REQUEST FOR PROPOSALS

For

Privacy Assessment

(MARS-E NIST 800-53 Rev 4)

IDAHO HEALTH INSURANCE EXCHANGE
(HIX)

dba

YOUR HEALTH IDAHO
(YHI)

Project: Idaho Health Insurance Exchange (HIX) Privacy Assessment - YHI

Response Date: February 27, 2015, Noon MST

February 11, 2015

CONTENTS

INTRODUCTION AND BACKGROUND

BACKGROUND

The Idaho Health Insurance Exchange doing business as Your Health Idaho ("YHI") is seeking qualified and experienced respondents ("Respondents") to submit a written proposal in response to this Request for Proposals ("RFP") to provide privacy assessment services ("Services") relating to the MARS-E (NIST 800-53) Revision 4 framework and privacy obligations outlined in 45 C.F.R. §155.260 of Final Rule of the ACA.

On March 23, 2010, the President signed into law the Patient Protection and Affordable Care Act ("PPACA"). On March 30, 2010, the Health Care and Education Reconciliation Act of 2010 was signed into law. These laws, collectively referred to as the Affordable Care Act, include laws designed to expand coverage, to provide more health care choices, to enhance the quality of care for all Americans, to hold companies more accountable, and to lower health care costs.

An independent Board representing key stakeholders has been appointed by the Governor, and has approved the creation of Your Health Idaho to oversee the implementation and ongoing operations of the Idaho State Benefit Exchange for insurance policies effective January 1, 2015.

The mission of YHI is to establish a new online marketplace for Idaho where individuals and small businesses can search for, compare and make an informed decision about the health insurance coverage that is best for them and their families in a private and secure solution.

YHI is Idaho's state-based health insurance marketplace. YHI initially used the Federally-Facilitated Marketplace ("FFM," also known as healthcare.gov) as the back-end for the marketplace. November 15, 2014, YHI transitioned to using a state-based marketplace.

A YHI consumer typically interacts with three systems primarily:

1) yourhealthidaho.org: This is the front end to our two primary interfacing systems (Idaho Department of Health and Welfare and Get Insured ("GI")). The yourhealthidaho.org site is designed and maintained by Bursen Marsteller ("BM"). The front end is largely static and is used for public relations and communications. This portion of the system is hosted by Amazon Web Services ("AWS"). BM manages the relationship with AWS currently.

2) Department of Health and Welfare ("DHW") Integrated Eligibility System: DHW provides Eligibility Shared Services to YHI. The majority of YHI's consumers apply for an Advanced Premium Tax Credit ("APTC"). Applicants create an account (single sign on across DHW and the Marketplace) and fill out an application online. Approximately 24-48 hours later a DHW case worker manually works the application, following up as needed for additional information. DHW initially applies a ruleset to determine whether YHI's applicant should first be covered under a different program, and then runs a ruleset to determine whether the applicant is eligible for an

APTC under the ACA policy. If DHW determines the applicant is eligible for an APTC, the consumer is notified via email and instructed to log into the marketplace to shop.

3) Marketplace: The marketplace is based on software developed and operated by Get Insured. The primary and failover sites are hosted at Rackspace (hosting provider for Get Insured). After receiving an APTC eligibility determination (or without an APTC eligibility determination if the consumer so wishes), the consumer can browse for, compare, and enroll in a Qualified Health Plan ("QHP"). After enrollment, payment is handled by the insurance carriers through a payment redirect to the carrier site or through other manual methods. Nightly enrollments are sent from the marketplace to carriers to reconcile the day's enrollments in an 834 batch file.

YHI is soliciting proposals for a Privacy Assessment to begin in early-to-mid April. The output of the assessment will be the findings and recommendations to help YHI improve the business processes around user data privacy. Additionally YHI anticipates engaging a third-party security assessment of the MARS-e controls later this calendar year to test the security controls for the current version 3, in addition to the new version 4 controls (largely privacy-based).

