Nebraska Information Technology Commission

Vulnerability Threat Management

Project Proposal Form

Government Technology Collaboration Fund Grant

Project Title	**Vulnerability Threat Management**
Agency/Entity	**Security Architecture Work Group**

Notes about this form:

1. **USE.** The Nebraska Information Technology Commission ("NITC") is required by statute to "make recommendations on technology investments to the Governor and the Legislature, including a prioritized list of projects, reviewed by the technical panel, for which new or additional funding is requested." Neb. Rev. Stat. §86-516(8) In order to perform this review, the NITC and DAS Budget Division require agencies/entities to complete this form when requesting new or additional funding for technology projects.
2. **WHAT TECHNOLOGY BUDGET REQUESTS REQUIRE A PROJECT PROPOSAL FORM?** See the document entitled "Guidance on Information Technology Related Budget Requests" available at http://www.nitc.state.ne.us/forms/.
3. **DOWNLOADABLE FORM.** A Word version of this form is available at http://www.nitc.state.ne.us/forms/.
4. **SUBMITTING THE FORM.** Completed project proposal forms should be submitted as an e-mail attachment to rick.becker@nitc.ne.gov.
5. **DEADLINE.** Completed forms must be submitted by October 26, 2007 (the same date deficit budget requests are required to be submitted to the DAS Budget Division).
6. **QUESTIONS.** Contact the Office of the CIO/NITC at (402) 471-7984 or rick.becker@nitc.ne.gov

Section 1: General Information

Project Title	Vulnerability Threat Management
Agency (or entity)	Security Architecture Work Group

Contact Information for this Project:

Name	Steve Hartman
Address	501 South 14th Street
City, State, Zip	Lincoln, Nebraska 68509
Telephone	402 471-7031
E-mail Address	Steve.hartman@nebraska.gov

Section 2: Executive Summary

The Office of the CIO has used the Government Technology Collaboration Fund in the past to provide enterprise security assessments. KPMG, OmniTech, and most recently ManTech International have been retained to provide vulnerability assessments on our external and internal facing servers. These security assessments while valuable, are 'point in time' assessments and are immediately outdated with the next release of an exploit. The State Information Security Officer is issuing a RFP to purchase an in-house product to perform these vulnerability assessments on a more regular and consistent basis, thereby improving the overall security posture of the State of Nebraska. The vulnerability tool selected will allow an agency to schedule scans to run on a weekly, monthly or quarterly based upon the criticality of the system. A remediation report is created for each device, and once the agency has completed the mitigation steps, a second scan can be conducted to ensure that the vulnerability has indeed been corrected, a step that was missing from the annual security assessments in the past.

A complete vulnerability tracking solution will be integrated into the vulnerability tool to provide for monitoring and analysis regarding the effectiveness of an agency's remediation of known vulnerabilities.

The vulnerability tool will allow for role-based reports to be viewed through a web-based dashboard, while providing the necessary authentication and authorization controls required to prevent one agency from viewing another agencies reports. The State Information Security Officer will have the ability to produce executive level reports that span the enterprise.

Section 3: Goals, Objectives, and Projected Outcomes (15 Points)

1. Describe the project, including:
   - Specific goals and objectives;
     The State of Nebraska has provided enterprise security assessments for agencies through funding provided through the Collaboration Technology Fund. The State Information Security Officer, through the Office of the CIO, wishes to use the Government Technology Collaboration Fund to procure a product to perform the external and internal assessments ourselves on a regular and consistent basis.
   - Expected beneficiaries of the project; and
     All servers, Firewalls, and switches can be monitored by the vulnerability tool. Every Agency,

Board, and Commission will now have the ability to view their current status, run ad hoc reports and produce meaningful analysis that will be being to show trends and tendencies within an agency and throughout the State of Nebraska.

- Expected outcomes.
  All servers, firewalls, and switches will be scanned on a more consistent basis instead of the once every year or two. Agencies will have the information they need to actively harden devices and protect their infrastructure.

