Technical Panel
of the
Nebraska Information Technology Commission

Monday, April 17, 2006 - 9:00 a.m.
Varner Hall - Board Room
3835 Holdrege St., Lincoln, Nebraska

AGENDA

Meeting Documents:
Click the links in the agenda
or click here for all documents (xxx KB, xx Pages)

1. Roll Call and Meeting Notice

2. Public Comment

3. Approval of Minutes - March 14, 2006*

4. Standards and Guidelines*

- Recommendations to the NITC
  - Network Edge Device Standard for Entities Choosing to Connect to Network Nebraska | Comments Received (1)
  - Scheduling Standard for Synchronous Distance Learning and Videoconferencing | Comments Received (None)

- Set for 30-Day Comment Period
  - Web Cookie Policy
  - Wireless Local Area Network Standard
    Related documents:
    - Wireless Access Point Approval Process
    - Wireless LAN Security Checklist
  - Disaster Recovery Planning Procedures

5. Agency Information Technology Plan Form*

- Old: 2004 Agency IT Plan Form
- New: 2006 Agency IT Plan Form

6. New NITC Website (under construction)

7. Regular Informational Items and Work Group Updates (as needed)

- Accessibility of Information Technology Work Group
- CAP
- Security Work Group
- Statewide Synchronous Video Network Work Group

8. Other Business

9. Next Meeting Date

Tuesday, May 9, 2006

10. Adjourn

* Denotes Action Item

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

NITC and Technical Panel Websites: http://www.nitc.state.ne.us/
Meeting notice posted to the NITC Website: 16 MAR 2006
Meeting notice posted to the Nebraska Public Meeting Calendar: 16 MAR 2006
Agenda posted to the NITC Website: 14 APR 2006

TECHNICAL PANEL

Nebraska Information Technology Commission

Tuesday, March 14, 2006 - 9:00 a.m.
Varner Hall - Board Room
3835 Holdrege St., Lincoln, Nebraska

PROPOSED MINUTES

MEMBERS PRESENT:

Mike Beach, Nebraska Educational Telecommunications Commission
Brenda Decker, Chief Information Officer, State of Nebraska
Steve Henderson, Department of Administrative Services, State of Nebraska
Kirk Langer, Lincoln Public Schools
Walter Weir, University of Nebraska

MEMBERS ABSENT: Christy Horn, University of Nebraska, Compliance Officer

CALL TO ORDER, ROLL CALL, NOTICE OF PUBLIC MEETING

Mr. Weir called the meeting to order at 9:13 a.m. A quorum was present at the time of roll call. The meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on February 24, 2006. The meeting agenda was posted to the NITC Website on March 13, 2006.

PUBLIC COMMENT

There was no public comment.

APPROVAL OF MINUTES

Ms. Decker moved to approve the February 14, 2006 minutes as presented. Mr. Henderson seconded. Roll call vote: Beach-Yes, Decker-Yes, Henderson-Yes, and Weir-Yes. Results: Yes-4, No-O. Motion carried.

STANDARDS AND GUIDELINES - NETWORKING EQUIPMENT / EDGE DEVICES

This standard is addressed in LB 1208. When the time comes to develop the RFP, the specifications can be more detailed. Generic language in the standard would accommodate future upgrades and technology changes.

Mr. Langer arrived.

The ESU-NOC has reviewed the document. Discussion followed regarding the use of switches versus routers, the issue of security and bandwidth capacity.

It was recommended to strike the "with high bandwidth networking (≥ 10Mbps)" reference wherever indicated in the document.

Mr. Beach moved to approve the draft Networking Equipment/Edge Devices with the recommended revisions for the 30-day public comment period. Mr. Henderson seconded the motion. Roll call vote: Weir-Yes, Langer-Yes, Henderson-Yes, Decker-Yes, and Beach-Yes. Results: Yes-5, No-O. Motion carried.

STANDARDS AND GUIDELINES - SCHEDULING SOFTWARE

Mr. Beach stated that the wording and references were rearranged so that entities could cut and paste information into specification documents for bidding. Recommended changes included:

- Include a list of acronyms

- Clarify who is responsible for exemption process
- 1.1.1.10 change Maintenance fees to "Annual maintenance fees"

Mr. Langer moved to approve the draft Scheduling Software standard with the recommended revisions for the 30-day public comment period. Ms. Decker seconded. Roll call vote: Decker-Yes, Henderson-Yes, Langer-Yes, Weir-Yes, and Beach-Yes. Results: Yes-5, No-O. Motion carried.

AGENCY IT PLAN FORM: UPDATE ON STATE GOVERNMENT COUNCIL RECOMMENDATIONS

Members were asked to review the document. Mr. Becker stated that the State Government Council opinion is that Section 4 Future Goals should be the emphasis of the document and that here is a work group developing recommendations for Technical Panel April meeting.