SCOPE & EXPECTATIONS

This RFP is for services of a contractor to complete all tasks and work required to deliver a Data Privacy Assessment Report and Privacy Impact Assessment (PIA) of the YHI HIX system. The primary drivers of the privacy assessment are:

1. Protecting and ensuring the privacy of Exchange (YHI HIX) managed personally identifiable information ("PII")
2. Meeting customer expectations around:
    - Compliance with applicable privacy laws (Idaho and federal) , regulations (Idaho and federal), contracts, and data use/sharing agreements
    - Protection against identity theft and fraud
    - Protection against reputational and brand risks

The assessment should evaluate the current YHI HIX system boundary and provide YHI a mechanism to assess:

1) The YHI business environment in which PII will be collected, created, used, disclosed, retained and destroyed
2) Whether YHI has properly interpreted and implemented the privacy obligations outlined in Section 155.260 of Final Rule of the ACA.
3) Assess privacy risks across:
    - Manual processes (face to face or data entry)
    - Interfacing DHW, YHI, and GI systems
    - Relevant third parties (AWS, Rackspace, print vendors, etc.)

The scope of the assessment would include (but is not limited to):

1.) Identifying user data sources and flow of information within and to and from the Exchange
2.) Review of the HIX system documentation for privacy implementation
3.) List all of the Exchange privacy documentation in which Final Rule privacy requirements have been incorporated
4.) Identify privacy risks and the mitigation plan
5.) Assess the privacy exposures and privacy measures relating to the business functions that involve the PII data. Business functions to initially assess include (but are not limited to):
    - Eligibility
    - Initial enrollments
    - Dis-enrollments
    - Passive renewals
    - Active renewals
    - Administration (reports from third parties, etc.)
    - Consumer Assistance
    - Exemption Determinations
    - Submission of Notices
    - Eligibility Appeals
    - Financial Functions including premium payments
    - Navigator and Broker programs
    - Quality Assessments, Disclosures & Data Reporting
6.) Assess the privacy breach response plan and processes in place for compliance with applicable law and industry practices
7.) Assess the operational, administrative, technical, and physical safeguards to protect PII data and to prevent unauthorized or inappropriate access, use, or disclosure of data for compliance with applicable law. The assessment will be largely qualitative in nature with focus on the safeguard mechanisms around data protection
8.) Assess organizational compliance with its privacy policies and procedures

Where maturity allows and where the risk warrants it, tests of controls are preferred to observation and inquiry. The technical testing of networks, systems and computers, and the software operating on and in them will be out of scope of this assessment.

Based on the business processes assessed, the assessment should cover risks pertaining to:

- Rights of the individual (notice, choice and consent, data subject access to data)
- Controls on the information (information security and integrity)
- Lifecycle of the information (collection, use and retention, and disclosure)
- Management (administration, monitoring and enforcement, penalties and sanction of regulators)
- Breach and incident identification, reporting and management

As YHI's system spans multiple entities (YHI, DHW, GI, and multiple third parties), the assessment should specifically consider organizational governance:

- Legal agreements and inter-organizational agreements (data use agreements, data sharing agreements, and how they relate to YHI's business processes)
- Maturity of privacy functions
- Inter-organizational incident response policies and procedures
- Management of vendors, and reporting and governance information flows within YHI and with its vendors
- Oversight functions
- Training (YHI internally but also with partners and vendors)
- Management of complaints

In order to obtain an Authority to Connect (ATC) to the Federal HUB, YHI completed a PIA, System Security Plan, and other documents comprising the ATC package. After gaining an understanding of the business processes and data structures, the assessment should include a review of the ATC PIA and the other components of the ATC package.

DELIVERABLES

YHI would expect the following deliverables:

Deliverable #	Deliverable Name	Description
1	Initial Request List	Initial list of policies, procedures and artifacts required by the vendor to aid in its preparation of the assessment.
2	Project plan	Project plan that describes the project timeline, dependencies, percent complete, milestones, tasks, due dates, and resources assigned, covering the full scope of the project.

3	Current State Assessment	The report that provides in-depth detail about the findings from assessment of business processes against data privacy and security requirements and applicable laws, regulations and good industry practices
4	Gap Analysis and Recommendations	The consolidated report that describes the gaps identified in the Current State Assessment, the impacts to YHI, and recommendations as to how each gap can be remediated.
5	Executive summary report and closing meeting	The report that provides an executive-level overview of the project scope, key findings, business risks and impacts, associated root causes and recommendations.
6	Weekly Status Reports	Weekly status reports of progress made on planned work and deliverables, updated risks and issues logs, and copies of notes taken during interview sessions and workshops.

