How many web applications will be included?	1(GI)
19.1	How many of the web applications are accessible to the internet?	1(GI)
19.2	How many web applications are NOT accessible to the internet?	None.
19.3	For each web application included in the scope of this assessment, would you please provide the approximate number of pages in each application?	1,553 JSPs
19.4	For each web application included in the scope of this assessment, how many user levels/roles will be tested? (e.g. guest, admin, user, etc.)	10-15 Privileged Admin Users (GI) and approximately 150-200 End users should be included in such a test.
20	Does the scope of the project include social engineering testing of manager/user awareness and training?	See Attachment A.
20.1	If so, how many of the 10-15 Privileged Admin Users (GI) and approximately 150-200 End users should be included in such a test?	Sampling requirements are included in the RFP.
21	Are there any restrictions on when the work can be performed (e.g. only at night, only during business hours, only on weekends).	Penetration/vulnerability testing window is 8pm-6am M-F, and weekends(GI & Rackspace).
22	Since this is a new system, have any previous assessments been performed?	No MARS-e conducted previously. OIG and CMS/Third-party audits completed for other state exchanges. Rackspace SSAE16 compliant.
22.1	If so, which firm(s) performed these services in the past?	N/A
23	The RFP states that “the Proposal must include a commitment to support YHI at least through April 31 2015 for required Services.” It also states that from “October 25, 2014 – April 30, 2015 – YHI reserves the right to require additional Services to assist in its efforts to meet CMS security assessment requirements. Aside from the SAR services listed in the RFP’s deliverables chart and the Remediation Recommendations – POA&M report, what other “required services” and/or “additional services “are being referred to here?	Additional services will be negotiated as needed.
24	Will there be dedicated resources from all stakeholders (i.e. YHI, GI, the Department of Insurance, and Rackspace)?	YHI & GI will provide resources as needed.
25	How many people is the RFP requiring the offeror to supply?	The RFP is not a request for a number of resources. The RFP is seeking a set of services that need to be provided, and each Respondent will determine the staffing required, and should describe that staffing in the Proposal (and the cost for such staffing).
26	Would you elaborate on the preferred method for vendors to invoice for project expenses related to travel, hotels, etc.	Please propose a method and we will address it after it is awarded.
27	Who will be responsible for coordinating discussions, access, etc. with Accenture, Vim, and First Data Government Solutions?	The respondent that receives the award will coordinate discussions, access, etc. with Accenture PMO team.
28	Which organization developed the documentation for MARS-E Compliance?	YHI & GI.
29	Is the exchanged currently functioning?	Exchange is currently functioning in development.
30	Are the security controls currently in place?	Hardware infrastructure deployment in progress. - GI & Rackspace; YHI controls are in progress.
31	To meet your due dates, how are we to provide a SAR by if the actual environment won’t be available till after September 22nd?	Please propose a method and we will address it after the RFP is awarded.
31.1	Would this be considered part of the scope of the RFP assessment?	Yes.
32	For the follow up services, is this something that we are to provide with our response or is this something that may be scoped at a later date?	Additional services will be negotiated as needed.
33	Are physical copy's required by Friday?	No, physical copy's are due by Monday.
35	When proposals are made public, will pricing also be made public?	The pricing will be made public is some form.
36	Are interviews conducted onsite or remotely?	We are open to allowing interviews to be conducted remotely and/or on site.
37	Among the 1553 pages on the GI site, how many of those pages are dynamic?	For the purposes of scoping, respondents should assume that a high percentage of pages are dynamic. If the high number of dynamic pages results in a increase in the over all cost, then respondents should note that in there proposal.
38	Will resourced be available during the Columbus day holiday and any other holidays observed by the state of Idaho as non-working holidays?	YHI resources will not be available on non-working holidays observed by the State of Idaho. The respondent that receives the award will be expected to take into considering all YHI non-working days in order to meet all project deadlines.