REGULAR INFORMATIONAL ITEMS AND WORK GROUP UPDATES (AS NEEDED)

Accessibility of Information Technology Work Group. Christy Horn was not present to provide a report.

CAP, Brenda Decker. The group is meeting today to discuss edge device standard developed by a CAP work group, recommendations for two Tier II communities, and a name change for the group.

Security Work Group, Steve Hartman. Mr. Hartman was not available to report. Mr. Henderson reported that the group has been developing a wireless access standard. The group is also organizing a Security Conference on May 24th. The work group will also be developing a standard/guideline regarding remote access. They will make a recommendation to Technical Panel.

Statewide Synchronous Video Network Work Group, Mike Beach. The work group focus has been the development of the scheduling standard and will regroup if LB 1208 is enacted.

OTHER BUSINESS

Pandemic issue affects the work force, revenue, educational opportunities, etc. In the near future, Mr. Weir would like the Technical Panel discuss this topic.

Mr. Weir announced the NU Tech Day event to be held on March 15th at UNL's Kaufmann Building (http://nuitday.nebraska.edu/). If successful, the University may take it out state to different locations.

NEXT MEETING DATE/TIME AND ADJOURNMENT

In order to accommodate the 30-day public comment period for the proposed standards, the panel will need to change the next meeting date. The next meeting of the NITC Technical Panel will be held on Monday, April 17, 2006, 9:00 a.m. at Varner Hall, 3835 Holdrege Street in Lincoln, Nebraska.

With no further business to conduct, Ms. Decker moved to adjourn. Mr. Henderson seconded. All were in favor. Motion carried.

Meeting was adjourned at 10:25 a.m.

Technical Panel
of the
Nebraska Information Technology Commission

Draft Document
30-Day Comment Period

Title: Network Edge Device Standard for Entities Choosing to Connect to Network Nebraska

Notes to Readers:

1. The following document is a draft standard under review by the Technical Panel of the Nebraska Information Technology Commission (NITC). This document is available in both PDF and Word versions at http://www.nitc.state.ne.us/standards/index.html.
2. If you have comments on this document, you can send them by e-mail to rick.becker@nitc.ne.gov, or call 402-471-7984 for more information on submitting comments.
3. The comment period for this document ends on April 14, 2006.
4. The Technical Panel will consider this standard and the comments received at their meeting currently scheduled for April 17, 2006. Final approval of the standard would be considered by NITC at their meeting currently scheduled for May 1, 2006. Information about these meetings will be posted on the NITC web site at http://www.nitc.state.ne.us/.
5. Special Note: This document is related to a legislative bill, LB 1208, currently under consideration by the Nebraska Legislature. Depending on the outcome of that legislation this document may be modified. The standards setting process usually takes several months from conceptualization to final approval by the NITC. In anticipation of the potential implementation timeline of LB 1208, the NITC Technical Panel had to begin formulating the standards that were called for in the legislation (i.e. scheduling system software standards, distance learning equipment, network edge devices) in February 2006 so as to not impede the entities affected by the bill.

Nebraska Information
Technology Commission

STANDARDS AND GUIDELINES

Network Edge Device Standard for Entities Choosing to Connect to Network Nebraska

Category	**Network Architecture**
Title	**Network Edge Device Standard for Entities Choosing to Connect to Network Nebraska**
Number	

Applicability

☐ **State Government Agencies**
- ☐ All ..... **Not Applicable**
- ☐ Excluding _____ ..... **Not Applicable**

☑ **State Funded Entities -** All entities receiving LB 1208 funding for matters covered by this document ..... **Standard**

☑ **Other:** Educational entities electing to connect to *Network Nebraska* ..... **Standard**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval (see Section 4.3).
Guideline - Adherence is voluntary.

Status	☐ Adopted	☑ Draft	☐ Other:_____
Dates	Date: March 14, 2006 Date Adopted by NITC: Other:		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Technical Standard

All education entities that receive state funding for telecommunications, and education entities that wish to connect to Network Nebraska for purposes of transmitting data across the state shall comply with this standard. State agencies reach compliance through their services by the Division of Information Technology Services and are not directly affected by this standard.

1.1 Network Edge Device Specifications for new purchases

- QoS capabilities
- Sufficient ports for desired network design
- Security and/or firewall features
- Routing and/or routing protocol
- Traffic shaping and rate limiting
- VLAN (802.1q) support
- Secure remote management (SSH)
- Hardware based encryption acceleration
- Performance to meet anticipated usage demand
- Compatibility with central site router features
- Network Nebraska support team familiarity with equivalent devices

Option A:
Layer 3 Router (for basic site deployment)

Option B:
Enhanced Layer 3 Router (for larger site deployment or higher performance)

Option C:
Layer 3 Switch

1.2 Network Edge Device Specifications for existing equipment

- QoS capabilities
- Sufficient ports for desired network design
- Security and/or firewall features
- Routing and/or routing protocol
- Traffic shaping and rate limiting
- VLAN (802.1q) support
- Secure remote management (SSH)
- Hardware based encryption acceleration
- Performance to meet anticipated usage demand
- Compatibility with central site router features
- Network Nebraska support team familiarity with equivalent devices

2.0 Purpose and Objectives

The purpose of this standard is to set minimum standards and specifications for network edge devices that would perform the routing and switching functions of voice, video, and data across the network and assure that packets would get to their correct destination while maintaining the appropriate quality of service (QoS).

