Nebraska Information Technology Commission

Project Proposal Form

New or Additional State Funding Requests
for Information Technology Projects

FY2005-07 Biennium

Project Title	**Security Audits**
Agency/Entity	**Office of the Chief Information Officer**

About this form…
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." 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. For more information, see the document entitled "Guidance on Information Technology Related Budget Requests" available at http://www.nitc.state.ne.us/forms/.

Electronic versions of this form are available at http://www.nitc.state.ne.us/forms/.

For questions or comments about this form, contact the Office of the CIO/NITC at:

Mail: Office of the CIO/NITC
521 S 14th Street, Suite 301
Lincoln, NE 68508
Phone: (402) 471-3560
Fax: (402) 471-4608
E-mail: info@cio.state.ne.us

Submission of Form
Completed forms must be submitted by the same date biennial budget requests are required to be submitted to the DAS Budget Division. Completed project proposal forms must be submitted via e-mail to info@cio.state.ne.us. The project proposal form should be submitted as an attachment in one of these formats: Microsoft Word; WordPerfect; Adobe PDF; or Rich Text Format. Receipt of the form by the Office of the CIO will be confirmed by e-mail. If an agency is unable to submit the application as described, contact the Office of the CIO prior to the deadline, to make other arrangements for submitting a project proposal form.

Section I: General Information

Project Title	Security Audits
Agency (or entity)	Office of the Chief Information Office

Contact Information for this Project:

Name	Steven Schafer
Address	521 South 14th Street
City, State, Zip	Lincoln, Nebraska 68508
Telephone	402.471.4385
E-mail Address	slschafe@notes.state.ne.us

Section II: Executive Summary

Provide a one or two paragraph summary of the proposed project. This summary will be used in other externally distributed documents and should therefore clearly and succinctly describe the project and the information technology required.

The purpose of this project is to engage a qualified firm to conduct annual security audits / assessments of the information technology infrastructure for state government. Topics of interest include network security, wireless security, application security, and security policies and procedures. The exact scope of each security assessment will focus on one or more of these areas. The Security Work Group will help set priorities and define the scope of work for each assessment.

The NITC security policies (Information Security Management Policy) provide guidance for establishing effective security programs. One requirement is to conduct regular security audits. The Network Security Policy states, "An audit of network security should be conducted annually."

The HIPAA (Health Insurance Portability and Accountability Act) proposed rule for Security and Electronic Signature Standards (45 CFR Part 142) imposes a comprehensive set of security requirements for "covered entities" that "electronically maintain or transmit any health information relating to an individual." The regulations pertaining to "Administrative Procedures to Guard Data Integrity, Confidentiality, and Availability" includes a requirement for "Security Testing." Given the breadth of HIPAA requirements and the potential penalties for violators, state government requires an independent evaluation of compliance efforts.

Guidelines pertaining to federal Bioterrorism Preparedness and Response grants require "regular independent validataion and verification of Internet security, vulnerability assessment, and security and continuity of operations…" (Critical Capacity #13, Focus Area E – Health Alert Network / Communications and Information Technology).

The National Strategy to Secure Cyberspace recommends that state and local governments "establish IT security programs … including awareness, audits, and standards."

In 2003, the Office of the CIO engaged Omnitech Corporation to conduct an external perimeter security sweep of the state's network. The initial evaluation took place during April to June of 2003. This included an automated vulnerability scan and testing of devices exposed to the Internet. In March 2004, Omnitect conducted a second vulnerability scan of the state's network.

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

1. Describe the project, including:
   - Specific goals and objectives;
   - Expected beneficiaries of the project; and
   - Expected outcomes.

   The purpose of conducting a current-state Information Security Assessment is to obtain a realistic measure of the potential exposures to which information resources of state agencies are exposed. This provides a baseline and corrective action priority list so that appropriate counter measures can be implemented. Managing risks requires identification of threats, their impact, and severity under certain conditions.

Specific goals and objectives include:

- Identify security problems and vulnerabilities;
- Recommend remedial steps;
- Promote attention to security issues and the use of best practices to improve security of information systems.

Additional objectives will be developed in conjunction with the Security Work Group.

State agencies are the direct beneficiaries of this project by getting advice about the security of computer systems that they use. Policy makers and the general public are indirect beneficiaries, if the project results in better security.

