Date of Last Revision: March 7, 2005

Nebraska Information Technology Commission
Strategic Initiatives

Strategic Plan For
Network Nebraska

Objectives

The primary objective of this initiative is to develop a broadband, scalable telecommunications infrastructure that optimizes the quality of network services to every public entity in the State of Nebraska.

Benefits

Through aggregation of demand, adoption of common standards, and collaboration with network services and applications, participants can achieve many benefits, including:

- Lower network costs;
- Greater efficiency for participating entities;
- Interoperability of systems providing video courses and conferencing;
- Increased collaboration among all K-20 educational entities;
- New educational opportunities;
- Competitiveness with surrounding states; and
- Better use of public investments.

Current Status

The Division of Communications, the University of Nebraska, Nebraska Educational Telecommunications Commission, Department of Education, Public Service Commission, and the Nebraska Information Technology Commission have formed the Collaborative Aggregation Partnership (CAP) to guide and implement Network Nebraska. The Division of Communications and University of Nebraska have entered into a memorandum of agreement to formalize their participation in this joint effort.

Using existing resources and aggregating existing demand from state government and the University of Nebraska, CAP has developed a multipurpose core backbone extending from Norfolk, Omaha, Lincoln, Grand Island, Kearney, North Platte, and Alliance. A shared circuit also connects Scottsbluff to the backbone at Grand Island.

State and University circuits have been moved to the backbone to take advantage of the economies and efficiencies offered by aggregation. The K-20 community has started to migrate to this service as contracts have allowed. Project 42 (consisting of ESUs 10, 11,

15 and 16) has purchased services from Network Nebraska to serve the schools in their areas.

A contract has been signed for Internet 1 service that will allow Network Nebraska to begin to offer lower rates to network participants. This could significantly increase participation in Network Nebraska. Internet 2 service is also available to educational participants through the University of Nebraska.

Future

The major components of this initiative include:

1. Development of a scalable, reliable, and secure telecommunications infrastructure that enables any type of eligible entity (i.e. local and state government, public and private K-12 and higher education, health care institutions) to purchase the amount of service that the entities need, when they need it, on an annual basis;
2. Establishment of a catalog of value-added applications that enables eligible entities to pick and choose services that are pertinent to them (e.g. Internet1, Internet2, and videoconferencing);
3. Investigate possible implementation of a network operations center that offers a helpdesk, network diagnostics, and engineering assistance in order to ensure acceptable qualities of service;
4. Investigate establishment of a billing or accounting center to accept service orders, extend service agreements, provide consolidated billing, and to maintain customer accounts.

Recommended Actions

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

Action items for Network Nebraska for the remainder of FY 2005.

1) Develop and offer Internet I services to eligible network participants by January 10, 2005
   - University of Nebraska signs contract with provider for Internet I services no later than August 31, 2004.
   - Division of Communications purchases Internet I services from the University no later than September 15, 2004.
   - Collaborative Aggregation Partnership (CAP) agrees on rates to be charged to eligible network participants for Internet I services no later than September 15, 2004.
   - Working through the NITC and the various Councils, CAP will distribute information related to the new Internet I charges to eligible network participants during the months of October, November and December 2004.

- Orders will be taken by CAP for new service and the circuits will be provisioned during the months of October, November and December, 2004.
- Internet I service turned up the first working day of January, 2005 for initial orders.

a. Lead Entity: CAP, in cooperation with staff of UNCSN and DOC, and assisted by NITC Councils.
b. Timeframe: August, 2004 – January, 2005.
c. Funding: No additional funding required for this action item.
d. Status (March 2005): Network Nebraska Internet service has been extended to eligible participants at a unit price approximately 50% of the October 2003 unit price. In addition, a service provider was contracted to provide redundant service out of the Omaha area. As of March 2005, an estimated 250,000 persons are being served by Network Nebraska Internet and transport services within state government, higher education, and K-12. This includes all four campuses of the University of Nebraska, two state colleges, three of the six community colleges, and all or part of the schools represented by ESUs 10, 11, 15, 16, and 18.

2) Identify Tier II communities that offer opportunities for aggregation for services onto the network – ongoing.

- Both the University and the State will begin by providing a list to CAP of the communities where service is currently being provisioned that indicates the total amount of bandwidth currently being consumed no later than September 15, 2004.
- CAP will analyze the listings for opportunities to aggregate the existing service when coupled with other opportunities within the community no later than November 15, 2004.
- CAP will order service for the next Tier II community aggregation no later than January 15, 2005.
- New service will be provisioned by the provider and the move of existing service will be coordinated by CAP with the customer between January and March of 2005.
- Opportunities for the next Tier II community will be explored and started over again no later than May 15, 2005.

a. Lead Entity: CAP.
b. Timeframe: September, 2004 – May, 2005
c. Funding: No additional funding required for this action item.
d. Status (March 2005): Additional Tier II communities are still being considered. Wayne, Nebraska is aggregating Internet service from municipal and education entities through wireless service provided by Wayne State College. Tier II aggregation discussions have also occurred with Mid-Plains Community College in North Platte, UNK and ESU10 in Kearney, and the municipalities of Scottsbluff and Gering.