ADMINISTATIVE

PROPOSAL INQUIRIES

Respondents may make written inquiries regarding this RFP any time during the inquiry period listed on the RFP cover sheet. YHI may not respond to any improperly formatted inquiries, and will not respond to any verbal inquiries. YHI will try to respond to all proper inquiries within 24 hours, excluding weekends and State holidays. YHI will not respond to any inquiries received after the due date set forth below for questions. YHI may extend the proposal due date. Any inquiry and YHI's response will be made available publicly.

Inquiries should be emailed to rfp@yourhealthidaho.org. Answers will be provided in an open forum on February 20, 11:00 AM MST.

To attend the February 20 Open Call, use this information:
1-888-204-5987
Access code 1694933

DUE DATES

All proposals are due by 5:00 pm, MST, on February 27, 2015. Any proposals received at the designated location after the required time and date specified for receipt shall be considered late and non-responsive. Any late proposals will not be evaluated for award.

SCHEDULE OF EVENTS

All times listed is Mountain Standard Time (EST). Event	**Date**
1. RFP Distribution to Vendors	February 11, 5:00 PM MST
2. Questions from Vendors Due	February 18, 5:00 PM MST
3. Open Call to Answer Questions Received by February 18, 5:00 MST	February 20, 11:00 AM MST
4. Proposal Due Date	February 27, Noon MST
5. Interviews of Candidates, if needed	March 2 – March 4
6. Anticipated Committee Recommendation of Vendor	March 20 (subject to change)
7. Anticipated Board Approval of Vendor	March 27 (subject to change)
8. Anticipated Work Commencement Date	On or after April 6

PROPOSAL SUBMITTAL

Each Respondent must submit signed copies of its proposal to RFP@YourHealthIdaho.org. We recommend an email follow up to RFP@YourHealthIdaho.org if you are sending files over 2 MB – we will respond to confirm receipt.

Proposals submitted will be irrevocable and effective for a minimum of 45 days following the Proposal Due Date, during which time they can be accepted by YHI, and each proposal will follow this format:

- Cover Letter (include phone and e-mail contact)
- State Term Schedule (STS) Number
- STS Labor Category Code
- Respondent Information:
    - Respondent References (3 minimum) - form
    - Respondent Resume
    - Additional Respondent Information (optional)
    - Personnel who will be performing services and their backgrounds
- Vendor Hourly Rate for Work provided on a time and materials basis
- Cost of Deliverables (for each, indicate whether a fixed fee, not to exceed amount or hourly rate without any not to exceed amount, provided that it is understood that the successful vendor is likely to have proposed a fixed fee or not to exceed amount for the Deliverables above)
- Deliverable Timeline consistent with this RFP
- Conflict of Interest Statement disclosing any relationship or financial interest between Respondent or its officers or directors or 10% or greater shareholders and GetInsured, BM, YHI, or DHW or the officers of any of them, or any other relationship or financial interest that could reasonably be seen as creating a conflict of interest between Respondent and YHI in connection with its performance under this RFP if it is awarded the contract
- Payment Address
- Proof of Insurance
- W-9 Form
- Comments to our attached Independent Contractor Agreement (ICA), Appendix 1: We have attached in editable Word format our standard ICA. Each Respondent is required to return a copy marked with any proposed changes clearly tracked in editable Word format. If a proposal does not include proposed changes to our standard ICA, the Respondent submitting the proposal is accepting our standard ICA and the Respondent is agreeing to sign that form. We will consider the proposed revisions to our standard ICA as discussed below.
- Acknowledgement of Appendix 2, the Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities. This assessment may require the Vendor to access and/or store PII through the course of the assessment.
- Acknowledgement of Appendix 3, the Definitions to Non-Exchange Entities.

YHI will not be liable for any costs incurred by any offer or in responding to this RFP, even if YHI does not award a contract through this process. YHI may reject late proposals regardless of the cause for the delay. YHI may also reject any proposal that it believes is not in its interest to accept and may decide not to do business with any of the Respondents.

