

# Request for Offers (RFO) Addendum

RFO Number: RFO0136

Addendum Number: 1

Date of Addendum: 08/05/16

Original Posting Due Date, Time: 08/12/2016, 3PM CST

Revised Due Date, Time: N/A

Title: Web Vulnerability Assessment

## SCOPE OF ADDENDUM

The following are changes to the RFO: Modifying the Project Deliverables section of the RFO and posting answers to the questions received on the RFO. In this Addendum, changes to pre-existing RFO language will use ~~strike through~~ for deletions and underlining for insertions.

### Modifying the Project Deliverables Section:

The project will include the following tasks:

- Vulnerability scan (automated) of OSS websites and all public facing applications.
- Manual testing of OSS websites and all external applications for vulnerability assuming a motivated attacker or better.
- Internal vulnerability assessment (manual and automated) of the OSS environment in order to discover any vulnerability not associated with known applications, network, servers, etc.
- Identification and confirmation of false positives from the vulnerability scan.

Deliverables:

1. Completed web application security test performed according to the plan agreed upon by OSS and the selected vendor.
2. Final report including the following:
  - a. Executive summary
  - b. Identification of potential exposures and vulnerabilities for the network; websites and web applications; internal, external, and physical security. Report should identify application-specific vulnerabilities in addition to overall network vulnerabilities.
  - c. Severity of each vulnerability.
  - d. How each vulnerability was found – manual or automated and if automated what tool was used.
  - e. Analysis of each vulnerability found as a result of scanning using an automated tool to ensure it is not a false positive.
  - f. Recommendations for remediation of each vulnerability including prioritization of proposed actions, and approximate costs if known.
  - g. Recommendations for enhancing the security of the entire network.
3. Up to 16 hours (clock time) on site at OSS of meetings for planning, questions, and the reviewing of findings.
4. Up to 16 hours (clock time) for training. This can be done on site or via remote conferencing. The content and audience for the training will depend on the findings of the assessment. Training will

SITE RFO Addendum

Rev. 3/16

be targeted towards specific issues found during the assessment and will not need to include a formal curriculum or certification of those being trained.

## **Posting Answers to Questions Received**

The Minnesota Office of the Secretary of State received questionnaires from 12 vendors in response to the posting of RFO0136. Questions were sent in a variety of custom formats including bulleted lists, multiple choice, and spreadsheets. Many of the same questions were asked by multiple vendors with slightly different wording. In an effort to keep the official response comprehensible and concise, overlapping questions have been combined and reworded. Care was taken to respond to the root concerns across all questions.

## **External Application Assessment**

### **Q: How many data fields are present across the applications?**

A: There are approximately:

- 650 unauthenticated / public facing fields total across all applications
- 2500 authenticated fields total across all applications

NOTE: We intend the web application testing to be done as an unauthenticated / public user

### **Q: Describe the data sources used by the applications**

A: All applications use Microsoft SQL Server 2014 or greater for data storage.

### **Q: How many user roles are present in each application**

A: See the “# of Roles” column in the [application matrix](#) spreadsheet.

Notes:

We are not expecting a vulnerability scan for each role – just a scan as an unauthenticated user. The number of roles listed in the spread sheet does not include “unauthenticated” in the tally.

### **Q: How many pages are there in each application?**

A: Please see the “Approx Total # of Pages” column in the [application matrix](#) spreadsheet.

### **Q: You mention “other applications.” Besides the eight (8) identified applications, how many others will be included in the project?**

A: The RFO lists the applications in a conceptual manner. There are actually 11 websites and 3 web services in the mix for this project. See the [application matrix](#) spreadsheet for the complete listing of discrete applications.

### **Q: How many web service endpoints?**

A: Approximately 15. All require authentication.

### **Q: Do your web services have test harnesses?**

A: They have code-only development test harnesses, but none that could be used in this context.

### **Q: How many AJAX/Service calls are being used?**

A: We estimate that less than 25% of our pages use ajax. This would be less than 160 or so for all unauthenticated pages.