3) Create a Service Level Agreement for use by CAP and the eligible network participants no later than November 1, 2004.

- CAP will work with appropriate legal counsel to establish a Service Level Agreement that will detail the service that is being provided to the client.

These meetings will take place thru August and September with a final draft document due September 30, 2004.

- CAP will review the document with agency and university leadership, as well as the Chair of the NITC with final approval no later than October 15, 2004.
- CAP will make the final adjustments to the document and the document will be ready for distribution to eligible network participants by November 1, 2004.

a. Lead Entity: CAP, in cooperation with University of Nebraska and State of Nebraska legal staff.
b. Timeframe: September-November, 2004
c. Funding: Cost for legal services assumed by UNCSN and DOC.
d. Status (March 2005): The Service Level Agreement has been developed and distributed to eligible network participants and suggested changes are now being reviewed.

4) Create a Network Nebraska Level 1 Helpdesk no later than November 1, 2004.

- Members of CAP will estimate the numbers of calls that they are currently taking regarding information about Network Nebraska over the months of July and August 2004. That information will be collected by the CAP chair at the September 2004 meeting.
- A subcommittee of CAP consisting of the technical people will conduct a review of help desk software during the months of August and September. A recommendation will be brought to the CAP group at the October 2004 meeting.
- CAP has determined that the Level 1 Helpdesk will reside at NET. In order to transfer calls between the members of CAP, the NET telephone system will need an upgrade. This upgrade will be accomplished no later than October 31, 2004.
- A toll-free number will be installed for use by the Level 1 Helpdesk and eligible clients. The toll-free number will be ordered by September 15, 2004 and turned up for service no later than November 1, 2004.

a. Lead Entity: Nebraska Educational Telecommunications staff, in cooperation with CAP.
b. Timeframe: July-November, 2004
c. Funding: Cost for the toll-free number (888-NET-NEBR or 888-638-6327) service and cost for toll free calls minimal.
d. Status (March 2005): Call center is up and running staffed by NET.

5) Create a Network Nebraska Website no later than December 15, 2004.

- CAP will identify URL for website no later than August 15, 2004.
- The office of the NITC will identify initial information for the web site and present the information to CAP at the September 2004 CAP meeting.
- After approval from CAP, a “test” web site will be developed by and hosted at Nebraska On-Line no later than October 15, 2004.
- CAP members will test the web site and make suggestions to the NITC staff through November 30, 2004.
- Final changes will be made to the web site and the site will be unveiled to the users no later than December 15, 2004.

a. Lead Entity: University of Nebraska Computing Services Network staff, in cooperation with CAP and staff of the NITC.
b. Timeframe: August-December, 2004
c. Funding: No funding required for this action item.
d. Status (March 2005): Network Nebraska website, www.networknebraska.net is posted and fully functional. Additional documents and resources are being added and linked as needed.

6) Meet with the Technical Subcommittee of the Nebraska Statewide Telehealth Network to discuss issues related to network administration and management.
   a. Lead Entity: Technical Panel
   b. Timeframe: May 31, 2005
   c. Funding: No funding required for this task
   d. Status (March 2005): Ongoing.

Date of Last Revision: March 4, 2005

Nebraska Information Technology Commission
Strategic Initiatives

Strategic Plan for the
Statewide Synchronous Video Network

Objective

The objective of this initiative is to achieve a statewide synchronous video network capable of enhancing educational opportunities and citizen services through the exchange of interactive video between and among various sectors.

In order to accomplish this, a number of tasks must be completed.

- Identification of a single audio and video standard for low-bandwidth distance learning and videoconferencing;
- Acquisition of upgrade or replacement equipment and/or software that ensures compliance with the audio and video standard;
- Development or purchase of a scheduling system or enterprise resource management program that allows potential users to A) know the location and availability of resources, and B) set up or reserve ad hoc or regularly scheduled events with other entities;
- Development of a network bandwidth management system or network operations center that assures pre-determined qualities of service, depending upon the type of video traffic;
- Development of an event clearinghouse that allows promotion, marketing, and registration for interactive video events;
- Development of training modules for new users;
- Development of a cost and funding algorithm to allow shared use of the statewide backbone for interstate distance education and videoconferencing.