The RFP will establish specific outcomes and deliverables. They will include but not be limited to:

- Project plan
- Progress reports
- Findings and recommendations (non-public information)
- Summary of results (public document)
- Onsite presentation of findings and recommendations (non-public meeting)

2. Describe the measurement and assessment methods that will verify that the project outcomes have been achieved.

The CIO will review project deliverables against the requirements in the RFP and contract. The Security Work Group and agencies involved in the security assessment will have an opportunity to evaluate the deliverables. Agencies will be asked to respond to findings and recommendations specific to their operations.

3. Describe the project's relationship to your agency comprehensive information technology plan.

The mission of the CIO/NITC is "…to make the State of Nebraska's information technology infrastructure more accessible and responsive to the needs of its citizens, regardless of location, while making investments in government, education, health care and other services more efficient and cost effective." The basic strategy used by the office to achieve this mission has been to bring together representatives of various groups having an interest in information technology to share information, determine needs, aggregate demand, and collaborate on all matters relating to the mission. To achieve this, the NITC has created three councils (representing communities, education, and state government), a Technical Panel, and various working groups, which meet regularly and provide input to the NITC.

The project directly supports one of the NITC Strategic Initiatives (Security and Business Resumption). Security has also been a long-standing priority of the State Government Council and Technical Panel: "The State Government Council, in coordination with the Technical Panel, will work to implement (the NITC security) policies in state government."

Section IV: 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).

Tangible: Economic cost/benefit analysis;
Because this is a study, it will not create any direct economic benefits.

The information and recommendations stemming from the study have the potential for creating indirect economic benefits by avoiding the cost of security breaches that are avoided by implementing the recommendations of the study.

Intangible: Benefits of the project for customers, clients, and citizens and/or benefits of the project for the agency;
Below are several intangible benefits:

- The NITC fulfills its statutory mandate to develop broad strategies and encourage collaboration in the area of information technology.
- The State Government Council makes progress on its priority relating to security.
- Policy makers will know that a process is in place to evaluate the security of information technology systems.

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.

Other solutions that were evaluated and why they were rejected. Include their strengths and weaknesses. Explain the implications of doing nothing and why this option is not acceptable.

One option is to rely on individual agencies to sponsor security assessments of their systems. This is a poor option, because of the high degree of interdependency among agencies. Only an enterprise approach is effective for testing the overall security of the state's information systems.

Another option is to have one or more state agencies conduct the security assessment for all of state government. This option has several disadvantages, including lack of time and the need for an independent perspective. Some aspects of security audits and assessments require specialized knowledge and tools.

Doing nothing violates NITC security policies and increases the state's exposure to security vulnerabilities.

6. If the project is the result of a state or federal mandate, please specify the mandate being addressed.

The project will comply with NITC security policies and identify potential issues pertaining to several federal security regulations. In addition, there are several federal laws and regulations regarding privacy and security of information. These include HIPAA (Health Insurance Portability and Accountability Act), IT Requirements for Public Health Preparedness and Response for Bioterrorism (Center for Disease Control), Sarbanes-Oxley Act of 2002, Help America Vote Act of 2002 (HAVA), Graham-Leach-Bliley Act (GLBA), and the Family Education Rights and Privacy Act (FERPA).

An additional justification for attention to computer security issues is the National Strategy to Secure Cyberspace, published by the Department of Homeland Security in February 2003. One of the priorities of

the national cyberstrategy is "Securing Governments' Cyberspace." The foundation for the federal government's cybersecurity includes:

- Assigning clear and unambiguous authority and responsibility for security priorities;
- Holding officials accountable for fulfilling those responsibilities, and
- Integrating security requirements into budget and capital planning processes.

The national cyberstrategy encourages state and local governments to "establish IT security programs for their departments and agencies, including awareness, audits, and standards; and to participate in the established ISACs (Information Sharing and Analysis Centers) with similar governments."

Section V: 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.

   The project does not require the purchase of hardware, software or communications equipment. Findings and recommendations of the security assessment will help address security issues with existing and future technology systems. The primary strength of the proposed approach is that it will provide an independent assessment of specific security issues. The primary weakness is that the scope will be very limited in order to stay within budget.

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 project does not involve issues of reliability, security, and scalability in the usual sense.

   - Address conformity with applicable NITC technical standards and guidelines (available at http://www.nitc.state.ne.us/standards/) and generally accepted industry standards.