2. Describe the measurement and assessment methods that will verify that the project outcomes have been achieved.
   The product selected through the RFP process, will provide weekly, monthly, quarterly and year-to-date reports. Inside the reports will be a comprehensive risk mitigation plan along with the ability to assign work to staff and track the progress. (Copies of the requirements for the RFP are attached)

3. Describe the project's relationship to your agency comprehensive information technology plan.
   This is an integral component of the State Information Security Officer's strategic plan for 2007 – 2008. It will allow agencies the track their effectiveness in mitigating vulnerabilities in a timely manner and provide agency leaders with meaningful and useful metrics in determining the risk to their infrastructure, applications, and data.

Section 4: Project Justification / Business Case (25 Points)

4. Provide the project justification in terms of tangible benefits (i.e. economic return on investment) and/or intangible benefits (e.g. additional services for customers).
   The Office of the CIO has used the Collaborative Technology Fund to provide annual security assessments. For the same investment, the State of Nebraska can own a vulnerability tool that can be used throughout the year, providing weekly, monthly, or quarterly audits, while providing a mechanism to track incidents and remediation plans. Information detailing the risks the State of Nebraska faces can be produced ad hoc, rather than just once per year.

5. Describe other solutions that were evaluated, including their strengths and weaknesses, and why they were rejected. Explain the implications of doing nothing and why this option is not acceptable.
   An RFP is being issued that will examine multiple vendors and solutions in order to chose the product that best meets the requirements of the State of Nebraska at the most reasonable cost.

6. If the project is the result of a state or federal mandate, please specify the mandate being addressed.
   The State of Nebraska plans to use the vulnerability tool to provide Payment Card Industry Data Security Standard (PCI DSS) compliance for its credit card processing in the state.

Section 5: Technical Impact (20 Points)

7. Describe how the project enhances, changes or replaces present technology systems, or implements a new technology system. Describe the technical elements of the project, including hardware, software, and communications requirements. Describe the strengths and weaknesses of the proposed solution.
   Currently, the State of Nebraska hires an independent third party to come onsite once every year or two and perform a vulnerability assessment. The tools and products the State of Nebraska expects to purchase through the RFP are the exact same tools and products used by the leading consulting firms. However, instead of getting a single snapshot, moment-in-time, view of the State of Nebraska, we will be able to provide continuous insight into the State of Nebraska's infrastructure, which will

allow us to better measure compliance with NITC policies and business objectives.

The weaknesses of this solution, is that the products and tools in the marketplace may produce false positives (report a weakness that isn't there) or worse, a false negative (miss a vulnerability and not report it at all). The leading contenders in this space have been around for quite along time, and the accuracy rate is extremely high. But just to be safe, the State of Nebraska has included in the RFP the requirement that the tool has the ability to be 'tuned' to skip the false positives and to find the false negatives.

8. Address the following issues with respect to the proposed technology:
   - Describe the reliability, security and scalability (future needs for growth or adaptation) of the technology.
     The product chosen through the RFP process will be a best-of-breed solution, with a targeted implementation that spans the enterprise. The current estimate is that it will cover 1600+ servers, and 1000+ network devices. Agencies will have the opportunity to include all desktops and laptops at their own expense. The majority of the solutions in this market space are appliance based, and their reliability and security are excellent.
   - Address conformity with applicable NITC technical standards and guidelines (available at http://www.nitc.state.ne.us/standards/) and generally accepted industry standards.
     The ability to produce up to the minute vulnerability assessments across the enterprise is addressed in the NITC Information Security Policy, and will assist agency leaders as they perform annual risk assessments as called for under the Data Security Standard.
   - Address the compatibility with existing institutional and/or statewide infrastructure.
     The solution selected through the RFP process will be required to co-exist with the current infrastructure with minimal or no changes.

Section 6: Preliminary Plan for Implementation (10 Points)

9. Describe the preliminary plans for implementing the project. Identify project sponsor(s) and examine stakeholder acceptance. Describe the project team, including their roles, responsibilities, and experience.
   The project sponsor is the State Information Security Officer. Staff from the Office of the CIO will administer the appliance and updates. The State Information Security Officer and / or members his staff will administer the roles within the product. The initial implementation will be run in a non-authenticated mode, so no accounts or administration will be required on the agency's end, other than to perhaps create a firewall rule that will allow the appliance access to the agency LAN.