2.1 Background

Nebraska currently has about 200 local schools and campuses that use managed high-bandwidth interactive video and Internet services over 45 Mbps DS-3 circuits. As these contracts reach the end of their terms, it makes sense to retrofit the existing fiber so that it can be used to carry a variety of data applications using flexibly provisioned bandwidth. In order to accomplish this upgrade, more intelligent edge devices must be deployed at the school and campus level to be able to ensure an acceptable quality of service, packet prioritization, better security and firewall features, and remote management. The Technical Panel of the NITC, in cooperation with the operational staff of Network Nebraska, are naming these edge device standards for educational entities seeking to connect to Network Nebraska in order to comply with the provisions of LB 1208 (2006).

Approximately 100 other high schools have 100 Mbps or greater local connections that may opt to connect to Network Nebraska for reasons of statewide data exchange. This standard contains new equipment and existing equipment standards that would also apply to their edge device installation.

2.2 Objective

The objective of this standard is to prescribe the acceptable routing and switching device attributes that can be deployed at the local sites of Network Nebraska in order to achieve a multipurpose, converged network, capable of traffic prioritization and shaping, that performs reliably and ensures an expected quality of service.

The Specifications for purchase of new equipment affects those entities that will be upgrading existing fiber circuits and connecting to Network Nebraska in the 2007-2009 time frame.

The Specifications for existing equipment affects those entities that may have already upgraded to IP networking over high bandwidth circuits, have recently purchased or upgraded their edge equipment, and are connecting to Network Nebraska in the 2007-2009 time frame.

3.0 Definitions

3.1 IP

Internet Protocol. Packet-based protocol for delivering data across networks.

3.2 Mbps

Megabits per second. A unit of measure of data of 1,000,000 bits per second.

3.3 Network Nebraska
Network Nebraska is the term used to describe the statewide multipurpose telecommunications backbone and all of its associated service offerings and support. Network Nebraska is made possible through a consortium of public entities working together to provide a scalable, reliable and affordable infrastructure capable of carrying a spectrum of services and applications.

3.4 QoS
Quality of Service. The ability to define a level of performance in a data communications system.

3.5 router
A device or setup that finds the best route between any two networks using IP addressing, even if there are several networks to traverse. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create wide area networks.

3.6 SSH
Secure Shell (SSH client) is a program for logging into a remote machine and for executing commands on a remote machine. It is intended to replace rlogin and rsh, and provide secure encrypted communications between two untrusted hosts over an insecure network.

3.7 switch
A mechanical or solid state device that opens and closes circuits, changes operating parameters or selects paths for circuits on a space or time division basis.

3.8 VLAN
Virtual Local Area Network. Virtual LANs (VLANs) can be viewed as a group of devices on different physical LAN segments which can communicate with each other as if they were all on the same physical LAN segment.

4.0 Applicability

4.1 State Funded Education Entities
Education entities that are not State agencies but receive State funding for telecommunications (i.e. Legislative appropriations, Education Innovation Fund, Nebraska Universal Service Fund, ESU Core Services, Infrastructure Fund, etc.) are required to comply with this standard, if connecting to Network Nebraska.

4.2 Other Entities
Entities that are neither State agencies nor state-funded entities but choose to use the State-funded *Network Nebraska* for purposes of transmitting data or receiving Internet service must comply with this standard, if connecting to Network Nebraska.

4.3 Exemption

Exemptions may be granted by the NITC Technical Panel upon request by an agency or education entity.

4.3.1 Exemption Process

Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion; federal government requirements; or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 521 S. 14th Street, Suite 301, Lincoln, NE 68508). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the NITC Technical Panel may be appealed to the NITC.

5.0 Responsibility

5.1 NITC

The NITC shall be responsible for adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. (N.R.S. 86-516 §6)

5.2 *Network Nebraska* Operational entities

The Collaborative Aggregation Partnership, composed of the University of Nebraska Computer Services Network, the Department of Administrative Services--Division of Communications, and Nebraska Educational Telecommunications, will be responsible for sharing the responsibilities of the network operations portion of *Network Nebraska*. The responsibility for identification and mitigation of non-compliant entities with respect to the Network Edge Device Standard resides with the Collaborative Aggregation Partnership.

