Date of Last Revision: March 7, 2005

Nebraska Information Technology Commission Strategic Initiatives

Strategic Plan For
E-Government

Objectives

In a memo to all agencies dated November 19, 2003 (http://www.cio.state.ne.us/e-gov/Automation.pdf), the Governor identified four management principles for e-government:

1. It should be easy for citizens and businesses to find information regarding government;
2. The administrative burden of complying with government requirements should be as minimal as possible;
3. Self-service should be an option, if at all feasible; and
4. Government should present an integrated view of government information and services.

E-government is a continuous process of using technology to serve citizens and improve agency operations. Technology creates new opportunities for major change, including self-service, integration of information and services, and elimination of time, distance and availability of staff as constraint to providing information and services. An enterprise approach and cooperation of multiple jurisdictions are critical to achieving the goals of e-government, in order to integrate information and services and allow the easy exchange of information.

Benefits

The primary benefits of e-government are:

1. Improved services for citizens and businesses.
2. Increased efficiency and effectiveness for agencies.

Current Status

Where we are...

Since the adoption of the first *E-government Strategic Plan* in 2000, state agencies have continued to make progress toward the vision of having Nebraska government be open for business from any place and at any time through the use of e-government. The two major sources of this progress have been, first, from individual and collaborative agency initiatives and second, from enhancements to the state's Web portal, Nebrask@ Online (NOL). The following is a look at where we are in development of e-government services in state government. It is not intended to be a comprehensive list of all efforts but a general overview of the progress made since the first adoption of a strategic plan.

Looking at improvements in the state's Web portal, Nebrask@ Online, is a good starting point for this review because the portal is the front door for e-government in Nebraska. In 2000 the portal was redesigned to better serve citizens and businesses. The redesigned site presents information in categories, which reflected how users would most likely look for information and services. The idea behind the redesign was that users should be able to find the information they were seeking without having to know which specific agency or division of state government was responsible for that information or service. The goal was to get the user to the information they needed within two mouse clicks. The redesigned site was nationally recognized in 2001, 2002, and 2004 as a finalist in the "Best of the Web" competition, meaning the state's Web portal was in the top ten of state Web portals.

Building on the theme of categorizing information by topic, the next major revision to Nebrask@ Online involved creating "sub-portals" or "second-level portals." Each sub-portal provides a specific user group with information and value-added services of interest to that group. Sub-portals have been created for the following areas: business, citizen, education, and state employees.

Nebraska@ Online for Business was the first operational sub-portal, launched in May 2002. The site offers a number of features of value to the business community, two of which are a database of business forms and a customizable portfolio. The database contains information and links to more than 1200 state government forms that are used to regulate or otherwise interact with businesses. This database can be searched in a variety of ways, and can retrieve information without regard for the responsible agency. In this way, the user does not have to be familiar with which agency handles a form in order to obtain the information. An upgrade to Nebrask@ Online for Business and the forms inventory began in August 2004.

The other sub-portals -- Nebrask@ Online for Education, Nebrask@ Online for Citizens, and Nebrask@ Online for State Employees -- each provide the user group with an enhanced presentation and delivery of e-government information and services.

NOL has also implemented a "Payment Portal." This portal provides an enterprise approach to payment processing for e-government services. All online services can use a single payment portal to collect funds associated with the various e-government services provided. The portal will eliminate the need to recreate a payment system for each online application. The payment portal can process credit card, debit card or electronic check payments.

In addition to work on the state portal and sub-portals, NOL has developed and launched several specific e-government applications, including interactive electrical permits; water well registrations, more than 80 online professional license renewals for nine different agencies; and tax filing applications for income, sales and withholding taxes. Work is underway on a one-stop business registration system that will provide a single Web interface for several agency registration processes.

Since publication of the first e-government strategic plan, state agencies have added considerable content and many interactive services to their websites. A few examples include:

- Game and Parks Commission – Online campground and lodging reservations (http://www.ngpc.state.ne.us/parks/permits/reserve.asp)
- Department of Revenue – Tax Forms and online tax filing options such as Individual Income Tax forms 1040NS, 1040N; Sales and Use Tax Form 10; and the 941N for withholding payments (http://www.revenue.state.ne.us/electron/e-file.htm)
- Depatment of Labor – UIConnect for unemployment insurance taxes (http://www.dol.state.ne.us/)
- Public Employees Retirement System – Access to Pension-Related Information (http://www.npers.ne.gov/home.jsp)
- State Treasurer – Child Support Website (https://www.nebraskachildsupport.state.ne.us/)
- Nebraska Supreme Court – Court Records Retrieval System
- Nebraska Workers' Compensation Court - Claims Administrator's Extranet First Report of Injury Search Application

This background information is intended to show the basic direction of e-government activities since 2000. A more complete listing of e-government services is available at: http://www.state.ne.us/egov.html.