EVALUATION FACTORS FOR AWARD

REQUIREMENTS

The following will be considered in determining the Respondent to be selected for this engagement, according to a standardized scoring methodology:

- Adherence to the stated requirements and technical proposal response
- Relevant experience in the privacy and security space, especially performing assessments
- Relevant experience of the proposed team (specifically with NIST 800-53 Rev 3 and 4)
- Nature and volume of proposed changes to our Independent Contractor Agreement (ICA)
- Proposed fees and hourly rate(s)

The successful Respondent to this RFP will have demonstrated experience in healthcare, technology, and security and privacy assessments. The successful Respondent will also demonstrate an understanding of the Affordable Care Act ("ACA"), health insurance exchanges, healthcare regulations, insurance exchanges, insurance company and Medicaid information systems, and business operations, processes, and performance measurements. The successful Respondent may be required to pass a background check.

In response to this RFP, please provide a minimum of three references with contact information for each reference. Reference contacts must be from a client who managed or supervised you or your firm's work or who had oversight responsibility for you or your firm's performance for that work experience. The reference contact must be available to validate the experience provided on the dates specified in the resume. Include the following information for each reference:

1. Engagement name
2. Brief description of the engagement
3. Contact name and title
4. Contact phone numbers and email address

Respondents should also briefly describe their understanding of the services needed and the activities the Respondent will perform. Respondents should include expectations of all entities outside their own team and how Respondent would initially engage with YHI and its stakeholders to perform this work.

Respondents should provide a resume plus details on at least three relevant/similar contract negotiations that Respondent has successfully led or guided to a successful conclusion including a description of cost savings and unique contract arrangements achieved for the benefit of the client.

The Services will comply with all applicable rules, standards and specifications of the State of Idaho, the federal government and other regulatory agencies. The successful Respondent to this RFP must be qualified, and must have the demonstrated ability to provide similar services for other projects similar in size and complexity to the solutions project.

As much as is practical and to the extent allowed by Idaho and federal law, YHI requests that Respondents team with companies that have a significant presence in Idaho.

GENERAL INFORMATION

GENERAL TERMS
This RFP does not commit the YHI to enter into an agreement, to pay any costs incurred in the preparation of this proposal or in subsequent negotiations, or to procure or contract for any Services.

REVISIONS TO RFP
In the event that it is necessary to revise or amend any part of the RFP, timely addenda will be issued by email to those firms that respond to the RFP.

RESERVATION OF RIGHTS BY YHI
The issuance of this RFP does not constitute an assurance by YHI that any contract will actually be entered into by YHI and YHI expressly reserves the right to:

- Waive any immaterial defect or informality in any proposal or response procedure.
- Reject any and all proposals.
- Request additional information and data from any or all Respondents.
- Supplement, amend, or otherwise modify this RFP or cancel this RFP with or without the substitution of another RFP.
- Disqualify any Respondent who fails to provide information or data requested herein or who provides inaccurate or misleading information or data.
- Disqualify any Respondent on the basis of any real or apparent conflict of interest.
- Disqualify any Respondent on the basis of past performance on other projects.
- Prior to the response time, YHI may meet with and consult with some or all of the potential Respondents to this request.
- YHI may negotiate with any Respondent to this RFP and shall have the sole discretion to choose the best combination of qualifications and price for the Project and Services.
- YHI shall have the sole discretion to select one, none or several different Respondents to provide the Services, or portions thereof.

By responding to this RFP, each Respondent agrees that any finding by YHI regarding any fact in dispute as to this RFP or proposals received by YHI under this RFP shall be final and conclusive except as provided herein.

EVALUATION
An Evaluation Committee will evaluate and determine the individual and comparative merits of each of the proposals received. It is the responsibility of the Respondent to ensure that the proposal complies with this RFP, demonstrates qualifications, and provides the information requested. If the Respondent fails to provide any information requested in this RFP, such failure may result in either non-qualification of a particular category of service or

rejection of the proposal. The Evaluation Committee may choose to interview some, none or all Respondents.