### **Q: What are the URLs for the applications?**

A: Please see the [application matrix](#) spreadsheet for a list of URLs.

NOTES:

Some URLs have access control mechanisms and may not be reachable.

The Commissions and Appointments application is not in production yet, but is on track to be available when the project gets underway.

**Q: What technologies & frameworks are your applications using**

A: Please see the [application matrix](#) spreadsheet for per application details, but in general our web sites are using ASP.NET Webforms or ASP.NET MVC. Our services are a mix of WCF (SOAP), ASMX (SOAP), and XML over raw HTTP. All services are hosted in ASP.NET. Additionally, the web applications often use client side frameworks such as jQuery and Bootstrap.

**Q: What protocols do the applications use?**

A: HTTP for browser to app communication. HTTP for web service communication. TCP for database communication.

**Q: Do any applications use two-factor or multi-factor authentication.**

A: No

**Q: How many internet facing live hosts are in scope**

A: roughly 65 at the time of writing. We are virtualized so the exact number is always in flux. The number should still be in the same ballpark by the time the project is underway.

**Q: Are any applications hosted or managed by 3<sup>rd</sup> parties?**

A: MNIT provides the agency with internet and data center services, but the applications are all hosted and managed by the MN Secretary of State's IT team. There are no other 3<sup>rd</sup> parties involved.

**Q: Does a current network diagram exist?**

A: No

**Q: Does a data flow diagram exist?**

A: No

**Q: How many lines of code (or best guess) are in the websites to be tested?**

A: We estimate the entire codebase to be in the range of 280,000 to 470,000 LoC. The [application matrix](#) spreadsheet lists LoC for each app using Visual Studio's built in code metrics feature. However, this does not count code in the database, nor does it count HTML, JavaScript, or server-side code mixed in with HTML templates. Note: a code review is not in the scope of this project.

**Q: The RFO is not clear on the level of depth expected when assessing the websites. Is network level testing expected or is web application testing also expected. If web application testing is expected, is this credentialed or testing without credentials?**

A: We would like both network scanning and web application testing. Web application testing would be done as an unauthenticated user without credentials.

**Q: What is the total number of in scope active External IP addresses?**

A: Approximately 40.

**Q: What is the total number of Web sites with <1,000 total pages and <10 user input pages for Web Application Testing?**

A: Two when only considering unauthenticated pages.

**Q: What is the total number of Web sites with <5,000 total pages and <40 user input pages for Web Application Testing?**

A: 11 including the two mentioned in the previous answer.

**Q: Will the scope of testing include the Production and Quality Assurance (QA) environments?**

A: The external testing will be done against production, unless we decide we need a different environment as a result of our planning meetings. We do not need to test the applications in other environments otherwise.

**Q: Does that State require source code review for website applications?**

A: No. Source code review is not in scope.

**Q: Is testing to be performed at the State or can be performed offsite for website application testing?**

A: The external application testing needs to originate outside of the state network.

**Q: Which of the following statements best describes your PERIMETER (i.e. Internet facing or external) network and other remote testing objectives? a. A perimeter vulnerability assessment designed to identify the potential security concerns throughout the environment using a variety of tools and manual techniques, but no direct exploitation. b. A perimeter comprehensive penetration test in which in-depth testing of the perimeter network and actively exploit and penetrate systems and applications. c. No network level assess will be necessary against the perimeter network. Only application level testing will be required.**

A: Primarily "A," but there could be some of "B." This would need to be hammered out in planning meetings.

