Nebraska Information Technology Commission

Government Technology Collaboration Fund - 2004
Grant Application Form

For more information about Government Technology Collaboration Fund grants, see the Grant Guidelines at http://www.nitc.state.ne.us/sgc/grants/.

Contact information for questions regarding this form:
Rick Becker
Office of the NITC
521 S 14th Street
Lincoln, NE 68508
(402) 471-7984
rbecker@cio.state.ne.us

Section I: General Information

A. Project Title: Security Assessment

Submitting Agency (or Agencies): Office of the Chief Information Officer

Contact Information for this Project

Name:	Steven Schafer
Address:	521 South 14th Street, Suite 301
City, State, Zip:	Lincoln, NE 68508-2707
Telephone:	402 471-4385
E-mail:	slschafe@notes.state.ne.us

B. Certification for Request
I certify that to the best of my knowledge the information in this application is correct and that the application has been authorized by this entity to meet the obligations set forth in this application.

Name:	Steven Schafer
Title:	Chief Information Officer
Agency:	Office of the Chief Information Officer
Date:	August 31, 2001

Total Grant Funds Requested:	$75,000
Total Project Costs:	$95,000

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 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.

The purpose of this grant is to engage a qualified firm to conduct a security assessment of the information technology infrastructure for state government.

Section III: Goals and Objectives

1. *Describe the project, including the specific goals and objectives.*
   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.

2. Describe the project's relationship to the agency's comprehensive 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."

3. Describe, if applicable, how this project furthers the implementation of electronic government. [Preference will be given to projects, which support the State Government Council's priority of implementing electronic government as reflected in the goals of the Business Portal Action Plan and the E-Government Strategy (available at http://www.nitc.state.ne.us/sgc/).]

   Adequate security must be in place for e-government. The state's E-Government Strategy, Business Portal Action Plan, and draft e-government architecture all recognize the importance of addressing security issues. This project will build awareness of security issues, identify potential areas of weakness, and recommend improvements.

Section IV: Scope and Projected Outcomes

Describe the project's specific scope and projected outcomes. The narrative should address the following:

1. Beneficiaries of this project and the need(s) being addressed;
   State agencies will benefit by gaining additional insight into the adequacy of security efforts.

   Policy makers will benefit by knowing that security policies are being implemented and that the security of information systems is subject to periodic testing.

   Citizens will benefit from improvements to security of information resources.

   All three groups will benefit from steps that avoid the potential costs of non-compliance.

2. Expected outcomes of the project;
   The primary outcome of the project will be a report with findings and recommendations. The specific scope will be developed in conjunction with the Security Work Group. Tasks may include, but not be limited to:
   - Conducting an external vulnerability scan of the state's network and computer assets that are exposed to the Internet to identify known security vulnerabilities (two scans, every six months);

- Performing controlled assessment activities (manual and automated) on these primary network devices to exploit the vulnerabilities uncovered by the scans (two scans, every six months);
- Searching for unsecured wireless networks of state agencies (single engagement);
- Evaluating internal network security practices (single engagement);
- Evaluating application-level security for selected agencies (single engagement).

3. Measurement and assessment methods that will verify project outcomes;
   The scope of work, deliverables and detailed work plan will have sufficient specificity to evaluate whether the study achieves its stated purpose. Some aspects of the study will be subjective. Involvement of the State Government Council, Technical Panel, Security Work Group and other stakeholders (through the Security Work Group) will help assure a process for assuring a quality product.

Section V: Project Justification / Business Case

Please provide the project justification in terms of tangible benefits (an economic return on investment) and/or intangible benefits to the agency or the public. The narrative should address the following:

1. Tangible: Economic cost/benefit analysis;
   The proposed project will cost $95,000. 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.

2. 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 test the security of information technology systems.

3. 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.

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

4. If the project is required to comply with a state or federal mandate, please so indicate.
   The project will comply with NITC security policies and identify potential issues pertaining to several federal security regulations.

Section VI: Implementation

Describe the implementation plan -- from design through installation and ongoing support -- for the project. The narrative should address the following:

1. 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.

2. Define the roles, responsibilities, and required experience of the project team;
   The project team will include the CIO, consultants, and agency representatives. A project charter 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.

3. List the major milestones and deliverables for each milestone;

Milestone	Date	Deliverable
Submit grant application	June 30, 2004	Project Proposal Form
Obtain NITC approval	September 9, 2004	
Determine Scope (Security Work Group)	November 1, 2004	Draft Scope of Work
Develop RFP and Selection Process	December 1, 2004	Project charter, RFP, etc.
Select consultant	January 15, 2004	
Develop detailed work plan	January 30, 2004	Work Plan
Conduct security assessment	March 31, 2004	Preliminary findings
Prepare draft recommendations	April 30, 2004	Draft recommendations
Submit final documents	May 15, 2004	Final documents

4. Training and staff development requirements and procedures;
   Because it is a study, the project does not require any training or staff development.

5. Ongoing support requirements, plans and provisions.
   Agencies may need technical assistance in implementing security recommendations.

Section VII: Technical Impact

Describe how the project enhances, changes or replaces present technology systems, or if new systems are being added. The narrative should address the following:

1. Descriptions of hardware, software, and communications requirements for this project.
   Describe the strength and weaknesses of the proposed solution;
   The project does not require the purchase of hardware, software or communications equipment.

2. Issues pertaining to reliability, security and scalability;
   The project does not involve issues of reliability, security, and scalability in the usual sense.

3. 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 developing standards and guidelines pertaining to security.

4. Compatibility with existing institutional and/or statewide infrastructure.
   The project will identify new recommendations and options for security.

   The project will take into consideration other studies and efforts that are relevant to providing secure information technology systems. These include:
   - Security policies and procedures;
   - IMServices' Security and Directory Services Evaluation

Section VIII: Risk Assessment

Describe possible barriers and risks related to the project. The narrative should address the following:

1. List the identified risks, and relative importance of each;
   Below are several potential risks, listed in declining order of importance:
   - 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.
2. Identify strategies, which have been developed to minimize risks.
   Below are strategies for addressing these risks:
   - 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 IX: Financial Analysis and Budget

1. Provide the following financial information:

	GTCF Grant Funding	Cash Match	In-Kind Match	Other Funding Sources	**Total**
Personnel Costs			20,000		20,000
Capital Expenditures (Hardware, software, etc.)					
Contractual Services	75,000				75,000
Supplies and Materials					
Telecommunications					
Training					
Travel					
Other costs					
Total	75,000	❶	20,000 ❷		95,000 ❸

2. Provide a detailed description of the budget items appearing above.
   The in-kind match reflects staff time of the CIO and agencies that participate in the study. This includes administrative support, time spent developing the RFP, vendor selection, contract management, agency participation in the security assessment, and implementation of recommendations.

3. Match Requirement: This grant requires a 25% match from the agency. Please use the calculation below to ensure your application meets this requirement.

$$\frac{\text{Total Cash Match } \$0 + \text{Total In-Kind Match } \$20{,}000}{\text{Total Project Cost } \$75{,}000} \quad \$ \quad 0.25$$