PROPRIETARY MATERIAL

YHI assumes no liability for disclosure of proprietary material submitted by Respondents. Proposal submittals may be considered public documents under applicable state law except to the extent portions of the proposal are otherwise protected under applicable law. Any specific item of information that Respondent asserts is a trade secret and which is included in a proposal shall be segregated by Respondent from the other portions of the proposal and labeled as such. Respondent shall not label an entire document as a "trade secret," merely because a portion of that document is or may be a trade secret. If any information claimed by Respondent to be a trade secret becomes the subject of a public records or other such request for production, YHI will notify the Respondent and, upon the execution of an agreement to defend and indemnify YHI, will allow the Respondent to address the public records or other request on behalf of YHI in the appropriate forum.

Disposition of Proposals

All Proposals received by YHI shall upon receipt become and remain the property of YHI. YHI shall have the right to use all concepts contained in any Proposal and this right will not affect the solicitation or rejection of any Proposal.

Release of Claims

By submitting a Proposal, the Respondent agrees that it will not bring any claim or cause of action against YHI based on: 1) any misunderstanding concerning the information provided herein; 2) concerning YHI's failure, negligent or otherwise, to provide the Respondent with pertinent information as intended by this RFP; or 3) YHI's decision to select a different party as the SAR Vendor.

Subcontractors

In the event a Proposal is submitted that involves more than one organization, one organization shall be designated as the Respondent. All other participants shall be designated as subcontractors. All subcontractors shall be identified by name and for each proposed subcontractor, background information along with a description of the functions or tasks the subcontractor(s) would perform under this RFP must be included consistent with instructions found elsewhere in this RFP. The Respondent shall be wholly responsible for the entire performance whether or not subcontractors are used. The project leader (Project Manager) shall be an employee of the Respondent and meet all the relevant requirements.

The Respondent must acknowledge a binding agreement between the Respondent and any subcontractors has been executed. YHI reserves the right to review any subcontracting agreements.

Award

Notification of intended contract award, if any, shall be provided to the selected Respondent on or about the date specified in this RFP. Such notification shall be subsequently confirmed in writing. The contract award is subject to availability of funding. Until YHI returns a countersigned Contract Commitment and Independent Contractor Services Agreement, there is no binding agreement and YHI retains the freedom to determine how to proceed, notwithstanding any notification of intended contract award it may have provided.

Neither YHI nor the State of Idaho are liable for any work, costs, expenses, loss of profits, or any damages whatsoever incurred by the SAR Vendor prior to the official starting date, and contract work prior to this date may result in no payment. YHI reserves the right to modify this policy; any modification will be made in a written statement and signed by both YHI and the SAR Vendor.

Contract Negotiation Process

Upon completion of the evaluation process, YHI may select one Respondent to be the SAR Vendor, based on the evaluation findings and other criteria deemed relevant for ensuring that the decision is in the best interest of YHI and the State of Idaho. In the event that for any reason YHI does not complete the contract with the selected Respondent within three (3) days of such selection, YHI reserves the option of negotiating with another Respondent.

Protest Policy and Procedures

Respondents who submit Proposals in response to this RFP may protest the award of the contract resulting from this RFP. A Notice of Intent to Protest must be made in writing to the Issuing Officer and must be received no later than two (2) working days from the notice of non-award. If no such Notice of Intent to Protest is timely filed, the Respondent forgoes its ability to pursue a protest.

A Protest Notification must be made in writing to the Issuing Officer and must be received no later than five (5) working days from the notice of non-award. The Protest Notification must contain specific grounds for the protest. Supporting documentation must be included with the protest. A protest must state all grounds upon which the protesting party asserts that the solicitation or award was improper. Issues not raised by the protesting party in the protest are deemed waived. A protest that is incomplete or not submitted within the prescribed time limits will be summarily dismissed.

Only the following are acceptable grounds for protest:

- Failure to follow YHI procedures established in this RFP or YHI rules of procurement
- Errors in computing scores which contributed to the incorrect selection of a Respondent
- Bias, discrimination, or conflict of interest on the part of an evaluator

Disallowed grounds include:

- Evaluator qualifications to serve on the Proposal Review Team
- The professional judgment of the Proposal Review Team
- YHI's assessment of its own needs regarding the RFP