Digital State Survey

One measure of the progress we have made in implementing e-government is to look to national reports on e-government. The Center for Digital Government has conducted a detailed survey of digital government in all 50 states, called the "Digital State Survey."[1] Looking at how Nebraska has scored provides a tool for measuring our progress. However, as with all surveys, there are elements of subjectivity in this survey -- what is deemed an important aspect of e-government for those conducting the survey may not necessarily align with our focus in Nebraska. With that note, here is table showing how Nebraska has scored:

Digital State Survey Results				
Category	**2000 Ranking**	**2001 Ranking**	**2002 Ranking**	**2004 Ranking**
Electronic Commerce / Business Regulation	28	25	Unranked (>25th)	Not Available
Taxation / Revenue	29	9 (tie)	1 (tied)	Not Available
Law Enforcement / Courts	12	Unranked (> 25th)	Unranked (> 25th)	Not Available
Social Services	9	5 (tie)	7 (tie)	Not Available
Digital Democracy	13	3	17	Not Available
Management / Admin.	10	22	Unranked (>25th)	Not Available
Education	K-12: 31st Higher Ed: 17th	20	14 (tied)	Not Available
GIS / Transportation	(New category in 2001)	Unranked (> 25th)	21 (tied)	Not Available
Aggregate Ranking	14th	17th	Unranked (>25th)	22

[1] http://www.centerdigitalgov.com/

To move into the top ten, Nebraska must accomplish the following:

- Prepare a comprehensive strategy for online licensing;
- Develop an online business registration system;
- Provide online criminal history background checks;
- Establish a marketing strategy to improve adoption rates;
- Require testing and management tools for accessibility;
- Require online privacy statements;
- Provide an online system where constituents can request services, report problems, complain about services, and complete citizen satisfaction surveys about state services;
- Develop and implement an enterprise architecture for information technology;
- Provide an enterprise approach for knowledge resource management (including content management, business process automation, directory services, registries and repositories, and digital archive), and
- Provide an enterprise approach to security services.

Future

Where we are going...

This plan is the State Government Council's communication of where Nebraska state government needs to direct its efforts to achieve the greatest benefits from e-government. The vision and goals for e-government are:

Vision: The State of Nebraska will be open for business from any place and at any time through the use of e-government.

Goal 1: Government-to-Citizen and Government-to-Business
Anyone needing to do business with state government will be able to go to the state's Web site, easily find the information or service they need, and if they desire, complete all appropriate transactions electronically.

Goal 2: Government-to-Government
State agencies will improve services and increase the efficiency and effectiveness of government operations through collaboration, communication, and data sharing between government agencies at all levels.

Goal 3: Government-to-Employee and Internal Operations
Agencies will examine internal operations to determine cost-effective e-government applications and solutions. The purpose of these efforts is to improve efficiency and effectiveness by replacing manual operations with automated techniques. Automating internal operations is often a prerequisite for improving public access to information and services.

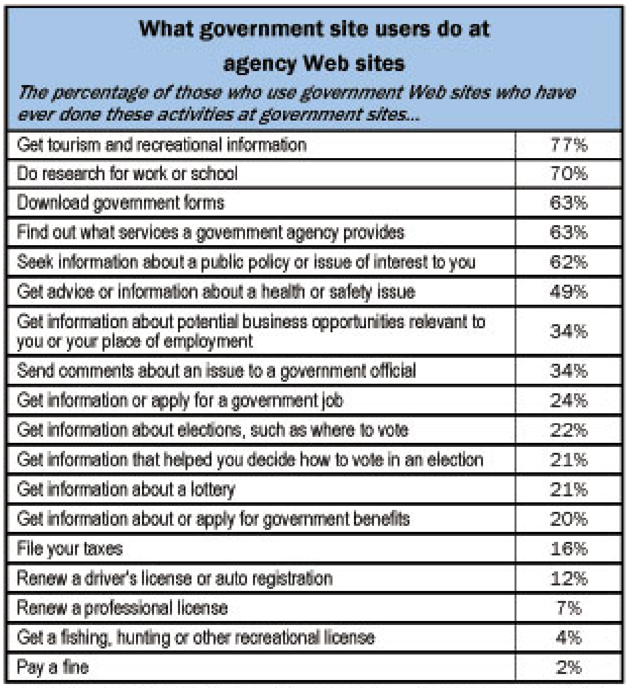
How citizens and businesses use e-government.

These goals are consistent with the expectations of citizens and businesses. A recent survey found that approximately 71 million Americans had sought information from a government Web site. This same survey also showed that 82% of Internet users "expect" to get the information or service they need from the agency's Web site.[2]

When businesses were surveyed about which activities they would like to perform online, 43% reported they would like to use the Internet to obtain or renew professional licenses and 39% wanted access to one-stop shopping to apply for all new business licenses and permits. Other services sought by business users, as reported by the survey, included: 38% access to criminal history background checks; 36% apply for a business permit; 34% obtain a limited criminal history report. Businesses sited the benefits of participating in e-government as: speed (51%); convenience - no line (43%); and better hours (22%).[3]

Citizens also reported improved interactions with government when using government Internet sites. Overall, 60% of government Web site users say such sites had improved their interaction with at least one level of government, and 45% said it had improved the way they interact with state government.[4]

The following table shows what government site users do at agency Web sites[5]:



What government site users do at agency Web sites

The percentage of those who use government Web sites who have ever done these activities at government sites...

