

# **IT Professional Technical Services Master Contract Program T#:902TS**

## **Statement of Work (SOW) For Technology Services Issued By**

**Public Employees Retirement Association of Minnesota**

**Project Title: Web Application Security Assessment Report**

**Service Category: Network (Data, Video, Voice) - Security**

### **Business Need**

PERA collects demographic information and payment information from hundreds of thousands of public employees, both while they are working and then while they are retired and receiving a pension benefit. For that reason, our databases hold a large amount of private data. We need to ensure that private data remains secure. In order to do that, we occasionally contract with an outside vendor to attempt to “hack” into our systems. PERA is in need of a vendor who can assess the vulnerability of our web applications.

### **Project Deliverables**

Deliverables will include the following:

- Web application vulnerability report that includes tests run, vulnerabilities found, implications, severity or risk level, and specific recommendations for remediation;
- An on-site presentation to present findings and recommendations to PERA;
- A meeting with PERA IT staff to transfer knowledge about tests that PERA could/should be running on a regular basis to assess the vulnerability/security of our web applications.
- Critical vulnerabilities will be communicated to PERA immediately.

### **Project Milestones and Schedule**

- May 1, 2012 Project Start Date
- May, 2012 Meet with agency, develop schedule, run vulnerability assessment
- June 15, 2012 Written report is due, meet with agency to discuss results.
- June 30, 2012 Project is complete

### **Project Environment (State Resources)**

Members and employers are able to access and change private information through our three web portals. They should, however, only be able to access their own data. Those who are not members/employers should not be able to access any of our data via our web portals. PERA will have a team available to work with the vendor as attempts are made to access data from the outside. The team will include our network administrator, our security engineer, our application architect, our application development supervisor, and the Assistant Director, who manages the IT division.

## Agency Project Requirements

PERA will ask the vendor to first attempt to access our data as an unauthenticated, unauthorized entity anonymously accessing the application, and then as a fully authenticated and authorized user of the applications. Both tests will be run on all three of our web applications. Various checks will be performed to identify weaknesses within the application or infrastructure that the applications depend on. The vendor will attempt to gather information about hosting servers, applications and their dependencies, and databases containing private data, and use that information to discover weaknesses within the applications and/or infrastructure.

## Responsibilities Expected of the Selected Vendor

The selected vendor is expected to work with PERA staff to set up the testing scenarios, then work offsite to run the various tests. Any critical findings will be reported to PERA immediately. The final written report will be discussed in a face-to-face meeting, and information about best practices in security assessments will be shared with PERA's IT team.

## Required Skills

Required minimum qualifications:

- 5 Years of experience conducting security assessments
- Vendor must have a Certified Information Systems Security Professional member on the assessment team.

## Process Schedule

- |  |                     |
|--|---------------------|
| • Deadline for Questions                     | 4/20/2012, 12:00 PM |
| • Anticipated Posted Response to Questions   | 4/20/2012, 1:30 PM  |
| • Proposals due                              | 4/25/2012, 1:30 PM  |
| • Anticipated proposal evaluation begins     | 4/26/2012           |
| • Anticipated proposal evaluation & decision | 4/27/2012           |

## Questions

Any questions regarding this Statement of Work should be submitted via mail or e-mail by 04/20/2012, Time: Noon

Name: Dave DeJonge

Department: PERA

Address: 60 Empire Drive, Suite 200, St. Paul, MN 55103

Telephone Number: (651) 201-2641

Email Address: dave.dejonge@mnpera.org

Questions and answers will be posted on the Office of Enterprise Technology website by approximately 1:30 on 4/20/12 ([http://www.oet.state.mn.us/mastercontract/statements/mcp902ts\\_active.html](http://www.oet.state.mn.us/mastercontract/statements/mcp902ts_active.html)).