Benefits

Since 1992, various entities within the State of Nebraska have spent an estimated 20 million dollars on interactive video capture and display equipment, fiber connectivity, and engineering design charges to provide for distance learning and videoconferencing. Considered cutting edge technology in the early years of operation, this investment resulted in over 300 high-quality, videoconferencing classrooms using multiple, incompatible video protocols spread over numerous separate political subdivisions. These service regions were established when groups partnered together to set up

interlocal agreements in order to receive grant funds, enter into contracts and hire staff to exchange high school and college classes. Other smaller videoconferencing networks were set up by other state agencies and hospitals but were not interoperable with the school and college sites.

In order for Nebraska to maximize the potential of its investment in interactive videoconferencing and to create unprecedented educational opportunities, all videoconferencing sites in this State must be in compliance with the State video compression standard and stakeholders must agree to work collaboratively to enhance the benefit for all end users.

Current Status

Currently, Nebraska enjoys one of the most robust distributions of local connectivity and bandwidth among any of its rural neighbors. This equates to 192 DS-3 (45 megabit per second, JPEG and MPEG2 video) circuits to high schools served by telephone companies and 112 high school sites that are served by cable companies with 100 megabit per second, full duplex, fiber circuits with H.263 video. Only about 10 high schools are left in rural areas of the State without high bandwidth connections, many at their own choosing. Other state agency and telehealth videoconferencing circuits consist of single or double dedicated T-1 (1.55 megabit per second) lines.

Nebraska high school distance learning classrooms are some of the busiest in the nation; with each classroom being used about 50% of the school day across the entire system. Taking high school credit courses and higher education dual credit and college credit courses at a distance, students are able to fulfill graduation requirements and expand their high school experiences with opportunities that are unavailable at their local high school. Some high schools permit community and adult education classes in the evening hours.

Distance learning consortia (interlocal agreements between neighboring districts) often are able to share the talents of one qualified instructor across several schools and sections of students each semester.

Unfortunately, due to the high costs of transporting high bandwidth (JPEG) video signals, distance learning consortia have been unable to afford course exchange with consortia in other parts of the State, thus limiting their credit course offerings and educational opportunities.

The original 10-year contracts between the distance learning consortia and the telephone company providers for JPEG video service will begin expiring in the Spring of 2006. With no chance of contract extensions for JPEG video service, the schools will need to upgrade to an H.323 Internet Protocol communication standard, new codecs (Coder-Decoders) to accommodate the H.263/H.264 video standards, and switch/router technology at the school site to manage the resulting data network. The later of the JPEG consortium contracts are not due to expire until 2009 but the industry has chosen to no longer manufacture nor repair JPEG video equipment, thus prompting an early conversion of these contracts to IP video.

Whereas Nebraska's (telco provided) interactive video efforts have been mostly localized with high bandwidth video, most other States have converted or are converting to IP video and have been trying to realize further educational programming through ad hoc enrichment activities and use of Internet2.

The current network will not be able to meet the future distance learning applications and the bandwidth needs for the Internet and Internet2. Therefore it is necessary to convert to the next generation distance learning (data) network.

Future

Nebraska has enormous potential to assemble one of the country's best telecommunications networks for education, health care, and government. The Nebraska Information Technology Commission and its advisory groups have fostered a collaborative environment for participative decision making among several major subsectors. The Collaborative Aggregation Partnership, a team of University of Nebraska, Division of Communications, and Nebraska Educational Telecommunications staff have been successful in negotiating statewide backbone contracts for scalable bandwidth for public entities. Technological developments and breakthroughs in routing technology in the past two years have greatly enhanced the quality of service related to IP-based, H.26X video compression.

The new Statewide Synchronous Video Network design incorporates the requirements established by the Statewide Synchronous Video Network Work Group of the Nebraska Information Technology Commission. This network design has the flexibility to support both proprietary and standard protocols, and allows the school full access to the available bandwidth. The network can grow to meet any bandwidth or application requirements, and has any optical interface available from Ethernet to OC192.

This network design is consistent with the goals of the Nebraska Information Technology Commission and will integrate into Network Nebraska. Most importantly for those who qualify, this network is eligible for E-rate discounts. All consortiums and member schools benefit because this is a plan toward statewide services and interconnectivity. Not only is video bandwidth available, but also data applications such as the Internet and Internet2. Asynchronous distance learning applications such as Blackboard, WebCT or Angel become a reality with the bandwidth that will be made available, and multiple classrooms become much more affordable.

The contracts for the current distance learning networks begin to expire in the next two years. This network is leading edge technology, is of carrier grade quality, and is scalable to meet any growth demands.

The vision of the future statewide synchronous video network includes the umbrella capacity for any interactive video unit to be able to interconnect with any other interactive video unit, regardless of location. The vision of the future also includes assurances for network security and quality of service within a particular sub-network (i.e. telehealth, State Patrol, K-12 distance learning). Most end users are in agreement that the State should purchase or contract for a single software scheduling system that can remotely

turn on a specific video unit, log system usage statistics, allow promotion of ad hoc education events, and secure permission for usage from local site coordinators.