Get tourism and recreational information	77%
Do research for work or school	70%
Download government forms	63%
Find out what services a government agency provides	63%
Seek information about a public policy or issue of interest to you	62%
Get advice or information about a health or safety issue	49%
Get information about potential business opportunities relevant to you or your place of employment	34%
Send comments about an issue to a government official	34%
Get information or apply for a government job	24%
Get information about elections, such as where to vote	22%
Get information that helped you decide how to vote in an election	21%
Get information about a lottery	21%
Get information about or apply for government benefits	20%
File your taxes	16%
Renew a driver's license or auto registration	12%
Renew a professional license	7%
Get a fishing, hunting or other recreational license	4%
Pay a fine	2%

Source: Pew Internet & American Life Project Government Web Site Survey, September 5-27, 2001. N=815. Margin of error is ±4%.

[2] Horrigan, J., *Counting on the Internet*, Pew Internet & American Life Project, http://www.pewinternet.org/, December 29, 2002

[3] *Benchmarking the eGovernment Revolution*, Momentum Research Group of Cunningham Communications (Commissioned by NIC), July 26, 2000.

[4] Larsen, E., *The rise of the e-citizen*, Pew Internet & American Life Project, http://www.pewinternet.org/, April 3, 2002.

[5] Ibid.

Best practices in other states.
As part of the Digital State Survey, the Center for Digital Government also looks at "best practices" in other states. The following is a list of some of these e-government best practices:

URL	Project Title	Category
http://www.michigan.gov/doingbusiness	Michigan Doing Business with the State (e-procurement system)	Architecture
http://www.oit.state.pa.us/oaoit/site/default.asp	Pennsylvania PA-Dynamic Site Framework (web content management tool)	Architecture
http://www.access.wa.gov	Washington Ask George (user friendly search tool)	Architecture
http://www.truckingks.org	Kansas E-Truck Stop (online access for motor carriers)	Business Portal
http://www.choosemaryland.org	Maryland Choosemaryland.org (business portal and site selection tool)	Business Portal
http://www.etides.state.pa.us/	Pennsylvania E-TIDES (common tax filing system for Revenue and Labor)	Business Portal
http://www.paopen4business.state.pa.us/	Pennsylvania Open for Business (online access for businesses)	Business Portal
http://www.townhall.state.va.us	Virginia Regulatory Town Hall (tracking rules and regulations)	Business Portal
http://www.sbe.state.va.us	Virginia Absentee Ballot Tracking	Citizen Portal
http://www.sots.state.ct.us/	Connecticut Campaign Finance Information System (electronic campaign filing system)	Citizens Portal
http://www.cyberdriveIllinois.com	Illinois Online Services for Motorists (central access to all MV-related services)	Citizens Portal
http://www.state.in.us/apps/lsa/session/billwatch/	Indiana BillWatch (bill tracking and e-mail updates)	Citizens Portal
http://legis.state.sd.us/mylrc/index.cfm	South Dakata My Legislative Research (customized bill tracking and e-mail notification)	Citizens Portal
http://www.coloradomentor.org/	Colorado Mentor Program (online resources for university admissions)	Education Portal
http://www.umuc.edu/	University of Maryland University College (online education model)	Education Portal
http://www.gis.state.ar.us/defaultIE.htm	Arkansas GeoStar (Internet-based GIS data clearinghouse)	GIS
http://www.sscgis.state.or.us/	Oregon Geospatial Data Clearinghouse	GIS
http://www.eva.state.va.us/	Virginia eVA (procurement system for state and local government)	Procurement
http://www.wa.gov/dis/academy/index.htm	Washington Digital Government Applications Academy	Training

Recommended Actions

(NOTE: These recommendations are still subject to change, pending additional advice from those entities that are participating in this strategic initiative.)

Goal 1: Government-to-Citizen and Government-to-Business

Citizen Portal Enhancements
The citizen portal, Nebrask@ Online for Citizens (http://www.nebraska.gov/citizen/), was launched in 2003. The following are specific actions and recommendations for value-added enhancements to this portal.

1.1 Work with the Secretary of State's Office to provide enhancements to election related information and services.
   a. Lead Entity: Nebrask@ Online Manager ("NOL") in cooperation with the Secretary of State's Office
   b. Timeframe: TBD
   c. Funding: Secretary of State / NOL

d. Status (March 2005): Completed. Enhancements made for November 2004 election.

1.2 Work with the Accountability and Disclosure Commission to provide for secure online filings and improved access to information.

a. Lead Entity: NOL (in cooperation with the Accountability and Disclosure Commission
b. Timeframe: January 31, 2005
c. Funding: State Records Board Grant
d. Status (March 2005): Improvements to information access completed, to be posted. Online filing on hold.

