

# **REQUEST FOR INFORMATION (RFI)**

**Minnesota State (Minnesota State  
Colleges and Universities) ITS  
(Information Technology Services)  
May 2018**

**Vulnerability Management Tools**

***DUE: Friday, June 1, 2018 @ 1:00 P.M. CST***

**Vendors should check the site daily (e.g. amendments, responses to questions) and are expected to review information on the site carefully before submitting a final proposal. <http://www.minnstate.edu/vendors/index.html>**

## **I. STATEMENT OF NEED**

The Minnesota State Colleges and Universities (Minnesota State) system is the fourth largest higher education system in the U.S. and is comprised of 37 institutions with 54 campuses that serve more than 430,000 students annually.

The purpose of this RFI is to gather information for a possible future RFP. The current need is to gain product information for the following:

Minnesota State's system office in collaboration with campus partners is in the process of identifying the scope and cost structure for tools to support the system's Vulnerability Management Program. This team is gathering information from vendors who can deliver methodologies, processes, architectures, and technologies that enable the identification (and potentially, also remediation) of information security vulnerabilities on approximately 80,000 computer systems, network and datacenter infrastructure devices, and other information technology resources running a wide variety of operating systems, middleware and application software.

**NOTE:** *This RFI does not obligate Minnesota State to purchase any goods or services or any consideration in any future Requests for Proposals (RFP). Responses to the RFI are not offers and cannot be accepted by Minnesota State to form a binding contract. No contract will result from any response to this RFI. This RFI shall not limit any rights of Minnesota State, and Minnesota State reserves all its rights including but not limited to its right to elect not to procure the goods and/or services that are the subject of this RFI and its right to procure them from a vendor that has not responded to this RFI.*

## **II. RFI PROCESS**

This section describes the process that the issuer of this Request for Information will follow in this solicitation and expectations about the nature of the responses.

### **A. Response Submittal**

Format Response: In 25 pages or less without marketing materials, provide detailed responses to the following questions:

1. Identify the Vulnerability Management Tools you have available.
2. Describe how these tools implement vulnerability identification (and remediation, if available).
3. Describe the environments supported by these tools (i.e., the operating systems, middleware, application software, devices and appliances for which vulnerabilities can be detected or managed). This information can be provided as an appendix or separate attachment to the response, the length of which does not count against the response page limit.
4. Describe the support for "unknown" devices, i.e., devices which are not included in the response to question 3.
5. Describe the architecture of these tools (i.e., scanning or agent based, appliances or servers required, cloud deployment, high-level communication paths, etc.).

6. Describe how these tools work with multiple physical sites which each have an “edge” network firewall; Minnesota State has more than 80 such sites.
7. For cloud-based solutions, describe:
  - a. How the solution works to find vulnerabilities with hosts “behind” a firewall having RFC-1918 (i.e., non-Internet routable) IP addresses.
  - b. How security of collected data is maintained.
8. Describe how your tools can provide role-based access controls, including the ability to limit data visibility for a specific role to at a sub-organization level. (This capability is required to allow distribution of effort and control of visibility of security data across the 37 institutions within the Minnesota State system.)
9. Describe how updates are provided to support newly-identified vulnerabilities.
10. Describe the vulnerability scoring system used by the tool(s), and any ability for customer-selectable scoring modifications or weights.
11. Describe any capabilities for assigning risk values to hosts or classifying hosts into categories for planning prioritization of remediation efforts.
12. Describe the data visualization, data discovery, reporting, and analytic tools available for processing vulnerability data, producing both actionable reports for practitioners and high-level summaries for management. Please focus on the level of customizability of these tools as delivered (i.e., not requiring any kind of professional services engagement).
13. Describe the ability of the tools to integrate with any 3<sup>rd</sup> party business intelligence, data visualization or data analysis tools. Does any tool have a published database schema which can be used to facilitate such integrations?
14. Describe any product APIs which can be used for task automation or data analysis.
15. Describe the product support provided, including mechanisms for contact and timeframes for initial response to and resolution of simple issues.
16. Describe training opportunities (e.g. in-person, web, train the trainer)
17. Describe any features expected to be available within the next 6-12 months (may include product timeline).
18. Describe strategies or services that would assist Minnesota State in converting and modernizing our existing vulnerability scanning system which utilizes the IP360 product from Tripwire. (Note: Minnesota State reserves the right to continue using the current solution if that solution is determined to best fit Minnesota State’s needs.)
19. Provide two (2) examples of successful higher education implementations.
20. General cost structures and options for providing qualified service (e.g. subscription, hosted, perpetual/concurrent licensing)
21. Contact Information.
22. Rank the webinar dates listed in section IV. in order of preference.

***NOTE:** Minnesota State is not liable for any costs incurred by Responders in developing the responses directly or indirectly related to this Request for Information (RFI). Respondent is responsible for all costs associated with creation of a response or any follow-up requests. All responses submitted become the property of Minnesota State.*

### III. Contacts

Any questions regarding this RFI should be sent via email no later than **Friday, May 11, 2018** to:

Jennell Flodquist  
ITS Purchasing & Contract Administrator  
651-201-1524  
[Jennell.Flodquist@minnstate.edu](mailto:Jennell.Flodquist@minnstate.edu)

RFI responses shall be submitted via email no later than **1:00 PM CST on Friday, June 1, 2018** to: [Jennell.Flodquist@minnstate.edu](mailto:Jennell.Flodquist@minnstate.edu)

### IV. RFI Schedule

Targeted Schedule of Events

Description	Date
RFI Issue Date	Thursday, May 3, 2018
RFI Questions Due Date/Time	Friday, May 11, 2018
RFI Q & A Posted Date	Friday, May 18, 2018
<b>RFI Due Date/Time</b>	<b>1:00 PM CST, Friday, June 1, 2018</b>
RFI Selection Notification	Friday, June 8, 2018
Planned Vendor Webinar Dates (in RFI response, please provide preferences of dates/times):	Monday, June 18, 10 – 11:00 AM CST Monday, June 18, 3 – 4:30 PM CST Tuesday, June 19, 10:30 AM – 12:00 PM CST Wednesday, June 20, 2:30 – 4:00 PM CST

### V. Review of Responses

All responses received by the deadline will be reviewed by representatives of Minnesota State. Because of the nature of an RFI, there will be no response rating or formal determination of solution.

### VI. Webinar with Script

Initial target goal is to invite in three (3) responders, but Minnesota State reserves the right to select one, none or more of the responders to present a webinar (a timed presentation of 1 hour and 15 minutes in length with Q &A for 15 minutes in length). Minnesota State reserves the right to have additional meetings with none, one or more of the responders. Webinar product demonstration will on the dates/times listed above in section IV. Please include preference of dates/times when responding to this RFI.

#### **SCRIPT (Responder will need to time-manage the presentation if requested to present)**

- Company Overview (No Marketing – Not a Sales Presentation)
- Describe Offering

- Show detailed functionality of offering
- Show how product can provide customized, role specific (i.e., practitioner, management, and executive level) reports at both the organization and sub-organization levels
- Future product functionality timeline
- Training Opportunities
- General Cost Structure and Licensing/Subscription Models
- Q&A (15 minutes)