10. List the major milestones and/or deliverables and provide a timeline for completing each.
    The RFP will be released in mid-October, with an expected award date in December 2007. Implementation will be after the first of the year, and we expect to complete the implementation in 5 business days. Agencies should be able to being scanning devices by the end of the January 2008.

11. Describe the training and staff development requirements.
    The products can be deployed in a number of configurations. It is the intention of the State Information Security Officer to deploy the product initially in a non-authenticated mode. The only requirements for this deployment is that firewall rule sets between the Office of the CIO and the agencies will need to be modified to allow the vulnerability scans to run across vLANs. Ultimately, the State information Security Officer would like to have the vulnerability scans to run in a full administrative mode, providing registry information, and change / configuration management capabilities. Training is to be included by vendor as part of the RFP request.

12. Describe the ongoing support requirements.
    As initially deployed, the on-going administrative support requirements will be minimal. All hardware related support and updates will be handled by the Office of the CIO.

Section 7: Risk Assessment (10 Points)

13. Describe possible barriers and risks related to the project and the relative importance of each.
    As mentioned before, the planned implementation will not require and administrator accounts to begin with, so the only potential barrier physically will be if the agency has a firewall rule that blocks the requests from the vulnerability tool. This can be easily corrected, with a firewall rule modification.

    Another potential risk is that that the vulnerability tool will consume high levels of bandwidth, causing performance denigration. We have spoken to the University of Nebraska about this issue, and their experience is that the bandwidth requirements for the vulnerability tools are low. Additionally, most scans can be scheduled to run during non-peak hours for maximum utilization of the network.

14. Identify strategies which have been developed to minimize risks.
    The RFP was developed in cooperation with the University of Nebraska, Central administration, who has already successfully implemented a vulnerability threat management solution. The University's Information Security Officer, Joshua Mauk has reviewed the RFP and the requirements for the State of Nebraska and has found them to be inline with industry best practices.

    Implementation will be in a phased manner, with phase 1 consisting of deploying the appliance in a non-authenticated mode. Minimal amount of setup, debugging, and administration will be needed for this phase. Once the State of Nebraska has been successfully using the vulnerability management tool, and has reached a maturity level of being able to consistently identify and remediate issues within pre-defined service level agreements (SLA) and with NITC policy, we will begin planning for phase 2 and run scans in an full administrative mode. This will allow agencies to document registry, configuration, and code changes on the devices and compare those results against the published change management entries recorded through the state's change management process.

Section 8: Financial Analysis and Budget (20 Points)

15. Financial Information

Financial and budget information can be provided in either of the following ways:

(1) If the information is available in some other format, either cut and paste the information into this document or transmit the information with this form; or

(2) Provide the information by completing the spreadsheet provided below.

Instructions: Double click on the Microsoft Excel icon below. An imbedded Excel spreadsheet will be launched. Input the appropriate financial information. Close the spreadsheet. The information you entered will automatically be saved with this document. If you want to review or revise the financial information, repeat the process just described.

Excel Spreadsheet
(Double-click)

16. Provide a detailed description of the budget items listed above. Include:
    - An itemized list of hardware and software.
      An RFP has been created, and was issued in October of 2008, to choose a product / vendor that meet the state's requirements for a vulnerability threat assessment tool.
    - If new FTE positions are included in the request, please provide a breakdown by position, including separate totals for salary and fringe benefits.
      No additional FTE or resources are required
    - Provide any on-going operation and replacement costs not included above, including funding source if known.
      The costs for the products are a perpetual license. It has not been decided if the Office of the CIO will develop a rate to recover some or all of the continued costs of the product, or if the Government Technology Collaboration Fund will be used in the future.
    - Provide a breakdown of all non-state funding sources and funds provided per source.
      Other finding sources - None
      Government Technology Collaboration Fund- $75,000