1.3 Work with the Legislature to provide additional tools to track legislative information. The Nebrask@ Online Manager is developing additional features, including the ability to track multiple bills from one location and the use of e-mail "push" technology.

a. Lead Entity: NOL (in cooperation with the Legislature Council)
b. Timeframe: November 1, 2004
c. Funding: State Records Board Grant
d. Status (March 2005): Completed.

1.4 Work with the Department of Motor Vehicles to provide for online vehicle registration and drivers license renewal. DMV is in the process of implementing two systems -- insured motorists database and digital drivers license system -- which will allow for the future deployment of these online services.

a. Lead Entity: Department of Motor Vehicles
b. Timeframe: TBD
c. Funding: DMV
d. Status (March 2005): No change.

1.5 Work with the Nebrask@ Online Manager and county officials to provide the means for online payment of property taxes and other local fees.

a. Lead Entity: NOL (in cooperation with county governments)
b. Target Completion Date: TBD
c. Funding: NOL (Reinvested Revenue)
d. Status (March 2005): State Records Board grant application submitted for a pilot project with six counties.

1.6 Prepare a comprehensive strategy for online licensing of regulated professionals.

a. Lead Entity: Office of the CIO
b. Target Completion Date: December 31, 2004
c. Funding: NOL (Reinvested Revenue)
d. Status (March 2005): Work ongoing.

Business Portal Enhancements

The business portal, Nebrask@ Online for Business (http://www.nebraska.gov/business/), was launched in May 2002. The following are specific actions and recommendations for value-added enhancements to this portal.

1.7 Working with the various agencies involved in business registration -- including the Secretary of State, Department of Revenue, and Department of Labor -- create an online system for business registration.

a. Lead Entity: Office of the CIO
b. Timeframe: TBD (Pending requirements analysis by NOL)
c. Funding: NOL (Reinvested Revenue)
d. Status (March 2005): Work group established. Analysis underway by NOL and agencies.

1.8 Prepare a report on the barriers and options for providing online access to certain, limited, criminal history information.

a. Lead Entity: Office of the CIO (in cooperation with the Nebraska State Patrol)
b. Timeframe: May 31, 2005
c. Funding: NOL No funding needed for this analysis
d. Status (March 2005): On hold.

1.9 Develop an online application for use by businesses attempting to find a suitable site for business development.

a. Lead Entity: Office of the CIO
b. Timeframe: TBD (Pending requirements analysis by NOL)
c. Funding: State Records Board Grant or NOL (Reinvested or Enhanced Revenue)
d. Status (March 2005): No change.

1.10 Improve the business forms database maintained by NOL and enhance the search capabilities.

a. Lead Entity: NOL and Office of the CIO
b. Timeframe: October 31, 2004
c. Funding: State Records Board Grant
d. Status (March 2005): Work on application completed, work on data is ongoing.

Education Portal
The Education Portal (http://www.nebraska.gov/education/) first became available to the general public in February 2003. The following are specific actions and recommendations for value-added enhancements.

1.11 Under sponsorship of the Education Council of the NTIC, The Nebrask@ Online Manager will work with the Education Council educational institutions to provide enhancements to the Education Portal, including but not limited to:

- Information Technology Training Calendar;
- Searchable database of educational courses, degrees, and programs;
- Statewide application for admission to higher education institutions.

a. Lead Entity: Office of the CIO / Education Council
b. Timeframe: TBD
c. Funding: State Records Board Grant
d. Status (March 2005): Information Technology Training Calendar under development; Searchable Database project terminated, no plan to continue, another source provides similar information; Statewide Application for Admission, project terminated, no plan to continue.

1.12 The Department of Education is developing online teacher/administrator certification.

a. Lead Entity: Department of Education
b. Timeframe: November 2004
c. Funding: NDE
d. Status (March 2005): Completed.

Goal 2: Government-to-Government

2.1 Develop strategies to address the following government-to-government activities:

- Intergovernmental Cooperation Groups. Expand upon current intergovernmental cooperative efforts like the CJIS Advisory Committee and GIS Steering Committee; and develop new cooperative groups for those agencies that have specific, shared interests.
- Integration of Government Information and Services. Develop strategies for using Internet technologies to provide integrated access to information and services to citizens, businesses, employees, and other governmental entities.
- Local Government Portal. Provide a one-stop Web site for information and services used by local governments.
- Forms Automation. Work with state agencies and political subdivisions to identify and prioritize opportunities for automating forms that local government uses to interact with state government.

a. Lead Entity: State Government Council
b. Timeframe: July 2005
c. Funding: None
d. Status (March 2005):
Intergovernmental Collaboration Groups: Status: The Juvenile Data Sharing Work Group (created by CJIS and SGC) sponsored a study to prepare a strategic plan for data sharing among entities providing services to children. That study will be finished in March 2005. The Steering Committee on Child Abuse and Neglect Information Exchanges prepared an interim report in October that recommended six short-term projects. MOAs for those projects have been signed (except for one) and those projects are now getting underway. Further information is available at: http://cio.nol.org/CTF/. In January, the Office of the CIO submitted an application to the National Governor's Association for a $50,000 grant to conduct a pilot project for using Global XML technology to enable existing systems to exchange data on child abuse cases. Nebraska's project is one of six out of 21 proposals, which was approved. We are waiting for the contract from NGA before initiating work.
Local Government Portal: On schedule to be incorporated into overall NOL site redesign currently planned for June 2005.
Integration of Government Information and Services: A Steering Committee is working on integrating the information system needs of the Foster Care Review Board into the NFOCUS system maintained by HHS.

