Project Title:
Third-Party Security Assessment - Minnesota Insurance Marketplace (MNsure)

Service Categories (vendor must be approved in at least 1 of the 4 categories listed):
- Analyst - Risk Assessment
- Architecture Planning & Assessment – Security
- Server – Security
- Network (Data, Video, Voice) – Security

Business Need
MN.IT Services and the Minnesota Insurance Marketplace (MNsure), collectively referred to as the State, are seeking a vendor to provide management with a Security Assessment for the MNsure system. This security assessment must evaluate the MNsure system’s implementation of, and compliance with, MNsure’s baseline security standards, implementation of federal MARS-E (Minimum Acceptable Risk Standard for Exchanges) controls, and NIST 800-53A moderate controls.

MNsure is a newly developed system that will offer an easy-to-use one-stop web portal through which citizens can search and compare health insurance plans. In July 2012, Minnesota entered into a contract to design and develop the technical capabilities, including a consumer friendly web portal. That contract covered the development of technology for the following functions: individual eligibility determination and enrollment; small employer eligibility and enrollment; certification and display of health benefit plan options and costs; navigator and agent/broker listing; display of health care provider information; premium aggregation and payment; and account administration. Since the inception, MN.IT security professionals have been integrated into the project and have been developing a system security plan that outlines security controls aligned with federal expectations based upon NIST 800-53.
Goal and Project Deliverables
The goal of this SOW is to evaluate and select an experienced vendor specializing in security and technical assessments, to provide a robust security assessment with documented outcomes and recommendations, as part of the overall system accreditation process.

The State desires the assessment be broken up into three phases: an initial pre-production assessment and recommendation (Aug. 2013); a secondary gap assessment follow up (Nov. 2013), and; a re-assessment covering added system functionality to be completed in the second quarter of calendar year 2014. The goal of the re-assessment is to evaluate any changes in the control structure that may have occurred.

Deliverables will include the following:

August 2013
• An opinion on compliance with security requirements for health insurance exchanges, stated in one of three categories:
  1. Fully compliant: Security controls designed and placed in operation satisfy the underpinning compliance requirements, in all material respects;
  2. Substantially compliant: Security controls designed and placed in operation satisfy the underpinning compliance requirements, with the exception of certain issues that are identified in an accompanying gap assessment report; or
  3. Not Compliant: When taken as a whole, the security controls designed and placed in operation do not satisfy the underpinning compliance requirements, in all material respects. A detailed gap assessment will document the basis for the adverse opinion on compliance.

Along with the opinion, the deliverables will include a detailed description of the methodology used to arrive at the opinion, including security controls tested and the results of each test. The State would expect that the security assessment results be documented in alignment with MARS-E and NIST 800-53A and the results would be presented in a manner that is similar to a FedRAMP Security Assessment found at: http://www.gsa.gov/portal/getMediaData?mediaId=155123.

• A Gap Assessment Report that describes all instances of noncompliance with security requirements for health insurance exchanges, along with recommendations for remedying the deficiencies. During the course of the engagement, critical vulnerabilities or issues of noncompliance must be communicated to identified management immediately;

• An on-site presentation to present findings and recommendations to MNsure and MN.IT Services management;

November 2013
• A follow up assessment of work done to remediate any issues in the Gap Assessment Report, including a written determination of whether all issues have in fact been remediated.

April 2014
• Report on security controls over any new functionality added after the completion of the first security assessment.

Project Milestones and Schedule
• July 22, 2013 – Project Start Date
• July 22, 2013 – Meet with management, develop schedule, begin assessment
• August 21, 2013 – Written report is due, meet with management to discuss results.
August 21, 2013 – September 2013 MN.IT and MNsure finalize system implementation and address any pre-production assessment findings
October 1, 2013 – MNSure production system initial deployment
November 11, 2013 – gap assessment begins
November 29, 2013 – gap assessment completed
December 6, 2013 – gap assessment report due, meet with management to discuss results.
January 1, 2013 – MNSure full system deployment and operations
March 2014 – re-assessment begins
June 2014 – Written report is due, meet with management to discuss results.

The state reserves the right to not retain the selected vendor for the secondary/post implementation assessments if it is not satisfied with the quality of the pre-production assessment.

Project Environment (State Resources)

Staff Descriptions:
   a. The contractor will report administratively to the MN.IT Services Risk and Compliance Manager.
   b. MN.IT security professionals will be available to help the contractor gain an understating of and conduct tests of controls. However, the overall objective of this work order is to have an independent assessment of controls.