**Q: Which of the following statements that best describes your Web Application testing objectives? a. Path of least resistance testing against the applications during standard pen testing. Manual and automated techniques will be employed from an unauthenticated perspective to find entry points into the system, but will focus on finding a path in and not on total coverage of the application. b. An assessment of the applications with a strong reliance on automated tools. Manual testing will still be included, but will focus on false positive removal and high level application flaws. c. A deep look into the application from a manual perspective. Time will be spent understanding application and the specific threats that it exposes.**

A: "A"

## **Internal Vulnerability Assessment**

**Q: How many servers, workstations, network printers, network switches, and endpoint devices are included in the internal vulnerability assessment?**

A:

- 215 active servers (mix of virtual and physical – this number includes the internet facing hosts mentioned earlier)
- 173 workstations
- 7 Network printers
- 24 switches
- 2 firewall / load balancer appliances
- 5 fiber / SAN switches
- 2 Security / Intrusion Detection appliances

NOTE: The server and Workstation numbers are always in flux but should still be around these numbers when the project gets underway.

**Q: Do you have any BMS / ICS devices present? (Building management, HVAC etc...)**

A: No

**Q: How many assets/systems/data are in scope to be assessed?**

A: The internal assessment would not be targeted towards any systems in particular other than the environment as a whole including aforementioned internal only and externally facing hosts.

**Q: Are any of the targets considered to be critical and nature or perhaps running delicate legacy software/applications?**

A: Yes. We would need to work with the awarded vendor on operating parameters for the internal assessment.

**Q: What do you consider as the most safeguarded data?**

A: This would vary by business unit, but in general it would be any data deemed "private" by state statute or internal policy. We would be willing to clarify this with the awarded vendor.

**Q: Does a current network diagram exist?**

A: No

**Q: Does a data flow diagram exist?**

A: No

**Q: Does network segmentation exist?**

A: Yes

**Q: What is the total number of in scope internal Class C Networks?**

A: Approximately 10

**Q: The RFO states that the you have two locations and that each location needs to be assessed. Can one location be reached from the other across the network? Or, is it permissible to conduct all test activities from one location?**

A: Yes, both locations can access each other and share the same network segmentation. We would want some testing done from both locations. Exact details would have to be hammered out during the project kickoff.

**Q: What is the total number of in scope active internal IP addresses?**

A: Approximately 300

**Q: If unsure about the specific IP targets OR if the number of IP addresses to test is large (e.g. over 100), is sampling acceptable?**

A: Yes

**Q: Would you like us to perform Internal Testing as an Unauthorized User from outside the network?**

A: Yes

**Q: Would you like us to perform Internal Testing Onsite as a Trusted User with access to the network?**

A: Yes. We would hammer out operational parameters during planning meetings. You should estimate for up to 3 different levels of privilege (such as clerical staff, management, super-user, etc...) in addition to the unauthorized scenario.

**Q: 3. Which of the following statements that best describes your INTERNAL network and other onsite testing objectives? a. An internal vulnerability assessment designed to identify the potential security concerns throughout the environment using a variety of tools and manual techniques, but no direct exploitation. b. An internal comprehensive penetration test in which in-depth testing of the perimeter network and actively exploit and penetrate systems and applications.**

A: Primarily "A," but there could be some of "B." This would need to be hammered out in planning meetings.

**Q: For internal assessments, can all IP addresses being tested be reached from a single internal network port?**

A: Yes

**Q: Are you also requesting an internal security assessment of the two locations (on-site with a review of policies, architecture, etc.)?**

A: Some of the actual penetration testing should occur from both locations. Review of policies, network architecture would only occur at one location.

## **Social Engineering and Physical Security**

**Q: How many locations are in scope?**

A: 2 buildings / 3 office spaces (One of the locations has two office spaces occupied by the agency)

**Q: Is email phishing in scope for this project? How many users are being targeted? How many campaigns?**

A: Yes. 76 users are in scope. We want a minimum of one campaign but would be open to more if the vendor advises additional campaigns.

**Q: Is telephone impersonation in scope for this project? How many users are being targeted? How many campaigns?**

A: Yes. 76 users are in scope. We want a minimum of one campaign but would be open to more if the vendor advises additional campaigns.