     The project will help with implementing security policies and with developing standards, guidelines, and best practices pertaining to security.

   - Address the compatibility with existing institutional and/or statewide infrastructure.

     The project will identify new recommendations and options for security.

Section VI: 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.

   Project implementation will include developing an RFP, selecting a qualified company to conduct the security assessment, preparing a detailed work plan, and then performing the work..

Project sponsor(s) and stakeholder acceptance analysis;

- The project sponsor is the Chief Information Officer.
- The main issue regarding stakeholder acceptance is whether state agencies will cooperate with the consultant in conducting the study and implementing any recommendations. The project will seek stakeholder acceptance by involving affected agencies in the study. Agencies will be involved in refining the scope of the study, developing the RFP and vendor selection.

The project team will include the CIO, consultants, and agency representatives. The RFP and detailed work plan will define the roles and responsibilities of each participant. The consultant will provide the methodology and expertise to conduct the security assessment.

10. List the major milestones and/or deliverables and provide a timeline for completing each.

Milestone	Date	Deliverable
Submit Budget Request	September 15, 2004	Project Proposal Form
Obtain Budget Authorization	June 1, 2005	Appropriations Bill
Determine Scope (Security Work Group)	November 1, 2005 (and November 1, 2006)	Draft Scope of Work
Develop RFP and Selection Process	December 1, 2005 (and December 1, 2006)	Project charter, RFP, etc.
Select consultant	January 15, 2006 (and January 15, 2007)	
Develop detailed work plan	January 30, 2006 (and January 30, 2007)	Work Plan
Conduct security assessment	March 31, 2006 (and March 31, 2007)	Preliminary findings
Prepare draft recommendations	April 30, 2006 (and April 30, 2007)	Draft recommendations
Submit final documents	May 15, 2006 (and May 15, 2007)	Final documents

11. Describe the training and staff development requirements.

Because it is a study, the project does not require any training or staff development, except that the presentation of findings and recommendations provide an opportunity for exchanging information and knowledge. Past security assessments included the opportunity for agency staff to be involved during the vulnerability testing phase, as a training exercise. The scope of the RFP will determine whether this is offered again.

12. Describe the ongoing support requirements.

Agencies may need technical assistance in implementing the findings and recommendations.

Section VII: Risk Assessment (10 Points)

13. Describe possible barriers and risks related to the project and the relative importance of each.

Below are several potential risks, listed in declining order of importance:

- Some aspects of security testing could disrupt agency operations;
- Not gaining the cooperation of key stakeholders;
- Not achieving the entire scope of the project;
- Not finding qualified experts who will fulfill the goals of the study;
- Not following the timeline.

14. Identify strategies, which have been developed to minimize risks.

Below are strategies for addressing these risks:

- The RFP, contract, and work plan will place a high priority on not disrupting agency operations.
- Key stakeholders will be invited to participate in every aspect of the study.
- For the dollars available, it will be difficult to achieve all of the objectives of the study. There are two strategies to address this risk. First, the CIO is prepared to devote time to help coordinate the study. Second, participating agencies will need to cooperate in implementing recommendations.
- The RFP process and involvement of stakeholders in the vendor selection process will help insure that we choose a qualified consultant to conduct the study.
- The timeline is fairly aggressive to achieve a completed study by the end of May 2004. It is also a rather artificial timeline, since it is done without a detailed work breakdown structure or input from the consultant. As project sponsor, the CIO has responsibility to keep the project on track. There are no major consequences of missing the timeline.

Section VIII: 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)

The budget request is for $50,000 per year in cash fund authority. The source of cash fund will be the Information Technology Infrastructure Fund. Effort will be made to identify additional funding sources.

16. Provide a detailed description of the budget items listed above. Include:
    - An itemized list of hardware and software.

      No hardware or software will be purchased.

    - If new FTE positions are included in the request, please provide a breakdown by position, including separate totals for salary and fringe benefits.

      No new FTE are included in the request.

    - Provide any on-going operation and replacement costs not included above, including funding source if known.

      The project is for contractual services to conduct the security assessment.

    - Provide a breakdown of all non-state funding sources and funds provided per source.

      Discussions are underway regarding the potential availability of federal matching funds or grants.

17. Please indicate where the funding requested for this project can be found in the agency budget request, including program numbers.

Agency 65, Program 101 (CIO), Subprogram 07.