Goal 3: Government-to-Employee and Internal Operations

3.1 State Employee Portal Enhancements. The State Government Council will identify specific improvements and value-added services to be incorporated into the state employee portal, Nebrask@ Online for State Employees (www.nebraska.gov/employee/).

a. Lead Entity: State Government Council
b. Timeframe: July 2005
c. Funding: None
d. Status (March 2005): No change.

Other Actions and Recommendations

4.1 Develop a marketing strategy to increase public awareness and the use of e-government services.

a. Lead Entity: NOL
b. Timeframe: TBD
c. Funding: NOL (Reinvested Revenue)
d. Status (March 2005): A meeting was held with agency PIOs on October 1 to explore different strategies for marketing. NOL has hired a marketing director. NOL is developing recommendations for the next State Records Board meeting.

4.2 Prepare draft standards for all agency home pages to include privacy and security statements.

a. Lead Entity: Webmasters Work Group
b. Timeframe: December 2004
c. Funding: None
d. Status (March 2005): Webmasters Work Group developed draft standard under review by the State Government Council. Draft security statement to be reviewed by the State Government Council and State Records Board.

4.3 The SGC will work with other entities to investigate ways of providing authentication, especially for first time encounters with users.

a. Lead Entity: Office of the CIO
b. Timeframe: December 2004
c. Funding: TBD
d. Status (March 2005): No change.

Date of Last Revision: March 7, 2005

Nebraska Information Technology Commission
Strategic Initiatives

Strategic Plan For
Security and Business Resumption

Objectives

This initiative will define and clarify policies, standards and guidelines, and responsibilities related to the protection of the state's information technology resources. Information security and business resumption will serve statutory goals pertaining to government operations and public records. These include:

1. Insure continuity of government operations (Article III, Section 29 of the Nebraska Constitution; Nebraska Revised Statutes Sections 28-901 and 84-1201);
2. Protect safety and integrity of public records (Nebraska Revised Sections 28-911, 29-3519, and 84-1201);
3. Prevent unauthorized access to public records (Nebraska Revised Statutes Sections 29-3519, 81-1117.02, and 84-712.02);
4. Insure proper use of communications facilities (Nebraska Revised Statutes Section 81-1117.02); and
5. Protect privacy of citizens (Nebraska Revised Statutes Section 84, Article 7).

Information security refers to policies and procedures that are aimed at preventing problems that would threaten the safety and integrity of information resources. Business resumption refer to plans and activities aimed at responding to an event in a manner that mitigates the severity of problems and accelerates recovery.

Benefits

A strategy for security and business resumption of information technology systems is essential for meeting the statutory objectives listed above. 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).

Some of the federal laws carry substantial penalties. In particular, HIPAA imposes civil penalties of up to $25,000 per person, per year, per standard as well as criminal penalties from $50,000 and one year in prison to $250,000 and 10 years in prison (when malice, commercial advantage and personal gain are involved).

Security is also important for protecting critical systems that impact large numbers of people in the state. A few examples include:

- Unemployment assistance ($2.2 million paid out per week to 18,000 people)
- Child support ($4.4 million paid per week to 20,000 recipients)
- Medicaid claims (156,000 claims per week; $21.4 million payments per week)
- NFOCUS payments for multiple human services programs ($26 million paid each month for 185,000 cases)
- State accounting and payroll system
- Law enforcement
- Tax collection
- Homeland Security functions

The FBI conducts an annual survey of computer security issues affecting U.S. corporations, government agencies, financial institutions, medical institutions, and universities. The 2004 CSI/FBI Computer Crime and Security Survey included the following findings:

- 79% of survey participants reported one or more security incidents;
- 78% reported virus attacks;
- 59% reported insider abuse of Net access;
- 49% reported laptop/mobile theft;
- 39% reported system penetration;
- 37% reported unauthorized access to information;
- 15% reported abuse of wireless networks;
- 10% reported misuse of public web applications, and
- 7% reported web site defacement.

The 2004 survey is available at: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf.

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.”

Adequate security is also essential to expansion of e-government. Surveys show that concerns about security is one reason that the public is cautious about using on-line services, especially for conducting financial transactions or providing personal information.