System Control Expectations:
The State has worked to produce a detail system security plan (SSP) that describes security control expectations that are aligned with federal MARS-E and NIST 800-53. Controls are documented in MS Word templates. System Technology Architecture:
A list of architecture components is available upon request. Please contact Barry Caplin (barry.caplin@state.mn.us) at 651-431-2143 for more details.

Security Architecture:
An overview of the security components includes:
Responsibilities Expected of the Selected Vendor

a. The selected vendor is expected to work with State staff throughout the assessment and be onsite. Any critical findings will be reported to management immediately. The final written report will be discussed in a face-to-face meeting.
b. The selected vendor will develop a testing plan that will utilize their experience in selecting appropriate controls for review.
c. The selected vendor will provide the State with the names of primary staff (including any sub-contractual work) assigned to the project. The state reserves the right to request changes to any staffing assignments.
d. The selected vendor will provide monthly documentation of work completed along with relevant invoicing.
e. The selected vendor will assure that assigned staff be trained in appropriate technical capacity.
f. The selected vendor must obtain approval from the State before conducting any automated scans or tests of controls.
g. The selected vendor is expected to conduct testing in accordance with NIST 800-53A and the deliverable results would be presented in a manner that is similar to a FedRAMP Security Assessment Test Case template found at: http://www.gsa.gov/portal/getMediaData?mediaId=155123, such that controls, gaps, and recommendations are categorized by MARS-E/NIST 800-53 control families.
h. The vendor will produce a formal written report to summarize the assessment results, including any necessary improvement recommendations.

Required Skills (to be scored as pass/fail)

The contractor/subcontractor must demonstrate the following:

- 7 Years of experience conducting security and compliance assessments, with at least one project that demonstrates familiarity with HIPAA and IRS rules as they impact data privacy and security, and subsequent HITECH legislation.
- Demonstrated experience in testing technical controls in Cisco networks, Window and UNIX operating systems, Oracle databases, and complex applications.
- Vendor must be familiar with NIST Certification and Accreditation processes and the NIST 800-53 family of controls.
- Vendor must have a Certified Information Systems Security Professional and Certified Information Systems Auditor members on the assessment team.

Desired Skills

- Familiarity with new Minnesota Insurance Marketplace (MNsure) regulations
- Familiarity with other federal mandates governing federal tax information and social security data.

Agency Contact

Questions about this SOW may be directed electronically no later than 12:00 PM CDT on July 10, 2013, to Barry Caplin
MN.IT Chief Information Security Officer for Department of Human Services
barry.caplin@state.mn.us
Questions and answers will be posted on the Office of Enterprise Technology website by approximately 12:00 PM CDT on July 11, 2013 (http://mn.gov/buyit/statements/mcp902ts_active.html).

Other persons ARE NOT authorized to discuss this SOW or its requirements with anyone throughout the selection process and responders should not rely on information obtained from non-authorized individuals. If it is discovered a Responder contacted other State staff other than the individual above, the responder’s proposal may be removed from further consideration.

The STATE reserves the right to determine if further information is needed to better understand the information presented. This may include a request for a presentation.

**Submission Format**

**Response Requirements**
The proposal should be assembled as follows:

**Cover Page:**
- Vendor Name
- Vendor Address
- Vendor City, State, Zip
- Contact Name for Vendor
- Contact’s direct phone
- Contact’s email
- Resource Name being submitted

**Overall Experience:**
1. Provide narrative, including companies and contacts where your resource has demonstrated the required skills noted above. If resource cannot demonstrate this background, the State reserves the right to discontinue further scoring of the proposal.
2. Points will also be awarded based on the desired skills noted above. Provide one paragraph which highlights the resource’s desired skills noted above.
3. Attach a resume(s) for proposed resource(s) in addition to the narrative description. Be certain the resume has dates of work and notes whether the resource was an employee or consultant.
4. Also include the name of ONE reference who can speak to the resources work on a similar project. Include the company name and address, reference name, reference email, reference phone number and a brief description of the project this resource completed.

This section of Overall Experience is worth 50% of the proposals total score.

**Project Approach and Outcome:**
Describe the approach vendor will take to execute this work and ensuring all completion of all deliverables or additional work as deemed appropriate. The Vendor will submit an overview of what will comprise the completed learning experience. Vendor should also submit a high level timeline for the work.
Remember to include any assumptions or requirements/responsibilities from/of State staff. Also include any best practices which would make this project successful that have not been mentioned in the deliverables. Please clearly delineate if additional work is being added to the scope so the cost may be analyzed appropriately.

This section of Project Approach and Outcome is worth 20% of the proposals total score.