17. Please indicate where the funding requested for this project can be found in the agency budget request, including program numbers.
    Not applicable

Nebraska Cyber Security Center Strategic Plan 2007

Focused

- *"Close or narrow attention"*
- *"A condition in which something can be clearly apprehended or perceived"*

Daily we are bombarded with new products that promise to solve all our security problems, yet no one has the budget or resources to buy them all and even if you did, it would in reality be a disaster trying to get all these products to work together. Rather than try and purchase a host of products, the Nebraska Cyber Security Center is committed to deploying only those components that will meet our security goals in a cost effective and responsible manner. Our challenge is to develop a comprehensive plan that provides the most 'bang-for-the buck" while continuing to provide the maximum amount of protection for the enterprise using a defense-in-depth approach.

The Nebraska Cyber Security Center is cognizant of the fact that there are millions of events and transactions that occur daily on thousands of devices and that it is impractical to think that any one person or persons could monitor all these events in real time. Therefore, the Nebraska Cyber Security Center will centralize as many of these events in a central location, providing an ideal location to perform analysis in an effective and timely manner. This analysis center will enable us to produce highly detailed compliance reports for our customers and auditors.

Strategic components:

- Qualys / Retina eEye / Foundstone
  - *RFP Fall 2007/ Full implementation January 2008*
- F5
  - *DOL / NIS complete*
  - *Additional sites (App FW summer 2008)*
- Fortigate
  - *All new Fortigate FWs in place and configured Fall 2007*
  - *Change Management for FW modifications - Jan. 2008*
- Net IQ / Network Intelligence / eIQ
  - *Homeland Security Grant 2008*
- WebInspect / AppScan
  - *Purchase Sept/ Oct. 2007*
  - *All OCIO web applications by end of year.*
  - *All web applications by spring 2008*

Secure

- **"***dependable; firm; not liable to fail, yield,"*
- *"safe from penetration or interception by unauthorized persons"*
- **"***to guarantee the privacy or secrecy of"*

With the Nebraska Cyber Security Center taking a more focused approach in 2007, we must be confident that the solutions we put into place are:

- industry-tested best practices,
- they provide sufficient coverage to accomplish our security goals
- changes are closely monitored, and
- are cost effective solutions that enable eGovernment.

The Nebraska Cyber Security Center will promote training and awareness programs that will raise the level of awareness to insider threats, social engineering attacks, and general security best practices. An additional area of emphasis will be in developing solid documented processes and procedures for the infrastructure and applications that will enable us to accurately test the continued security posture of the State of Nebraska.

Lastly, we will perform vulnerability assessments on a regular schedule for all servers. We will also monitor and track all updates and configuration changes to systems and applications to ensure continued effective protection of our critical assets.

A statewide risk assessment, listing all the critical applications, devices and systems within the State of Nebraska, the vulnerabilities associated with each asset, the likelihood of an exploit occurring for that asset and the impact for the agency (ies) and / or State of Nebraska.

Strategic components:

- Security Awareness training for all state employees
  - *MS-ISAC CBT modified and deployed Fall 2007*
  - *All state employees using CBT Jan. 2008*
- Specialized training for key technology frontline workers
  - *CISSP Training (SANS)*
  - *SANS certification training*
- Nebraska Cyber Security Conference
- Vulnerability Threat Management (Qualys / Retina / Foundstone)
- Risk Assessment

Relevant

- *"Having a bearing on or connection with the matter at hand"*
- *"Pertinence to the matter at hand"*

The Nebraska Cyber Security Center will make all decisions concerning the purchase of products and the implementation of processes or procedures to ensure they are a necessary component that fits into the overall security architecture. The Nebraska Cyber Security Center will *not* be exploring or implementing new technologies that will not be of an immediate benefit to the State of Nebraska.

The Nebraska Cyber Security Center will be focusing more closely on the metrics gathered by the various devices already in place within the State of Nebraska. An evaluation of those metrics will result in the capturing and reporting of meaningful security metrics, and producing a *balanced scorecard* each month for distribution to agency directors, the executive branch, and the legislature.

Lastly, we will continuously evaluate our security program against the ever changing threat landscape to ensure that the products, processes, and procedures continue to provide effective coverage of all our critical assets.

Strategic parnters:

- NITC Security Architecture Work Group
- NITC Technical Panel
- Office of the CIO Leadership team
- Partnership with the University of Nebraska
- Partnership with MS-ISAC
- Partnership with local governments

IV. PROJECT DESCRIPTION AND SCOPE OF WORK

The bidder must provide the following information in response to this Request for Proposal.

A. PROJECT OVERVIEW

The Office of the Chief Information Officer seeks proposals from qualified bidders to provide the State of Nebraska with an enterprise Vulnerability Management solution.

B. PROJECT ENVIRONMENT

The Office of the Chief Information Officer operates primarily in a Windows environment, and as such is responsible for managing the threats across a distributed network. The State of Nebraska has additional platforms, e.g. AS-400, zSeries, Linux, Mac OS, etc. which may or may not be included in the scans. The State of Nebraska owns approximately 1600 servers and 15,000 desktops, as well as other network devices.

C. BUSINESS REQUIREMENTS

Provide internal vulnerability assessments on all state devices.

D. SCOPE OF WORK

The Office of the Chief Information Officer manages devices for State of Nebraska agencies in accordance with state statutes. As such, a secure computing environment is required. The Office of the Chief Information Officer wishes to purchase a Vulnerability Management solution to be deployed in multiple phases. The first phase comprises 1600 servers. Additional phases include the deployment of the solution to other platforms, as well as to desktops.

E. TECHNICAL SPECIFICATIONS

Bidders must address each of the following technical specifications. The bidder's response must provide enough detail in narrative form to allow the Evaluation Committee to score the bidder's approach to each technical specification. Minimal responses such as "Yes", "No", "Noted", "Agreed" or "Accepted" will be considered non-responsive.

Required	Desired	Technical Specification
X		automatically discover new servers, desktops, etc... on the network
Response:		
	X	scan without the use of agents
Response:		
X		map all discovered assets in physical and or logical topology
Response:		
X		scan servers, desktops, routers, and other network devices
Response:		
	X	scan AS-400, zSeries, Linux, Mac OS, etc.
Response:		
	X	monitor changes to assets, e.g. new files added or changes to configuration files
Response:		
X		ability to schedule scanning tasks
Response:		
	X	automatically generate incident handling and ticket tracking to the asset custodian
Response:		
	X	integrate with HelpDesk systems (vendor to list products);
Response:		
X		create automatic and customizable reports that meet compliance needs of FISMA, HIPAA, ISO27000, PCI
Response:		

X		group and prioritize assets
Response:		
X		restrict views to business units through a role based web enabled dashboard
Response:		
X		provide remediation action lists
Response:		
	X	integrate with Security Information Event Management (vendor to list products)
Response:		
	X	integrate with Anti-Virus (vendor to list products);
Response:		
	X	integrate with Microsoft SMS
Response:		
	X	integrate with Microsoft Windows Server Update Services (WSUS)
Response:		
	X	export reports to optional formats (vendor to list formats)
Response:		
X		tune the event engine to reduce or eliminate false positives
Response:		
X		configure scans for performance issues, specific ports/services and specific vulnerabilities
Response:		
X		produce a score that indicates the risk based upon criticality and sensitivity of the asset (vendor to describe the methodology)
Response:		
X		encryption of vulnerability data
Response:		
X		non-reputable audit trails
Response:		
	X	two-factor authentication
Response:		
X		compliant with PCI DSS version 1.1
Response:		

F. DELIVERABLES

1. Implementation Plan.
2. Vulnerability Management solution and price schedule (price schedule should be based on the number of device scans, e.g. 1600 servers and incremental pricing for non-server devices); inclusive of all expenses.
3. Maintenance and support plan and associated cost, if any.
4. Training plan and associated cost, if any.