Current Status

Every version of the Statewide Technology Plan of the NITC has included one or more action items pertaining to security for information technology systems. Past achievements include:

- Establishing the Security Work Group, with broad representation from state government and education sectors, to provide a forum for sharing information and developing standards and guidelines. Agendas and minutes are located at: http://www.nitc.state.ne.us/tp/workgroups/security/index.htm).
- Adopting a comprehensive set of security policies in January 2001 by the NITC. These policies include: Information Security Management, Access Control, Disaster Recovery, Education, Training and Awareness, Individual Use, Network Security, and Security Breaches and Incident Reporting.
- Publishing three security handbooks tailored to security officers, IS technical staff, and the general user.
- Offering training on the use of the security handbooks.
- Developing detailed information on:
    - Incident Response and Reporting Procedures;
    - Disaster Recovery Planning Procedures;
    - Wireless Local Area Network Guidelines;
    - Remote Access Guidelines.
- Sponsoring a Security Awareness Day (July 15, 2002).

All NITC policies, handbooks, procedures and guidelines are available at: http://www.nitc.state.ne.us/standards/index.html (under Security Architecture).

In 2002, the Nebraska Emergency Management Agency (NEMA) added a provision to the State Emergency Operations Plan that requires "Each state agency and local government (to develop) a continuity of operations plan and a disaster plan for information technology." In 2003, NEMA awarded $75,000 to the Department of Administrative Services (DAS) for a "Continuity of Operations Study". DAS has contracted with a company specializing in developing business continuity plans. The outcome will be a complete business continuity plan for all divisions of DAS. It will also provide a template that can be used for other agencies. By including a 'train-the-trainer' concept as well as involving multiple agencies in the project, DAS intends to encourage development of business continuity plans in all agencies.

The NITC has also funded two security audits. In March 2004, Omnitech conducted a limited security assessment of the state's network. The external vulnerability scan identified a total of 2,720 potential vulnerabilities with the following breakdown: 91 high-risk, 640 medium risk, and 1,989 low risk. Twelve agencies had one or more high-risk vulnerabilities. Agencies are in the process of evaluating the assessments and what steps they need to take. Not all of the potential vulnerabilities can or should be removed but all of the high and medium risk vulnerabilities will be accounted for by the agency responsible for the host that is vulnerable. In 2003, the results were 3,262 potential vulnerabilities (136 high risk, 1,182 medium risk, and 1,944 low risk). Seventeen agencies last year had one or more high-risk vulnerabilities.

These summary statistics indicate some progress in reducing the number of potential vulnerabilities, but the March 2004 results underscore the need for more attention on securing our information assets.   These potential vulnerabilities may expose state government to the risk of disruption of services, legal liability, and financial loss.

Several agencies have undertaken special projects and initiatives to improve security of information technology systems. These include:

- Department of Administrative Services
    - Implemented layered security and firewall management of the state's network;
    - Developed directory services capability for better authentication and identity management;
    - Updating the disaster recovery plan for Information Management Services Division;
    - Distributing security notices from the Multi-State Information Sharing and Analysis Center to agency security contacts.
- Health and Human Services
    - Designated a security officer for information technology;
    - Implemented HIPAA Privacy and Security regulations;
    - Developing agency security policies and procedures;
- Department of Roads
    - Designated a security officer for information technology;
    - Updating the disaster recovery plan for information technology services;
    - Developing agency security policies and procedures.
- University of Nebraska
    - In collaboration with DAS-IMServices, NU is developing a shared, fast recovery capability, through mutual assistance of physically distant data centers. Fiber optic cable has been installed between the State and University.
    - Hired a University Information Security Officer
    - Work is progressing on the design and implementation of a Directory Service / Identify Management System.
    - Disaster recovery plan is going through major revisions to update and incorporate new options.
    - UN has implemented various firewalls in locations where it is needed.
    - Implemented a University-wide security focus group to share information, patch management, awareness training, incident reporting, and other educational opportunities.
    - University-wide licensing for McAffee Anti-Virus Software
    - Implemented various federally mandated regulations (HIPAA, GLBA, FERPA).
- Multiple Agencies
    - Implementing recommendations stemming from the March 2004 Network Perimeter Security Sweep.

Future

Security is a continuous effort to manage the risk to information systems. The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected. Security must be balanced against other business needs, such as providing public access or remote access to information.

The previous section demonstrates the progress that is being made. Further improvement in security and disaster recovery is needed in several areas:

- Monitor and reduce the number of vulnerabilities of computer systems;
- Provide better patch management, including enforcement of patch management policies;
- Promote survivability of systems as a security strategy;
- Demonstrate the ability to recovery critical computer systems following a disaster, including table top exercises of disaster recovery plans;
- Improve awareness on the part of users regarding security policies and sound security practices;
- Insure adequate security for wireless systems through encryption capabilities and other means;
- Deploy intrusion detection and protection technologies to protect critical infrastructure;
- Provide redundant services for critical infrastructure such as additional Internet access points;
- Plan for additional infrastructure to extend the distances for shared disaster recovery facilities.