Cost:
This contract will be Time and Materials. Based on the work described in the Project Deliverables section of this Statement of Work, show a final hours/best estimate of total cost for this project. Be sure and note any additional best practice work described in your Project Approach.

This section of Cost is worth 30% of the proposals total score.

State Forms
Include the following forms in the last section.

- Conflict of interest statement as it relates to this project
- Required forms to be returned or additional provisions that must be included in proposal
  1. Affirmative Action Certificate of Compliance (if over $100,000)
     http://www.mmd.admin.state.mn.us/doc/affaction.doc
  2. Affidavit of non-collusion
     http://www.mmd.admin.state.mn.us/doc/noncollusion.doc
  3. Certification Regarding Lobbying
     http://www.mmd.admin.state.mn.us/doc/lobbying.doc
  4. Veteran-Owned/Service Disabled Veteran-Owned Preference Form
     http://www.mmd.admin.state.mn.us/doc/vetpref.doc

DO NOT include marketing materials or any other information not requested.

Submission Information
All proposals must be sent by email to:
Agency: MN.IT Services
Name: Mark Mathison
Title: Information Risk and Compliance Manager
Address: mark.mathison@state.mn.us
Phone: 651.201.2792
Not later than 12:00 PM CDT, July 15, 2013, as indicated by the date and time recorded on the agency’s email clock.

The subject line shall read: MNSure Security Assessment
Late proposals as indicated by e-mail “Received” field will not be considered.

- The electronic submission must be in Adobe Acrobat PDF format.
- Cost proposals must be sent in a separate email with the same deadline, subject line: MNSure Security Assessment - Cost.
- The submitter must be an authorized member of the firm.
- Prices and terms of the proposal as stated must be valid for the length of any resulting contract. Hourly rates cannot exceed previously submitted as part of the 902TS Master Contract Program.

All material submitted in response to this SOW will become the property of the STATE and will become public record after the evaluation process is completed and an award decision is made. If the vendor submits information to this SOW that it believes to be trade secret materials, as defined by the Minnesota Government Data Practices Act, Minnesota Statutes 13.37, the vendor must:

a. Clearly mark all trade secret materials in its response prior to submission,
b. Include a statement with the response justifying the trade secret designation for each item, and
c. Defend any action seeking release of the materials it believes to be trade secret, and indemnify and hold harmless the STATE, its agents and employees, from any judgments awarded against the STATE in favor of the party requesting the materials, and any and all costs connected with that defense. This indemnification survives the State’s award of a contract. In submitting a response to this SOW, the vendor agrees that this indemnification survives as long as the trade secret materials are in possession of the STATE. The STATE is required to keep all the basic documents related to its contracts, including responses to SOW’s for a minimum of seven years.

The STATE does not consider the hourly rates and references submitted by vendors to be trade secret material.

Once submitted, all proposals constitute binding irrevocable offers to enter into a business relationship with the STATE for a period of 180 days. Acceptance of proposals shall occur upon final execution of a contract.

SOW Evaluation Process
Proposals will be evaluated as follows:

Overall Experience – 50%
Project Approach and Outcome – 20%
Cost – 30%

Target Dates
Project Schedule
The project is anticipated to begin on July 22, 2013. The project end date will depend on vendor proposals, however a completed pre-production assessment must be ready no later than August 21, 2013.
Process Schedule
Questions due Wednesday July 10, 2013 by 12:00PM CDT
Proposals due Monday, July 15, 2013, NOON CDT
Anticipated proposal evaluation begins Monday, July 15, 2013
Anticipated decision Thursday, July 18, 2013

This Statement of Work does not obligate the State to award a work order or complete the assignment and the State reserves the right to withdraw or cancel this Statement of Work any time prior to the decision to engage the selected vendor. The State also reserves the right to reject any and all proposals.

General Requirements

Proposal Contents
By submission of a proposal, Responder warrants that the information provided is true, correct and reliable for purposes of evaluation for potential award of a work order. The submission of inaccurate or misleading information may be grounds for disqualification from the award as well as subject the responder to suspension or debarment proceedings as well as other remedies available by law.

Liability
Each party will be responsible for its own acts and behavior and the results thereof. The Minnesota Torts Claims Act, Minn. Stat. § 3.736 and other applicable laws govern the State’s liability.

