

Request for Information

for

Vulnerability Assessment and Discovery Service

for

Consolidated Technology Services

A16-RFI-184

Issued: June 1, 2016

1) SUBJECT

This Request for Information (RFI) is seeking information about a solution to be the core infrastructure for the service of Vulnerability Assessment and Discovery. We are requesting that vendors ensure that the responses provided can meet the requirements identified by Washington State Consolidated Technology Services (CTS), doing business as Washington State Technology Services (“WaTech”).

2) RESPONSES DUE

We are requesting that vendors respond with any preprinted materials that would provide the information we request, and short answers to the questions listed in the criteria section of this RFI.

Please provide your responses in an electronic format, such as Acrobat or Microsoft Word. This will assist in our review process. We value your time and do not want you to spend your time preparing lengthy responses. After reviewing the responses, vendors may be selected for presentations to be given locally in the Olympia area, or via the web. Please include in your response how you would propose to do a presentation if you are selected.

Vendors should also be prepared to provide fully-functional evaluation copies of any proposed software upon request, as a follow up to this RFI.

Responses to this RFI should be submitted to the Project Coordinator no later than June 15, 2016 at 4 p.m. local time, Olympia, WA.

Please do not cut and paste your responses into this RFI. Instead provide your response as a separate document and include numbers referencing the RFI section you are responding to. Only the one electronic copy need be submitted.

E-mail is the preferred method of delivery. Hardcopy responses and materials will be accepted; faxed responses will not. Please submit responses to the RFI Coordinator at the following address and/or email:

Mailing Address

Attn: **Christie Turner**
Consolidated Technology Services
Office of Legal Services
1500 Jefferson Street
PO Box 41501
Olympia, WA 98501

Questions should be directed to the RFI Coordinator at Christie.Turner@watech.wa.gov or (360) 407-8817.

3) DESCRIPTION

WaTech is seeking information about a solution to be the core infrastructure for the WaTech provided service of Vulnerability Assessment and Discovery. WaTech, as a central service provider, currently provides this service to agencies of Washington State. The Vulnerability Assessment and Discovery service will provide a multi-tenant solution for:

- Finding, assessing, and reporting security weaknesses
- Identifying remediating and mitigating strategies
- Discovering assets on the network and identifying key characteristics of the assets
- Assessing compliance against industry standards such as HIPAA, PCI, CIS, NIST, etc.

WaTech, in the role of a central service, provides this service to the agencies of Washington State. WaTech builds, deploys, manages, and supports the infrastructure from which the service is provided. WaTech provides the service as a multi-tenant solution with each state agency consuming one or more tenants. WaTech provides this service with the administration fully delegated to the agency or tenant owner. WaTech expects the vendor to provide the platform to deliver this enterprise class multi-tenant solution to its customers, the agencies of Washington State.

For each set of requirements, please describe if the requirement is out of the box, needs to be configured, or requires additional modules or components

1. Describe the multi-tenant architecture and design
 - 1.1. List the multi-tenant features
 - 1.2. Identify how the primary components can be deployed with central management and decentralized deployment
 - 1.3. Describe how the solution can be deployed by a central agency service provider to maintain a federated architecture. Describe the deployment models supported for the federated architecture – on premise, cloud, and hybrid cloud.
 - 1.4. Describe how the scanners can be centrally placed or remotely behind an agency firewall
 - 1.5. Describe how scans can occur with different origin locations and still support unified reporting
 - 1.6. List any scanning deployment limitations, such as if deployment of the scanner behind certain firewalls or other network equipment is not supported
 - 1.7. Describe the process for creating and maintain tenants
 - 1.8. Describe how the tenant data is segmented and inaccessible by other tenants. How this segmentation is accomplished even when tenants share common subnets.
 - 1.9. Describe how the central service provider can delegate tenant administration through role based access. What are the roles and features per role? How can the roles be customized?
 - 1.10. List the directory services supported for central service provider and tenant administrator authentication
 - 1.11. Describe how each tenant owner can utilize different directory services for user authentication
 - 1.12. List the features that are not custom assignable to a specific tenant
2. Describe the support for web application scanning
 - 2.1. List the technologies supported by anonymous and authenticated web application scanning – such as HTML 4, HTML 5, JavaScript, JSP, etc.
 - 2.2. Describe the scope of scanning capabilities. Describe how scope extends beyond the OWASP top ten
 - 2.3. List the types of authentication supported for web application scanning
3. Describe the support for host scanning
 - 3.1. List the platforms and versions supported by the anonymous and authenticated host scanning capabilities – such as Windows, Linux, etc.

