

**State of Connecticut
Department of Information Technology**

**Web Application and Web Service Vulnerability Assessment
Tool**

RFI #10ITZ0079

AMENDMENT # 1

provides the following:

- Vendor Question and Answer document

Note: A signature line has been included below. A copy of this page signed in ink is required with the Proposal to show that vendors have received this Amendment.

VENDOR'S SIGNATURE ACKNOWLEDGING RECEIPT

(This page should be signed and returned WITH PROPOSAL. If vendor fails to submit signed Amendment, vendor will still be responsible for adhering to its content)

APPROVED:_____

JACQUELINE SHIRLEY
DIRECTOR
IT CONTRACTS AND PURCHASING DIVISION

RFI - #10ITZ0079
Question and Answers

The following questions were received regarding the RFI referenced above. Answers are provided below the question.

- 1. Q.** Is the State interested in a service based offering or would the State prefer to purchase a product to do this?

A. The State is interested in purchasing a tool for this function. The State is not interested in a service based offering.
- 2. Q.** Is there an opportunity to talk with the State about the solution needed? Either directly or in a bidders conference?

A. As this is a request for information, there is no bidders' conference. When the State decides on a proper course of action regarding this tool, the appropriate venue for interaction with vendors may be provided.
- 3. Q.** As far as the printed copies to be airmailed are concerned, is the following an accurate understanding of what vendors should send to the State: 1 (one) - Original + 4 (four) copies + 1 (one) CD-R with recorded material (or should one CD-R for each set, totaling 5 (five) CDs be sent?).

A. One electronic copy of the response should be provided with each printed copy of the response, so the total would be 5 (five) electronic copies, one with each of the printed copies.
- 4. Q.** Would the State prefer that the offered product be via annual subscription or perpetual license?

A. The State prefers perpetual licensing for the product with an annual maintenance subscription for updates and support.
- 5. Q.** Is the State interested in a desktop tool single power users or a web based platform built for the entire organization?

A. The intended usage model is detailed in section 4.2 of the RFI document.

STATE OF CONNECTICUT

RFI-#10ITZ0079

Department of Information Technology

Request for Information

For

Web Application and Web Service Vulnerability Assessment
Tool

Issue Date:

August 20, 2010

Question Deadline Date:

September 3, 2010, @ 5:00 P.M. EST

Response Deadline:

September 17, 2010, @ 2:00 P.M. EST

Issued by:

Department of Information Technology
101 East River Drive
East Hartford, CT 06108

1	REQUIREMENTS AND DEADLINES FOR QUESTIONS AND RESPONSES.....	3
2	RESPONSES TO RFI	3
2.1	Scope of RFI	3
2.2	Quality of Responses.....	3
2.3	Product and Service Availability.....	4
3	BACKGROUND.....	4
4	INFORMATION REQUIRED	4
4.1	Web Application and Service Vulnerability Analysis Tool	4
4.2	Usage	5
6.	FREEDOM OF INFORMATION ACT	6

1 REQUIREMENTS AND DEADLINES FOR QUESTIONS AND RESPONSES

This Request for Information (RFI) outlines the information being solicited from vendors and includes guidelines for content and format of responses. From this RFI's issuance date of August 20, 2010 vendors choosing to respond will have **two weeks** to respond with questions and **four weeks** to submit their completed written responses. Responses must be submitted no later than 2:00 pm EST on September 17, 2010.

All questions must be in written form, submitted using electronic mail and addressed to

marc.daloisio@ct.gov

Written questions must be submitted no later than 5:00 pm EST on September 3, 2010.

Late responses may or may not be considered, and the Department of Information Technology will determine this. The postal address for RFI responses is:

Marc D'Aloisio
State of Connecticut
Department of Information Technology
101 East River Drive
East Hartford, CT 06108

Parties desiring to respond to this RFI must do so in writing, providing one original and four complete copies of the submitted response. Please include an electronic copy with the original and each of the written copies. Responses will be reviewed by the agency and, depending on the results of that review, additional information or product/service demonstrations may be requested. No contract will result directly from this RFI. Following the review of submitted information, the Department of Information Technology (DOIT) will determine the best course of action. This RFI process is intended to help DOIT research a variety of available services so that DOIT can determine the best strategy for the State.

2 RESPONSES TO RFI

2.1 Scope of RFI

Responses to this RFI will be used by the State to gather company, and product information from vendors with the capability of providing a web application and web service vulnerability analysis tool. No contract will result directly from the RFI process. The responses to this RFI will be used to determine whether an RFP should be issued.

2.2 Quality of Responses

Well-organized and concise responses are encouraged in order to facilitate the State's assessment. Responses must follow the same order as this RFI document and utilize the same section numbering system.

2.3 Product and Service Availability

The State expects that the system and services described in response to this request for information are generally available as of the date that responses are due. Responders must explain any exceptions.

3 BACKGROUND

The State of Connecticut Department of Information Technology regularly conducts risk assessments related to various State information technology systems. These risk assessments serve to identify and evaluate the security posture of these systems in order to quantify and qualify compliance to various State and Federal requirements. One part of a risk assessment involves the identification of vulnerabilities within and exposed by the target of evaluation.

As more systems become web enabled, it is necessary to identify and evaluate vulnerabilities in the web applications and web services that these systems expose for interface to users and other systems.

4 INFORMATION REQUIRED

Each of the following paragraphs in this section should be acknowledged and answered. Thorough answers that address all points are expected. Responses should clearly address both transitional and ongoing issues.

4.1 Web Application and Service Vulnerability Analysis Tool

Responses to this RFI must include the following information relative to web application and service vulnerability assessment tools:

1. What features make your product the best product for web application and web service vulnerability assessment?
2. What web technologies/environments does your product support (analyze)?
3. Is your product capable of analyzing web services? Please describe this capability.
4. Is your product capable of static code analysis? If so, what technologies/languages?
5. Please describe how your product spiders a web application and its capabilities to discover hidden items or content.
6. Please describe to what standards your product analyzes and reports to, what pre-configured policies are included, and capability to create custom policies within the product.
7. Please describe from what sources patterns for the testing and identification of vulnerabilities are derived.
8. Does the product have a method for the user to create and use custom tests? Please describe this capability, if it exists, including APIs, interfaces, etc/

9. Please describe how your product reduces false positives and false negatives. Please provide any available metrics on false positives and negatives reported by your product.
10. Please describe the update procedure for your product. Is it automatic? Approximately how often are updates available?
11. Does your product incorporate a fuzzing capability? Is it automatic, manual, or both?
12. Please describe the licensing models for your product.
13. Please describe how your product stores, and makes available for reuse, previous scans. What database technology is used? Is it included with the product?
14. What are the system and architecture requirements for your product?
15. Is your product SCAP compliant - has it been validated by the NIST SCAP Validation Program to the current effective version of SCAP?
16. Please describe the reporting capabilities of your product. What formats and layouts are provided / supported? Are reports customizable? If so, how?
17. Does your product perform analysis and provide reports relative to Federal regulatory requirements such as HIPAA, IRS 1075, and SSA?
18. Please supply the LIST prices of your product for initial purchase and license renewals
19. Please describe the availability, cost, and logistics of training related to your product.

4.2 Usage

While State contracts have language regarding licensing, the following explains, for licensing purposes, how we intend to use the product.

The Information Technology Security Division (ITSD) employs approximately twelve people. For vulnerability assessment, we have five dedicated laptop computers on which we install various tools and software we use. These laptops are available to any of the twelve (but usually a core group of four) individuals for use as needed. The web application vulnerability analysis tool may be licensed for, and installed on, one or more of the five laptops for use by Division personnel as needed.

This information is furnished to help respondents provide relevant information with regard to number 12 of item 4.1 above.

5. DISCLAIMERS

The Department is asking for responses to this RFI for informational purposes only and will not be obligated in any way to use any of the information received. Vendors responding to this RFI will not be compensated in any way. Also, responding to this RFI will not enhance any vendor's chances of receiving future work from the State. Similarly, not responding to this RFI will not be a detriment to any vendor when competing for future work.

All RFI responses submitted by vendors will become the property of the State of Connecticut.

6. FREEDOM OF INFORMATION ACT

Due regard will be given for the protection of proprietary information contained in all proposals received; however, vendors should be aware that all materials associated with the procurement are subject to the terms of the Freedom of Information Act (FOIA) and all rules, regulations and interpretations resulting there from. It will not be sufficient for vendors to merely state in general terms that the proposal is proprietary in nature and, therefore, not subject to release to third parties. Any proposal that makes such a general or overarching claim may be subject to disqualification. **Those particular sentences, paragraphs, pages or sections which a vendor believes to be exempt from disclosure under the Act must be specifically identified as such.**