39	Will resourced be available during the Columbus day holiday and any other holidays observed by the state of Idaho as non-working holidays?	Please note Proprietary Materials section of the RFP and ensure that you are fully informed as to applicable law, including the Idaho Public Records Law. Without limiting the laws that may apply and solely for convenience, we note the manual posted by the Idaho Attorney General at: http://www.ag.idaho.gov/publications/legalManuals/PublicRecordsLaw.pdf
40	Does insurance need to be proven with submission?	YHI will accept an express representation that the insurance listed in the Proposal is currently in effect, and certificates of coverage will be provided upon request from YHI.
41	Can we get the ID statue for trade secret vs proprietary vs confidential?	Understanding applicable law is the obligation of each Respondent. Without limiting that obligation, please note our response above regarding the materials made available by the Idaho Attorney General.
42	The RFP makes mention of a conflict of interest disclosure, is there a form?	No, there is no form. Please make a statement about COI in the response.
43	Will the list of conference call participants be published?	No, no attendance was taken.
44	Could you please elaborate on whether or not NIST 800-53A can be used for a test methodology?	NIST SP 800-53 is in scope, assessors may use the 53A methodology, but we would not expect to fail specific 800-53A test cases when there may be another way we are meeting the 800-53 control.
45	When is the go live date?	October 31st.
46	Will controls be changing during assessment period?	We don't anticipate changes to the controls.
47	How many rounds of retesting will there be?	We would expect retest after the draft SAR for the final SAR 10/3 and before final 10/17 ATC.
48	Would YHI like the Is the vendor is was awarded the contract to use the sample SAR as a template?	Deviations could be approved, but should be approved by YHI & CMS in advance.
49	In regards to the outline provided on page 7, are there technical response requirements - page count?	Please use existing sections to include approach, timelines etc. No page count limit, but please keep as short as possible.
50	Has any preliminary testing been conducted on any of the components?	GI started vulnerability assessments several weeks ago, and is currently ongoing. We anticipate all self-identified high findings will be corrected or in progress by the time the assessment starts.
51	What vulnerability scanning tools are currently being used?	The requested information is confidential and cannot be disclosed publicly. YHI will disclose to the SAR Vendor after contract execution.
52	Should we assume that there is an incumbent bidder in this RFP process?	No, there is no incumbent bidder. This is the first assessment that will be conducted in the YHI environment. YHI will also have to address NIST SP 800-53 Rev 4 in the next 6 months.
53	In regards to scanning tools, does YHI have a preference in providing a system with tools for the assessor to use or should vendor bring there own tools?	we assume vendor brings standard tools.
54	Can additional information be disclosed regarding current security told in place?	YHI encourages each respondent to propose the tools it will use.
55	Will assessor perform configuration scans?	We ask that vendors propose a method in there response.
56	Will assessor participate in remediation's?	No, we believe assessors will be independent.
57	Will vendor need to provide training?	No, please provide detailed POA&M's with enough information so that we can proceed with remediation's, but no training.
58	Has the government performed independent cost estimates for this task?	No, we have not performed any such cost estimate.
59	Can you provide more information about number of databases, database types, OS's, etc.?	Some information was provided in the RFP. Because of security concerns, we are not able to provide more information. If respondents have concerns regarding specific systems, then they should make note of that in there proposal.
60	References for the corporate entity?	Yes, this is for the corporate entity.
61	Are resumes also needed?	Yes, please include relevant resumes with similar experience.
62	Does YHI want the vendor to exploit vulnerabilities detected in pen test or vulnerability test?	No. We would like the vendor to validate, but not exploit of the detected vulnerability.
63	At SAR, will the vendor participate?	No, there will be no participation with the awarded vendor and CMS. Questions may be directed to assessor via YHI.
64	For concerns on risk management, are looking for privilege escalation issues?	Yes, if any specific testing or tools are to be used, then please call that out in the proposal.
65	**Additional Note**	Please note that we do not anticipate any automated testing as part of the initial Draft SAR Phase I, tentatively discussed for 9/19. We anticipate that system testing may occur during the next phase leading up to a final SAR on 10/3. Other timelines meeting the Go-Live dates may be proposed by the vendor.