**Q: Are USB (media) drops in scope for this project? How many locations?**

A: Yes - 3 office spaces across two buildings

**Q: Would you like us to attempt to gain physical access to any facilities or assets? How many locations?**

A: Yes - 3 office spaces across two buildings

**Q: Which of the following statements that best describes your physical security testing objectives? a. Physical Facility Penetration Test – Attempt to gain unauthorized access through magnetically sealed doors, physical key locks, ventilation, etc. b. Physical Security Threat Assessment - Consultants will perform a walkthrough accompanied by client personnel from the perspective of an attacker and examine physical points of entry and internal security controls for weaknesses or vulnerabilities of the in-scope facilities.**

A: Both are considered in-scope.

## **General**

**Q: Are you seeking an individual resource, a team, or specialized company to perform web application security testing?**

A: We are seeking a specialized company to co-run the project along with a small team of agency stakeholders. We are not expecting our agency to manage individual resources provided by a vendor.

**Q: How many resources can be submitted to this RFO?**

A: The RFO does not indicate a high or low limit on the number of resources that may be submitted. Therefore, it is up to each vendor to assess how many resources it deems are necessary for the project.

**Q: One of the evaluation requirements is an application security test plan, is there a guide or preferred format to present the information?**

A: No, the presentation of this information is at the vendor's discretion.

**Q: Regarding mandatory qualifications: Is it required that we submit documentation of formal testing procedures for common vulnerabilities such as OWASP and social engineering along with the proposal (thus making them available to the public) or can they be submitted after receipt of an award?**

A: This needs to be part of the initial submission. However, we do not need implementation details of the procedures included. An overview of the types of testing you would do and common vulnerabilities you would look for would suffice.

**Q: Proposal states the vendor will need to us an automated tool to do part of the assessment. Does the State provide an already established tool or does the vendor choose?**

A: The vendor will provide tooling.

**Q: For a sample report, we need an NDA first and then can only show them via WebEx and cannot include the redacted report in the submission. Will this work for MNIT?**

A: No this will not work. We would allow for a fully anonymized or fabricated report as long as it illustrated

what the end report would be like. However, we cannot sign an NDA or meet with the vendor as part of the awarding process.

**Q: You want 5 examples of similar assessments. We do not share our customer's information, nor do we say what we did for them. We would not be able to meet this requirement as stated and would need further clarification of what they are looking for in this area.**

A: We would allow for the five examples to be completely anonymous. For example, it could be presented as for a "Fortune 500 Company" rather than naming the client. However, the corporate references needed for the project plan cannot be anonymous.

**Q: Will the State consider changing the liability language to Version 4 or negotiate with vendors on this topic prior to award?**

A: No

**Q: Are there any "out of bounds" systems and/or operations? Are there any direct interfaces with mission critical systems that would require additional care that could impact the systems in scope? Are there critical hours / dates that should be considered in evaluating the timing of testing?**

A: Yes. In general, we will not be disrupting the service level to our end users or our internal staff. We also would like to avoid putting data into systems without a way to clean it out after testing. A set of operational guidelines will need to be hammered out during kickoff and planning meetings.

**Q: Training of OSS staff is not listed in the deliverables. It is listed as a project requirement. Could you please clarify this requirement and whether you want to include training as a deliverable? What types of people need to be trained (technical, general user, etc.)?**

A: The RFO did not specifically include training as a deliverable; as a result of these Questions and Answers/Addendum, training is hereby included as a deliverable with a cap of up to 16 clock hours of training. The actual content, amount of training, and what audiences are involved would depend on the outcome of the assessments. This would be more of a targeted follow-up activity rather than a formal curriculum.

**Q: Has the OSS had this scope of services performed in the past, and can those reports be shared with the winning bidder?**

A: Yes, the agency went through a similar project in 2008 minus the physical and social engineering aspects. At this point in time we don't believe we can legally share a copy of the report without the permission from the vendor, but we would be able to recap the findings.

**Q: Is the State looking to have the vendor to assure/certify the security state of election related data?**

A: No

**Q: How many employees are in your organization?**

A: Approximately 90

This addendum shall become part of the RFO and should be returned with, or acknowledged in, the response to the RFO.

RESPONDER NAME:

SIGNATURE:

TITLE:

DATE: