MEETING AGENDA

State Government Council
of the
Nebraska Information Technology Commission

Tuesday, November 20, 2007
1:30 p.m. - 2:30 p.m.
Nebraska State Office Building - Conference Room 6Z
301 Centennial Mall South
Lincoln, Nebraska

AGENDA

Meeting Documents: Click the links in the agenda
or click here for all documents.

1. Roll Call, Meeting Notice & Open Meetings Act Information

2. Public Comment

3. Approval of Minutes* - August 9, 2007 and September 6, 2007

4. Government Technology Collaboration Fund Grant Application*

   - Security Architecture Work Group - Vulnerability Threat Management

5. Update on Email Conversion

6. Review NITC Strategic Initiatives for the 2008 Statewide Technology Plan

7. Other Business

8. Agency Reports

9. Next Meeting Date - January 10, 2008

10. Adjourn

* Denotes action items.

(The Council will attempt to adhere to the sequence of the published agenda, but reserves the right to adjust the order of items if necessary and may elect to take action on any of the items listed.)

NITC and State Government Council Websites: http://www.nitc.state.ne.us/
Meeting notice posted to the NITC Website: 4 OCT 2007 (meeting date changed on 15 OCT 2007)
Meeting notice posted to the Nebraska Public Meeting Calendar: 4 OCT 2007 (meeting date changed on 15 OCT 2007)
Agenda posted to the NITC Website: 16 NOV 2007

MEETING MINUTES

STATE GOVERNMENT COUNCIL
Nebraska Information Technology Commission
Thursday, August 9, 2007, 1:30 p.m. - 2:30 p.m.
Nebraska State Office Building - Lower Level B
301 Centennial Mall South, Lincoln, Nebraska
PROPOSED MINUTES

MEMBERS PRESENT:

Dennis Burling, Department of Environmental Quality
Tom Conroy, OCIO - Enterprise Computing Services
Josh Daws, Secretary of State's Office
Keith Dey, Department of Motor Vehicles
Pat Flanagan, Private Sector
Dick Gettemy, Department of Revenue
Steve Henderson, Alt. for Brenda Decker, Chief Information Officer
Glen Morton, Workers' Compensation Court
Jim Ohmberger, Health and Human Services
Gerry Olligmueller, Budget Office
Mike Overton, Crime Commission
Doni Peterson, Department of Administrative Services
Bob Shanahan, Department of Labor
Rod Wagner, Library Commission
George Wells, Correctional Services

MEMBERS ABSENT: Bob Beecham, NDE Support Services; Mike Calvert, Legislative Fiscal Office; Rex Gittins, Department of Natural Resources; Dorest Harvey, Private Sector; Lauren Hill, Governor's Policy Research Office; Jeanette Lee, Department of Banking; Terry Pell, State Patrol; Jayne Scofield, OCIO - Network Services; Janice Walker, Supreme Court and Bill Wehling, Department of Roads

ROLL CALL, MEETING NOTICE & OPEN MEETINGS ACT INFORMATION

Mr. Henderson called the meeting to order at 1:35 p.m. There were 15 voting members at the time of roll call. It was stated that the meeting notice was posted to the NITC, State Government Council and Nebraska Public Meeting Calendar Websites on July 2, 2007 and that the agenda posted to the NITC Website on August 6, 2007. A copy of the Open Meetings Act was located on the front table.

PUBLIC COMMENT

There was no public comment.

APPROVAL OF JUNE 14, 2007 MINUTES

Mr. Flanagan moved to approve the June 14, 2007 minutes as presented. Mr. Conroy seconded. All were in favor. Motion carried.

STANDARDS AND GUIDELINES - INFORMATION SECURITY POLICY

Purpose: To provide a uniform set of reasonable and appropriate security safeguards for protection of the confidentiality, integrity, availability and privacy of State of Nebraska information collected, stored, and used to serve the citizens of the State of Nebraska. This Information Security Policy contains the minimum safeguards, responsibilities and acceptable behaviors required to establish and maintain a secure environment.

The primary objectives are to:

- effectively manage the risk of exposure or compromise to State resources;
- communicate the responsibilities for the protection of information;
- establish a secure, resilient processing environment;
- provide security controls for internally developed software to protect unauthorized access, tampering, or programming errors;
- provide a formal incident management processes; and
- promote and increase the awareness of information security.

Mr. Burling left the meeting.

STANDARDS AND GUIDELINES - DATA SECURITY STANDARD

Purpose and Objectives: It is the objective of this policy to provide safeguards to protect that information. Common methods of protecting information include, but are not limited to:

- Staff education
- Restricted data access and usage
- Administrative policies and procedures
- Data encryption
- Network encryption
- Account authorization
- Strong passwords
- Biometric authentication
- Physical security
- Network Firewalls
- Server hardening

Several council members expressed concern that more time was needed to review the Information Security Policy and the Data Security standard.

Mr. Flanagan moved to table the Information Security Policy and the Data Security Standard until the September meeting. Mr. Gettemy seconded. Roll call vote: Dey-Yes, Conroy-Yes, Daws-Yes, Flanagan-Yes, Gettemy-Yes , Henderson-Yes, Morton-Yes, Ohmberger-Yes, Olligmueller-Yes, Overton-Yes, Peterson-Yes, Shanahan-Yes, Wagner-Yes, and Wells-Yes. Results: Yes-14, No-0. Motion carried.

STANDARDS AND GUIDELINES - PASSWORD STANDARD

Standard: Passwords are a primary means to control access to systems; therefore all users must select,
use, and manage passwords to protect against unauthorized discovery or usage.

Password Construction: The following are the minimum password requirements for

State of Nebraska passwords:
• Must contain at least eight (8) characters
• Must contain at least three (3) of the following four (4):
o At least one (1) uppercase character
o At least one (1) lowercase character
o At least one (1) numeric character
o At least one (1) symbol
• Must change at least every 90 days
• Must not repeat any character sequentially more than two (2) times
• Can not repeat any of the passwords used during the previous 365 days.

Mr. Shanahan moved that the Password Standard also be tabled until the September meeting. Mr. Dey seconded. Roll call vote: Conroy-No, Daws-Yes, Dey-Yes, Flanagan-Yes, Gettemy-Yes , Henderson-Yes, Morton-Yes, Ohmberger-Yes, Oligmueller-Yes, Overton-Yes, Peterson-Yes, Shanahan-Yes, Wagner-Yes, and Wells-Yes. Results: Yes-13, No-1. Motion carried.

Mr. Hartman will schedule informational sessions to review the Information Security Policy, Data Security Standard and the Password Standard prior to September meeting for the council members and agency representatives. It was suggested that the NITC Security Work Group be informed of its status.

STANDARDS AND GUIDELINES - EMAIL STANDARD FOR STATE GOVERNMENT AGENCIES

Purpose: To provide a single email system for all state government agencies.

There is a currently an approved standard but the language is not consistent with the state's conversion to a single email system for all state government agencies. It was suggested to further define the term email.

Mr. Conroy moved to recommend approval of the Email Standard For State Government Agencies. Mr. Oligmueller seconded. Roll call vote: Conroy-Yes, Daws-Yes, Dey-Yes, Flanagan-Yes, Gettemy-Yes , Henderson-Yes, Morton-No, Ohmberger-Yes, Oligmueller-Yes, Overton-Yes, Peterson-Yes, Shanahan-Yes, Wagner-Yes, and Wells-Abstain. Results: Yes-12, No-1, Abstain-1. Motion carried.

SHARED SERVICES UPDATES - - VOIP AND VRU
Bob Howard

Mr. Howard provided an update on the current use of VoIP in state government.

OTHER BUSINESS

New members of the Office of the CIO were introduced: Linda Lewis and Tim Cao.

AGENCY REPORTS

There were no agency reports.

NEXT MEETING DATE AND ADJOURNMENT

The next meeting of the NITC State Government Council will be held a week early on September 6, 2007, 1:30 p.m.

With no further business, Mr. Henderson adjourned the meeting at 2:45 p.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by Rick Becker, Office of the CIO.

MEETING MINUTES

STATE GOVERNMENT COUNCIL
Nebraska Information Technology Commission
Thursday, September 6, 2007, 1:30 p.m. - 2:30 p.m.
Nebraska State Office Building - Lower Level C
301 Centennial Mall South, Lincoln, Nebraska
PROPOSED MINUTES

MEMBERS PRESENT:

Dennis Burling, Department of Environmental Quality
Randy Cecrle, Workers' Compensation Court
Tom Conroy, OCIO - Enterprise Computing Services
Josh Daws, Secretary of State's Office
Brenda Decker, Chief Information Officer (Alternate Steve Henderson for part of meeting.)
John Erickson, Governor's Policy Research Office
Pat Flanagan, Private Sector
Rex Gittins, Department of Natural Resources
Bill Miller, State Court Administrator's Office
Jim Ohmberger, Health and Human Services
Gerry Oligmueller, Budget Office
Mike Overton, Crime Commission
Jayne Scofield, OCIO - Network Services
Bob Shanahan, Department of Labor
Len Sloup, Department of Revenue
Rod Wagner, Library Commission

MEMBERS ABSENT: Bob Beecham, NDE Support Services; Mike Calvert, Legislative Fiscal Office; Carlos Castillo, Department of Administrative Services; Dorest Harvey, Private Sector; Jeanette Lee, Department of Banking; Beverly Neth, Department of Motor Vehicles; Terry Pell, State Patrol; Robin Spindler, Correctional Services and Bill Wehling, Department of Roads

ROLL CALL, MEETING NOTICE & OPEN MEETINGS ACT INFORMATION

Mr. Henderson welcomed Len Sloup as the new alternate to the Council from the Department of Revenue. Mr. Henderson called the meeting to order at 1:30 p.m. There were 14 voting members at the time of roll call. It was stated that the meeting notice was posted to the NITC, State Government Council and Nebraska Public Meeting Calendar Websites on August 16, 2007 and that the agenda posted to the NITC Website on August 31, 2007. A copy of the Open Meetings Act was located on the front table.

PUBLIC COMMENT

There was no public comment.

Mr. Gittins arrived at the meeting at 1:33 p.m.

APPROVAL OF AUGUST 9, 2007 MINUTES

Mr. Henderson indicated that we will pass over this item and approve the August minutes at the next meeting.

STANDARDS AND GUIDELINES - Recommendations to the Technical Panel and NITC

Mr. Henderson provided background information on the three documents to be discussed at this meeting. All three were on the last meeting agenda and action was postponed until today. During the interim, the Technical Panel has posted the documents for the 30-day comment period which ends on September 9. Also, Mr. Hartman held three informational meetings on these documents which members were invited to attend. Links to the agenda included draft revisions based on the comments received to date. Mr. Hartman shared these changes with the Security Architecture Work Group and they recommend approval of the changes.

STANDARDS AND GUIDELINES - INFORMATION SECURITY POLICY

Mr. Hartman reviewed the changes to the document and entertained questions from members.

Mr. Oligmueller arrived at the meeting at 1:48 p.m.

Members recommended moving the sentence on page 11 beginning "To provide accountability..." to page 9 at the end of the "Agency Accountability" section; and keeping the deleted language regarding "fixed asset guidelines" and adding "or agency" after "DAS".

Ms. Scofield left the meeting at 2:15 p.m.

Ms. Decker arrived at the meeting at 2:19 p.m.

Mr. Conroy moved to recommend approval of the Information Security Policy as revised. Mr. Ohmberger seconded. Roll call vote: Overton-Yes, Burling-Yes, Conroy-Yes, Decker-Yes, Sloup-Yes, Flanagan-Yes, Daws-Yes, Gittins-Yes, Erickson-Yes, Shanahan-Yes, Cecrle-Yes, Ohmberger-Yes, Oligmueller-Yes, Wagner-Yes, and Miller-Yes. Results: Yes-15, No-0. Motion carried.

STANDARDS AND GUIDELINES - DATA SECURITY STANDARD

Mr. Hartman reviewed the changes to the document and entertained questions from members. The due date for the first report will be October 31, 2008.

Mr. Flanagan moved to recommend approval of the Data Security Standard as revised. Mr. Daws seconded. Roll call vote: Overton-Yes, Burling-Yes, Conroy-Yes, Decker-Yes, Sloup-Yes, Flanagan-Yes, Daws-Yes, Gittins-Yes, Erickson-Yes, Shanahan-Yes, Cecrle-Yes, Ohmberger-Yes, Oligmueller-Yes, Wagner-Yes, and Miller-Yes. Results: Yes-15, No-0. Motion carried.

Mr. Gittins and Mr. Oligmueller left the meeting.

STANDARDS AND GUIDELINES - PASSWORD STANDARD

Mr. Hartman reviewed the document and entertained questions.

Mr. Hartman indicated that one of the written comments received discussed the expense of having to reprogram an application to force compliance with this standard. Mr. Hartman stated that the proposed standard does not require any programmatic enforcement and no requirement to reprogram. The requirement is on the user to meet the standard.

Members discussed two different approaches to this standard. One option is to only require the standard for the initial login (e.g. LAN login) and not apply this standard to other applications and resources once authenticated; and the second option is to have this apply to all passwords. As written, it is the latter approach.

Members also discussed the impact on e-government and other situations where there may be a business need to have a less stringent password. Mr. Hartman indicated that the work group would review this and may recommend changes; however, the standard does allow for agencies to apply for an exemption if there is a business need.

Mr. Miller moved to recommend approval of the Password Standard. Mr. Ohmberger seconded. Roll call vote: Overton-Yes, Burling-Yes, Conroy-Yes, Decker-Yes, Sloup-No, Flanagan-Yes, Daws-Yes, Erickson-No, Shanahan-Abstain, Cecrle-No, Ohmberger-Yes, Wagner-Yes, and Miller-Yes. Results: Yes-9, No-3, Abstain-1. Motion carried.

STANDARDS AND GUIDELINES - EMAIL STANDARD FOR STATE GOVERNMENT AGENCIES

The Council recommended approval of this document at the last meeting. Two recommended changes to the document will be made to the Technical Panel. First, to change it from a "standard" to a "policy"; and second, to add language which makes it clear this applies to employee/worker email accounts.

Ms. Decker expressed appreciation for all the work done on these documents and the input from members of the Council.

OTHER BUSINESS

None.

AGENCY REPORTS

There were no agency reports.

NEXT MEETING DATE AND ADJOURNMENT

The next meeting of the NITC State Government Council will be on October 11, 2007, 1:30 p.m.

With no further business, Ms. Decker adjourned the meeting.

Meeting minutes were taken by Rick Becker, Office of the CIO.

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.

Strategic Initiatives

The NITC has identified eight strategic initiatives, which address the NITC's goals of supporting the development of a robust telecommunications infrastructure; supporting community and economic development; promoting the efficient delivery of government and educational services; and ensuring the security of data and network resources and the continuity of business operations.   These initiatives would materially advance the vision and statewide goals as identified by the NITC. By emphasizing selected strategic initiatives, the NITC hopes to encourage funding of these initiatives and to encourage state agencies to work together to advance these initiatives.   This year's plan includes one new strategic initiative and an expanded initiative.   Public Safety Communications was added this year in recognition of the Office of the CIO's expanded involvement in public safety communications.   The eHealth strategic initiative builds on and expands the scope of the Nebraska Statewide Telehealth Network initiative included in earlier plans.   One strategic initiative from earlier editions of the statewide technology plan has been completed.   With implementation of a statewide K-12 distance learning network underway as a result of the passage of LB 1208 by the Legislature in 2006, the Statewide Synchronous Video Network strategic initiative has been completed.

The NITC has identified eight strategic initiatives which address the NITC's goals.

Supporting the Development of a Robust Telecommunications Infrastructure

Network Nebraska.   In order to develop a broadband, scalable telecommunications infrastructure that optimizes the quality of service to every public entity in the state of Nebraska, the Office of the CIO and the University of Nebraska engaged in a collaborative partnership that used existing resources to aggregate disparate networks into a multipurpose core backbone extending from Norfolk, Omaha, Lincoln, Grand Island, Kearney and North Platte to the Panhandle.   Benefits of Network Nebraska include lower network costs, greater efficiency, interoperability of systems providing video courses and conferencing, increased collaboration among educational entities, new educational opportunities, more affordable Internet access, and better use of public investments.

Supporting Community and Economic Development

Community IT Planning and Development.   The primary objective of this initiative is to foster community and economic development in Nebraska communities through the effective use of information technology.   The NITC Community Council has partnered with the University of Nebraska Cooperative Extension and Rural Initiative to form the Technologies Across Nebraska partnership.   Technologies Across Nebraska is a partnership of over 40 organizations working to help communities utilize information technology to enhance development opportunities. Through Technologies Across Nebraska's Podcasting Across Nebraska program, communities and regional groups are creating podcasts to promote local attractions and events and to provide information to citizens.   Technologies Across Nebraska's quarterly newsletter, *TANgents*, reaches over 1,000 individuals with an interest in technology-related development.

Strategic Initiatives

Promoting the Efficient Delivery of Services

eHealth. eHealth technologies include telehealth, electronic health records, e-prescribing, computerized physician order entry, and health information exchange. The State of Nebraska will build upon the success of the Nebraska Statewide Telehealth Network as it begins to address issues related to the adoption of electronic health records and health information exchange. The widespread adoption of electronic health records is expected to reduce medical errors, improve quality of care, and reduce health care costs for payers.

Public Safety Communications System. The Regional Interoperabilty Advisory Board, Office of the CIO, and the Nebraska Emergency Management Agency have established strategic goals and grants guidance to improve state and local interoperable communications capabilities. The statewide telecommunications strategy integrates regional communications systems, the mutual aid frequency plan, and the state communications infrastructure. The Office of the CIO has developed a plan for a statewide interoperable communications network that consolidates a core of state agencies on a single system platform.

Digital Education. The primary objective of the Digital Education Initiative is to promote the effective and efficient integration of technology into the instructional, learning, and administrative processes and to utilize technology to deliver enhanced digital educational opportunities to students at all levels throughout Nebraska on an equitable and affordable basis. This initiative will involve the coordination and promotion of several major systems and applications that have either been developed mostly at the local level or have not been replicated statewide.

State Government Efficiency. The State Government Council will address multiple items improving efficiency in state government, including implementing shared services and adopting standards and guidelines. The council has identified and is working to implement six shared services for state government agencies. Also, the council will continue to develop standards and guidelines to better coordinate state agency technology efforts. Benefits of these activities include lower costs, easier interoperability among systems, greater data sharing, and improved services.

E-Government. Through the use of technology, state agencies can enhance information sharing, service delivery, and constituency and client participation. Benefits include improved services for citizens and businesses, and increased efficiency and effectiveness for agencies.

Ensuring the Security of Data and Network Resources and the Continuity of Business Operations

Security and Business Resumption. This initiative will define and clarify policies, standards and guidelines, and responsibilities related to the security of the State's information technology resources. Benefits include lower costs by addressing security from an enterprise perspective, cost avoidance, and protecting the public trust.