Finding cost effective and workable solutions to these problems is essential to a good security program for state government.

Recommended Actions

(NOTE: These recommendations are still subject to change, pending additional advice from those entities that are participating in this strategic initiative.)

SECURITY

A. Conduct annual independent security audits

In the latest computer crime survey by the FBI, 82 percent of respondents indicated that their organizations conduct security audits. Multiple federal programs require periodic computer security audits, including HIPAA, HAVA, and Bioterrorism grants from the Center for Disease Control. Computer security audits are a widely accepted best practice across the public and private sector.

Actions include:

1. Request funding for the CIO to contract for security audits.
   a. Lead Entity: CIO
   b. Timeframe: September 1, 2004
   c. Funding: No funding required for this task
   d. Status (March 2005): Completed.
2. Investigate opportunities for aggregating efforts of several state agencies that face federal requirements for security audits.

   a. Lead Entity: CIO
   b. Timeframe: November 1, 2004 (and on-going)
   c. Funding: No funding required for this task
   d. Status (March 2005): Working with agencies.
3. Prepare RFP and Scope of Work
   a. Lead Entity: CIO (with assistance from Security Work Group)
   b. Timeframe: January 31, 2005
   c. Funding: If technical assistance is required for preparing the RFP, the cost will be paid either from the NITC grant or the budget of the Office of the CIO.
   d. Status (March 2005): RFP underdevelopment, to be released Spring/Summer 2005.
4. Conduct 2005 Security Audit
   a. Lead Entity: CIO
   b. Timeframe: April 30, 2005
   c. Funding: A grant application is pending before the NITC. The CIO is requesting funding for annual security audits as part of the FY2006 / FY2007 budget request.
   d. Status (March 2005): Pending release of RFP.

B. Implement centralized directory services

An analysis of security risks identified the need for an Enterprise Directory that provides identity management, single sign on, and role-based/policy-based authorization. In response to this need, IMServices is now implementing a directory services system that will be available to all agencies. Under the direction of the CIO and the NITC, a Work Group was established to make recommendations regarding business rules, polices and procedures for implementation. The system will provide single (or reduced) sign-on using role based authentication and authorization

Actions include:

1) Establish an authentication standard to be submitted to the NITC to seek approval by the March 2005 meeting
   a) Propose standard to State Government Council
      - Lead Entity: IMServices
      - Timeframe: September 16, 2004 meeting
      - Funding: No funding required for this task
      - Status (March 2005): Completed.
   b) Propose standard to NITC Technical Panel
      - Lead Entity: IMServices
      - Timeframe: December 14, 2004 meeting
      - Funding: No funding required for this task
      - Status (March 2005): Completed.

2) Content Management offerings to customers
   a) Implement the Content Management structure for all agencies -
      - Lead Entity: IMServices
      - Timeframe: March 31, 2005
      - Funding: IMServices
      - Status (March 2005): Work underway.

3) Two-factor authentication
   a) Propose standard to NITC Directory Workgroup
      - Lead Entity: IMServices
      - Timeframe: September 30, 2004 meeting
      - Funding: No funding required for this task
      - Status (March 2005): Timeline to be revised.
   b) Propose standard to SGC
      - Lead Entity: IMServices
      - Timeframe: December 2004 meeting
      - Funding: No funding required for this task
      - Status (March 2005): Timeline to be revised.

4) Pilot single sign-on
   a) Provide Web-Based Single sign-on (WSSO) guideline to any client/application that desires it.
      - Lead Entity: IMServices
      - Timeframe: September 30, 2004
      - Funding: IMServices
      - Status (March 2005): Timeline to be revised.

C. Implement incident reporting requirements

Very few agencies are complying with the NITC's incident reporting requirements. Centralized reporting serves the goal of increasing awareness of vulnerabilities and threats to state government as a whole. In particular, centralized reporting is necessary to discern patterns, identify areas of vulnerability, allocate resources, and develop statewide solutions. Centralized reporting does not substitute for internal reporting to management, reporting to law enforcement, or mobilizing a computer security incident response team (CSiRT). Agencies should develop procedures for internal and external reporting that will meet the needs of centralized reporting with little or no additional work.

Actions include:

1. Review incident reporting procedures to determine need for changes in what is reported and the reporting requirements.
   a. Lead Entity: CIO
   b. Timeframe: December 31, 2004
   c. Funding: No funding required for this task
   d. Status (March 2005): Completed. DOC developing an incident reporting process.

2. Communicate reporting requirements to agencies.
   a. Lead Entity: CIO
   b. Timeframe: March 31, 2005
   c. Funding: No funding required for this task
   d. Status (March 2005): Pending completion of previous item.

D. Network Security and Network Management

DAS Division of Communications (DOC) has made changes to implement a layered approach to network security. DOC and many agencies have focused more attention on network management, including patch management, virus protection, and intrusion detection.