## SOW Evaluation Process

All responses must be received by April 25, 2012 at 1:30 PM and will be evaluated on a "best value" basis with the following percentages:

- Company (15%)
- Experience and knowledge of proposed project staff with web application security assessments (30%)
- Work Plan (25%)
- Cost (30%)

**Statement of Work does not obligate the state to award a work order or complete the assignment, and the state reserves the right to cancel the solicitation if it is considered to be in its best interest. The Agency reserves the right to reject any and all proposals.**

# Response Requirements

Responses must include the following:

1. **Introduction** identifying respondent and respondent's representative during the procurement process (contact information).
2. **Company Overview** providing the company's history, growth, and experience providing web application vulnerability assessments to other agencies and/or entities. Please include a sample web application vulnerability report issued by the vendor.
3. **Experience of Personnel Assigned.** The response must outline the experience of the personnel assigned to this project in developing web application vulnerability reports, running network security assessments, and communicating the results to clients. Include a resume for each person who will be conducting the security assessment. In addition, include information about any applicable certifications earned by the personnel assigned to this project.
4. **Project Work Plan.** This section should demonstrate the vendor's understanding of the services requested in the Statement of Work and any problems anticipated in accomplishing the work; show the overall design plan for achieving the results outlined in the Statement of Work including a timeline for accomplishing the work; provide a list of various tools and tests that will likely be used to develop the assessment; and provide a detailed project approach, including organization and staffing, change management procedures, and status reporting.
5. **Cost Proposal** for the project including all project costs, not to exceed \$25,000.
6. **Affidavit of Non-Collusion** must be included. The form is found at the following URL: <http://www.mmd.admin.state.mn.us/doc/noncollusion.doc>

# Proposal Submission Instructions

- Response Information:
  - a) Responses should be addressed to Dave DeJonge, PERA's Assistant Director.
  - b) Responses should be submitted via email to [dave.dejonge@mnpera.org](mailto:dave.dejonge@mnpera.org) by April 25 at 1:30 PM CST.

# 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 this 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

### Indemnification

In the performance of this contract by Contractor, or Contractor's agents or employees, the contractor must indemnify, save, and hold harmless the State, its agents, and employees, from any claims or causes of action, including attorney's fees incurred by the state, to the extent caused by Contractor's:

- 1) Intentional, willful, or negligent acts or omissions; or
- 2) Actions that give rise to strict liability; or
- 3) Breach of contract or warranty.

The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the State's sole negligence. This clause will not be construed to bar any legal remedies the Contractor may have for the State's failure to fulfill its obligation under this contract.

## **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**

Responses to 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](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.

### **Preference to Targeted Group and Economically Disadvantaged Business and Individuals**

In accordance with Minnesota Rules, part 1230.1810, subpart B and Minnesota Rules, part 1230.1830, certified Targeted Group Businesses and individuals submitting proposals as prime contractors shall receive the equivalent of a six percent preference in the evaluation of their proposal, and certified Economically Disadvantaged Businesses and individuals submitting proposals as prime contractors shall receive the equivalent of a six percent preference in the evaluation of their proposal. Eligible TG businesses must be currently certified by the Materials Management Division prior to the solicitation opening date and time. For information regarding certification, contact the Materials Management Helpline at 651.296.2600, or you may reach the Helpline by email at [mmdhelp.line@state.mn.us](mailto:mmdhelp.line@state.mn.us). For TTY/TDD communications, contact the Helpline through the Minnesota Relay Services at 1.800.627.3529.

### **Veteran-owned/Service Disabled Veteran-Owned Preference**

In accordance with Minnesota Statute §16C.16, subd. 6a, veteran-owned businesses with their principal place of business in Minnesota and verified as eligible by the United States Department of Veterans Affairs' Center for Veteran Enterprises (CVE Verified) will receive up to a 6 percent preference in the evaluation of its proposal.

Eligible veteran-owned small businesses include CVE verified small businesses that are majority-owned and operated by either recently separated veterans, veterans with service-connected disabilities, and any other veteran-owned small businesses (pursuant to Minnesota Statute §16C.16, subd. 6a).

Information regarding CVE verification may be found at <http://www.vetbiz.gov>.

Eligible veteran-owned small businesses should complete and sign the Veteran-Owned Preference Form in this solicitation. Only eligible, CVE verified, veteran-owned small businesses that provide the required documentation, per the form, will be given the preference. The form is found at the following URL:

<http://www.mmd.admin.state.mn.us/doc/vetpref.doc>