4. Describe the support for host configuration scanning
 - 4.1. List the regulatory standards based benchmarking supported – such as HIPAA, PCI, CIS, NIST, etc. Describe how the standard applied can be customized per tenant.
 - 4.2. Describe how the host configuration scanning can be customized by platform type
5. Describe the SSL/TLS certificate discovery, assessment, and reporting capabilities
6. Describe the ability for the solution to discover, traverse, and report proxy software and hardware solutions
7. Describe the support for mobile devices
 - 7.1. Describe the support for mobile app scanning
 - 7.2. Describe the mobile device integration capabilities
8. Describe the vulnerability scoring methods and options. Include the options for custom categorization
 - 8.1. Identify the federal and industry standards compliance for the vulnerability scoring
 - 8.2. Describe the prioritization and categorization capabilities
 - 8.3. Describe the customization capabilities for prioritization and categorization
9. Describe the API library and the features supported
10. Describe how alerts are implemented. Describe how alerts can be set for different levels of vulnerabilities.
11. Describe the method and frequency for maintaining and updating the vulnerability definitions for all the tenants
 - 11.1. Identify how running and scheduled scans can complete while vulnerability definition updates are occurring
 - 11.2. Describe the support for zero day responses
 - 11.3. List the standard vulnerability definition libraries supported
12. Describe the host and application discovery capabilities
 - 12.1. List the host types supported for discovery
 - 12.2. List the common third party applications and databases supported for discovery
 - 12.3. List devices, including servers and network devices, supported for discovery
13. Describe the scheduling capabilities and methods
14. List the supported scan platforms – such as appliance, virtual machine, scanning client software, cloud based, etc.
15. Scans must be capable of originating outside the WATech and customer networks. Describe the support for scans external from the targets, such as cloud based scanning. Describe any limitations for externally originating scans, including subnet size and limitations on available features.
16. Describe how scanning can occur without agents on the target
17. Describe the reporting capabilities
 - 17.1. Describe the built in reports
 - 17.2. Describe the reports complying to industry standards
 - 17.3. Describe the ability to customize the fields in the reports
 - 17.4. Describe the ability to export to CSV and Excel
 - 17.5. Describe the ability to automate and schedule report generation
 - 17.6. Describe the ability to automate emailed reports
 - 17.7. Describe how the reports show all discovered vulnerabilities
 - 17.8. Discuss how reports identify remediation for discovered vulnerabilities
 - 17.9. Describe the support for customizable charts
 - 17.10. Describe how the reports identify the source of vulnerability specific to the page, website, or application on host
 - 17.11. Describe how the central service provider can report across all tenants
 - 17.12. List all other report types and reporting capabilities (use attachments)

- 17.13. List other export types (use attachments)
- 18. Describe the logging capabilities
 - 18.1. List the log formats supported
 - 18.2. Describe how each customer can view and receive only their own logs
 - 18.3. Describe support for integration with the third party logging products
- 19. Describe support for integration with the third party products
 - 19.1. Describe the support for integration with penetration testing / interactive application scanning third party products
 - 19.2. Describe the support for integration with third party products that can integrate with firewall rules and present assessments based on the rules
 - 19.3. Describe how scan results can be imported into third party web application firewall products to build security policies
- 20. Describe the encryption strategy
 - 20.1. Identify how data is encrypted in transit
 - 20.2. Identify how data is encrypted at rest
- 21. Describe how the solution can perform multi-threaded and uninterrupted scans of very large networks, such as /16 networks.
- 22. Describe the capability to create tickets for vulnerabilities
 - 22.1. Describe the capability to integrate with third party ticket management issues
 - 22.2. Describe the capability to integrate with email systems for ticket notifications
- 23. Describe how high availability is implemented
- 24. Describe the backup capability and retention policies, such as for scan results.
- 25. Describe the training programs offered. Describe how training can be customized by roles.
- 26. Identify the tools, features, and services available to migrate customers from other vulnerability assessment and discovery solutions
 - 26.1. Specify the degree and type of automation available for supported methods of migrating customers from other solutions

1) SAMPLE RESPONSE OUTLINE

Following is a suggested outline for a response to this RFI. This outline is intended to minimize the effort of the vendor and structure the responses for ease of analysis by WaTech. Nevertheless, vendors are free to develop their response as they see fit.

Section 1 – Responses to Requirements

Provide detailed answers to numbered requirements listed above.

Section 2 – Cost and Schedule Estimates

Provide estimates for all costs associated with implementing the Solution (e.g. Initial license fees, annual maintenance)

Provide estimates for time to import current contracts, templates, etc., into the Solution

Section 3 – Corporate Expertise

Briefly describe your company, your products and services, history, ownership, financial information, and other information you deem relevant.

In particular, please describe any projects you have been involved in that are similar in concept to what is described in this RFI, including management and operations approach, and any relevant lessons learned.

Section 4 – Additional Materials and Others Items We Should Consider

Please provide any other materials, suggestions, and discussion you deem appropriate.

2) OPTIONAL- INFORMATION EXCHANGE MEETINGS

WaTech may, in its sole discretion, consider meeting individually with potential vendors for follow up information as WaTech deems necessary. WaTech will contact the vendors if it decides to engage in informational exchange meetings.

3) DISCLAIMERS

This RFI is issued solely for information and planning purposes only and does not constitute a solicitation. The issuance of this RFI and your preparation and submission of information do not commit WaTech to any contractual relationship, directly or indirectly. WaTech will not reimburse or make payment for any costs incurred in the preparation and submittal of your response. The representations made by the Vendor in their Responses will be considered material representations of fact upon which reliance shall be placed if WaTech determines to enter into a subsequent RFP or contract.

Response Property of WaTech

All materials submitted in response to this RFI become the property of WaTech. WaTech has the right to use any of the ideas presented in any such materials.

Proprietary Information

Any information contained in the response that is proprietary or confidential must be clearly designated.

Marking of the entire response as proprietary or confidential will neither be accepted nor honored.

WaTech will not accept responses where pricing is marked proprietary or confidential.

To the extent consistent with chapter 42.56 RCW, the Public Disclosure Act, WaTech will maintain the confidentiality of Vendor's information marked "confidential" or "proprietary." If a request is made to view Vendor's proprietary information, WaTech will notify Vendor of the request and of the date that the records will be released to the requester unless Vendor obtains a court order enjoining that disclosure. If Vendor fails to obtain the court order enjoining disclosure, WaTech will release the requested information on the date specified.