Recommended Actions

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

A. Identification of a single audio and video standard for low-bandwidth distance learning and videoconferencing.

Actions include:

1. Approval of the H.263/H.264 video compression protocol and G.722, G.722.1, and G.728 audio compression protocols by the Nebraska Information Technology Commission.
   a. Lead Entity: NITC Technical Panel
   b. Timeframe: September 9, 2004
   c. Funding: No funding required for this task
   d. Status (March 2005): Completed.

B. Acquisition of upgrade or replacement equipment and/or software that ensures compliance with the audio and video standard.

Actions include:

1. Development and submission of a Congressional funding request to fund upgrade of classroom and networking resources necessary to bring K-12 and higher education distance learning facilities into compliance.
   a. Lead Entity: NITC Technical Panel's Statewide Synchronous Video Work Group
   b. Timeframe: September 3, 2004
   c. Funding: Actual request estimated at $13 million; no funding required to develop the request.
   d. Status (March 2005): Congressional request of $9.8 million was submitted on September 8, 2004. The funding request was declined.

2. Designation of a fiscal entity to oversee bidding, ordering, delivery and installation of equipment.
   a. Lead Entity: To be named.
   b. Timeframe: March 2005
   c. Funding: No funding required for this task.
   d. Status (March 2005): The white paper, "Converting distance learning networks to a high bandwidth, flexible infrastructure" provides several options for bidding and procurement of equipment and services. The Distance Education Enhancement Task Force, if created as described in LB 689, would provide recommendations for this action item by December 31, 2005.

3. Equipment RFP, bidding, ordering, delivery and installation of equipment
   a. Lead Entity: To be named
   b. Timeframe: August 2005 - July 2006
   c. Funding: Funding to oversee this task included in Congressional request.
   d. Status (March 2005): The Distance Education Enhancement Task Force, if created as described in LB 689, would provide recommendations for this action item by December 31, 2005.

C. Development or purchase of a scheduling system or enterprise resource management program that allows potential users to know the location and availability of resources, and/or set up or reserve ad hoc or regularly scheduled events with other entities.

Actions include:

1. Research scheduling systems and enterprise resource management programs.
   a. Lead Agency: NITC Technical Panel's Statewide Synchronous Video Work Group
   b. Timeframe: September 2004-December 2004
   c. Funding: No funding required for this task.
   d. Status (March 2005): Research continues on this action item.

2. Purchase or develop a scheduling system and/or enterprise resource management program.
   a. Lead Entity: To be named.
   b. Timeframe: Summer, 2005
   c. Funding: To be determined.
   d. Status (March 2005): The Distance Education Enhancement Task Force, if created as described in LB 689, would provide recommendations for this action item by December 31, 2005. Timeframe likely to be delayed until summer, 2006 at the earliest.

D. Explore options for a network bandwidth management system or network operations center that assures pre-determined qualities of service, depending upon the type of video traffic.

Actions include:

1. Explore options for a network operations center that assures particular qualities of service.
   a. Lead Entity: Network Nebraska (Collaborative Aggregation Partnership)
   b. Timeframe: Ongoing
   c. Funding: Funding to complete this task to be determined.
   d. Status (March 2005): The Distance Education Enhancement Task Force, if created as described in LB 689, would provide recommendations for this action item by December 31, 2005.

E. Development of an event clearinghouse that allows promotion, marketing, and registration for interactive video events.

Actions include:

1. Development of a web-based clearinghouse that allows originators to post events and users to register for or view the date, time and frequency of individual events.
   a. Lead Entity: Statewide Synchronous Video Work Group
   b. Timeframe: Fall, 2006
   c. Funding: To be determined.
   d. Status (March 2005): The Distance Education Enhancement Task Force, if created as described in LB 689, would provide recommendations for this action item by December 31, 2005.

F. Development of training modules for new users.

Actions include:

1. Development of training modules to accompany equipment orientation.
   a. Lead Entity: NITC Technical Panel's Statewide Synchronous Video Work Group, in cooperation with commercial equipment manufacturer.
   b. Timeframe: June-August, 2006 (Corresponding with equipment deployment)
   c. Funding: To be determined.
   d. Status (March 2005): The Distance Education Enhancement Task Force, if created as described in LB 689, would provide recommendations for this action item by December 31, 2005.

G. Development of a cost and funding algorithm to allow shared use of the statewide backbone for interstate distance learning and videoconferencing.

Actions include:

1. Research models from other States' education networks.
   a. Lead Entity: NITC Technical Panel's Statewide Synchronous Video Work Group, in conjunction with Network Nebraska (Collaborative Aggregation Partnership)
   b. Timeframe: Ongoing
   c. Funding: No funding required for this task.
   d. Status (March 2005): The Distance Education Enhancement Task Force, if created as described in LB 689, would provide recommendations for this action item by December 31, 2005.

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.