Disposition of Responses
All materials submitted in response to this SOW will become property of the State and will become public record in accordance with Minnesota Statutes, section 13.591, after the evaluation process is completed. Pursuant to the statute, completion of the evaluation process occurs when the government entity has completed negotiating the contract with the selected vendor. If the Responder submits information in response to this SOW that it believes to be trade secret materials, as defined by the Minnesota Government Data Practices Act, Minn. Stat. § 13.37, the Responder must: clearly mark all trade secret materials in its response at the time the response is submitted, include a statement with its response justifying the trade secret designation for each item, and defend any action seeking release of the materials it believes to be trade secret, and indemnify and hold harmless the State, its agents and employees, from any judgments or damages awarded against the State in favor of the party requesting the materials, and any and all costs connected with that defense. This indemnification survives the State’s award of a contract. In submitting a response to this RFP, the Responder agrees that this indemnification survives as long as the trade secret materials are in possession of the State.

The State will not consider the prices submitted by the Responder to be proprietary or trade secret materials.
Conflicts of Interest

Responder must provide a list of all entities with which it has relationships that create, or appear to create, a conflict of interest with the work that is contemplated in this request for proposals. The list should indicate the name of the entity, the relationship, and a discussion of the conflict.

The responder warrants that, to the best of its knowledge and belief, and except as otherwise disclosed, there are no relevant facts or circumstances which could give rise to organizational conflicts of interest. An organizational conflict of interest exists when, because of existing or planned activities or because of relationships with other persons, a vendor is unable or potentially unable to render impartial assistance or advice to the State, or the vendor’s objectivity in performing the contract work is or might be otherwise impaired, or the vendor has an unfair competitive advantage. The responder agrees that, if after award, an organizational conflict of interest is discovered, an immediate and full disclosure in writing must be made to the Assistant Director of the Department of Administration’s Materials Management Division (“MMD”) which must include a description of the action which the contractor has taken or proposes to take to avoid or mitigate such conflicts. If an organization conflict of interest is determined to exist, the State may, at its discretion, cancel the contract. In the event the responder was aware of an organizational conflict of interest prior to the award of the contract and did not disclose the conflict to MMD, the State may terminate the contract for default. The provisions of this clause must be included in all subcontracts for work to be performed similar to the service provided by the prime contractor, and the terms “contract,” “contractor,” and “contracting officer” modified appropriately to preserve the State’s rights.

IT Accessibility Standards

Deliverables and services performed as a result of this solicitation must comply with the Minnesota IT Accessibility Standards effective September 1, 2010, which entails, in part, the Web Content Accessibility Guidelines (WCAG) 2.0 (Level AA) and Section 508 Subparts A-D which can be viewed at:

http://www.mmd.admin.state.mn.us/pdf/accessibility_standard.pdf

Nonvisual Access Standards

Nonvisual access standards require:

1. The effective interactive control and use of the technology, including the operating system, applications programs, prompts, and format of the data presented, are readily achievable by nonvisual means;
2. That the nonvisual access technology must be compatible with information technology used by other individuals with whom the blind or visually impaired individual must interact;
3. That nonvisual access technology must be integrated into networks used to share communications among employees, program participants, and the public; and
4. That the nonvisual access technology must have the capability of providing equivalent access by nonvisual means to telecommunications or other interconnected network services used by persons who are not blind or visually impaired.
**Veteran-Owned Preference**

In accordance with Minn. Stat. § 16C.16, subd. 6a, (a) Except when mandated by the federal government as a condition of receiving federal funds, the commissioner shall award up to a six percent preference on state procurement to certified small businesses that are majority-owned and operated by:

1. recently separated veterans who have served in active military service, at any time on or after September 11, 2001, and who have been discharged under honorable conditions from active service, as indicated by the person's United States Department of Defense form DD-214 or by the commissioner of veterans affairs;
2. veterans with service-connected disabilities, as determined at any time by the United States Department of Veterans Affairs; or
3. any other veteran-owned small businesses certified under section 16C.19, paragraph (d).

In accordance with Minn. Stat. § 16C.19 (d), a veteran-owned small business, the principal place of business of which is in Minnesota, is certified if it has been verified by the United States Department of Veterans Affairs as being either a veteran-owned small business or a service disabled veteran-owned small business, in accordance with Public Law 109-461 and Code of Federal Regulations, title 38, part 74.

To receive a preference the veteran-owned small business must meet the statutory requirements above by the solicitation opening date and time.

If you are claiming the veteran-owned preference, attach documentation, sign and return the Veteran-Owned Preference Form with your response to the solicitation. Only eligible veteran-owned small businesses that meet the statutory requirements and provide adequate documentation will be given the preference.

**Foreign Outsourcing of Work Prohibited**

All services under this contract shall be performed within the borders of the United States. All storage and processing of information shall be performed within the borders of the United States. This provision also applies to work performed by subcontractors at all tiers.