Actions include:

1. Configure all public state IP addresses (164.119) behind the state's firewall complex
   a. Lead Entity: DOC
   b. Timeframe: December 31, 2004
   c. Funding: DOC
   d. Status (March 2005): Completed.
2. Implement an intrusion detection and prevention system on the State's Internet connection as a part of a layered defense.
   a. Lead Entity: DOC
   b. Timeframe: March 31, 2005
   c. Funding: DOC
   d. Status (March 2005): On schedule.
3. Investigate and recommend an enterprise solution to ensure that encrypted traffic adheres to State security requirements.
   a. Lead Entity: DOC
   b. Timeframe: March 31, 2005
   c. Funding: Funding not needed.
   d. Status (March 2005): On schedule.
4. Evaluate and recommend options for providing encryption to clients across the state's Wide Area Network
   a. Lead Entity: DOC
   b. Timeframe: June 30, 2005
   c. Funding: Funding not needed.
   d. Status (March 2005): On schedule.

BUSINESS RESUMPTION

E. Promote disaster planning for information technology systems, in conjunction with agency business continuity plans

Disaster recovery plans for information technology must be linked to an overall agency business continuity plan. A strategy for security and business resumption must encourage completion of agency business continuity plans in order for disaster recovery plans for information technology to be effective. Because many agencies depend on DAS for networking and computing services, it is essential that DAS develop a disaster recovery plan for its facilities and services.

Actions include:

1. Conduct an "executive overview" briefing (orientation exercise) to state agencies (using either the State Government Council or the Security Work Group as a

forum) explaining the progress and current and future activities in the development of disaster recovery plans.

a. Lead Entity: DAS – IMServices, DAS Division of Communications, and CIO
b. Timeframe: December 31, 2004
c. Funding: No funding required for this task
d. Status (March 2005): Pending completion of DAS contract with vendor.

2. Encourage agencies to develop agency business continuity plans and disaster plans for information technology by seeking funding sources, providing training on developing plans, and providing technical assistance. The focus should be at the business level.
   a. Task: Identify funding sources
      (1) Lead Entity: CIO
      (2) Timeframe: November 30, 2004
      (3) Funding: No funding required for this task
      (4) Status (March 2005): Pending completion of action item 1 above.
   b. Task: Identify next set of agencies for developing business continuity plans
      (1) Lead Entity: DAS Risk Management
      (2) Timeframe: February 1, 2004
      (3) Funding: The cost of preparing business continuity plans by agency is itemized in the DAS contract. Sources of funding have not been identified.
      (4) Status (March 2005): Pending completion of action item 1 above.

3. Identify and develop procedures for common elements that should be addressed in all or most business continuity plans and disaster recovery plans for information technology.
   a. Task: Investigate and communicate the availability of insurance to cover costs relating to replacement, repair and recovery services
      (1) Lead Entity: DAS Risk Management (subject to approval by DAS)
      (2) Timeframe: May 31, 2004
      (3) Funding: No funding required for this task
      (4) Status (March 2005): Pending completion of action item 1 above.
   b. Task: Develop and communicate policy and procedures for expedited purchasing of goods and services related to a disaster
      (1) Lead Entity: DAS Materiel with DAS IMServices as a critical stakeholder (subject to approval by DAS)
      (2) Timeframe: March 31, 2005
      (3) Funding: No funding required for this task
      (4) Status (March 2005): Pending completion of action item 1 above.

F. Implement shared disaster recovery facilities

Mission critical systems have three common requirements. Recovery times must be measured in hours, not days or weeks. Recovery facilities should be physically separated so that they will not be affected by a single disaster. There must be staff available to assist with the recovery efforts. Achieving these requirements is very expensive. Sharing disaster recovery facilities, and establishing a collaborative approach to disaster recovery is one strategy for managing costs. DAS IMServices and the University of Nebraska are jointly developing a fast recovery capability using mutual assistance of physically separated data centers

Actions include:

1. Develop a shared recovery capacity serving state government and the University of Nebraska.
   a. Lead Entity: DAS IMServices and NU
   b. Timeframe: ongoing
   c. Funding: The cost and source of funding have not been determined.
   d. Status (March 2005): Initial hardware and communications capabilities in place. Additional implementation work ongoing.
2. Conduct a briefing for state agency information technology staff (orientation exercise) describing the disaster recovery activities that will be performed by IMServices and the disaster recovery testing that has been completed.
   a. Lead Entity: DAS IMServices
   b. Timeframe: March 31, 2005
   c. Funding: No funding required for this task.
   d. Status (March 2005): On time.

G. Encourage testing and updating of disaster plans

Testing is the only way to insure that a disaster recovery plan is adequate and the organization is able to implement its plan.

Actions include:

1. Evaluate current status of testing and recommend testing strategies for different kinds of systems
   a. Lead Entity: CIO
   b. Timeframe: June 30, 2005
   c. Funding: No funding required for this task.
   d. Status (March 2005): October 2004: DAS performed a “table-top” disaster recovery exercise; November 2004: NEMA sponsored a statewide table-top exercise; and April 2005: a NEMA sponsored DAS exercise is scheduled.