Network Edge Device Standard for Entities Choosing to Connect to Network Nebraska

Comment 1

From: Michael Farrell [mike.farrell@nortel.com]
Sent: Monday, April 10, 2006 3:43 PM
To: rick.becker@nitc.ne.gov
Cc: Tom Rolfes
Subject: Network Edge Device Standard --Comments

Rick:

Per the e-mail from Tom Rolfes, attached is general feedback regarding your "Network Edge Device Standard":

Section 1.1, p.2
1) Nortel complies with all these requirements for options A, B, C.

2) Concern/feedback regarding the last bullet -- "Network Nebraska support team familiarity with equivalent devices"
-This can represent a "catch all" whereby Network Nebraska doesn't give all vendors an equal opportunity to prove "familiarity with equivalent devices".

-An example, on a recent State of Nebraska Proposal/Bid 1138 OF - Extreme Network Equipment, Nortel submitted an "equivalent bid" that was 1/2 the cost of the chosen bid ($2.547m vs. $1.205m) and we were not given an opportunity to explain why our solution was equivalent, nor were we provided any feedback at all in regards to our proposal/bid. Discounting my objectivity, as a vendor calling on the State of NE and a NE taxpayer, a discrepancy of $1m+ seems like reason to further explore the "equivalency" of alternate bid.

Section 2.2, p2
1) Nortel complies with all these requirements.

2) Concern/feedback regarding the last bullet -- "Network Nebraska support team familiarity with equivalent devices"
-This can represent a "catch all" whereby Network Nebraska doesn't give all vendors an equal opportunity to prove "familiarity with equivalent devices".

We appreciate the opportunity to provide feedback and look forward to the opportunity to work with the NITC as LB 1208 continues to take shape.

Sincerely,

Mike Farrell
Account Manager
Nortel
[13815 FNB Parkway, Suite 101, Omaha, Nebraska 68154. USA]
[**Office** : (402) 964-4318] [**ESN** : 245-4318] [**Mobile** : (402) 880-6190]
[**Fax** : (402) 964-4319] [**Email** : mike.farrell@nortel.com]

Technical Panel
of the
Nebraska Information Technology Commission

Draft Document
30-Day Comment Period

Title: Scheduling Standard for Synchronous Distance Learning and Videoconferencing

Notes to Readers:

1. The following document is a draft standard under review by the Technical Panel of the Nebraska Information Technology Commission (NITC). This document is available in both PDF and Word versions at http://www.nitc.state.ne.us/standards/index.html.
2. If you have comments on this document, you can send them by e-mail to rick.becker@nitc.ne.gov, or call 402-471-7984 for more information on submitting comments.
3. The comment period for this document ends on April 14, 2006.
4. The Technical Panel will consider this standard and the comments received at their meeting currently scheduled for April 17, 2006. Final approval of the standard would be considered by NITC at their meeting currently scheduled for May 1, 2006. Information about these meetings will be posted on the NITC web site at http://www.nitc.state.ne.us/.
5. Special Note: This document is related to a legislative bill, LB 1208, currently under consideration by the Nebraska Legislature. Depending on the outcome of that legislation this document may be modified. The standards setting process usually takes several months from conceptualization to final approval by the NITC. In anticipation of the potential implementation timeline of LB 1208, the NITC Technical Panel had to begin formulating the standards that were called for in the legislation (i.e. scheduling system software standards, distance learning equipment, network edge devices) in February 2006 so as to not impede the entities affected by the bill.

Nebraska Information
Technology Commission

STANDARDS AND GUIDELINES

Scheduling Standard for Synchronous Distance Learning and Videoconferencing

Category	**Video Architecture**
Title	**Scheduling Standard for Synchronous Distance Learning and Videoconferencing**
Number	

Applicability

☑ **State Government Agencies**
- ☑ All..... **Standard**
- ☐ Excluding _____.....**Not Applicable**

☑ **State Funded Entities -** All entities receiving state funding for matters covered by this document..... **Standard**

☑ **Other:** Entities using state-owned or state-leased communication networks for synchronous video……..**Standard**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval (see Section 3.1).
Guideline - Adherence is voluntary.

Status	☐ Adopted	☑ Draft	☐ Other:_____
Dates	Date: March 14, 2006 Date Adopted by NITC: Other:		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard

This document consists of a list of features that ought to be available in any system that is developed for use in scheduling of synchronous events using videoconferencing technology.

In the event that LB1208 becomes law, this document is to be considered a standard. In the event that LB1208 does not become law, this document is to be considered a guideline.

It is the intent that any and all such scheduling systems defined by the specifications below be accessible either through the Internet or within a defined intranet as decided upon by the system administrators.

The following sections attempt to describe the various levels and types of scheduling or coordination that might be considered.

1.1 Hardware control component

When attempting to link two or more sites electronically, some system must coordinate the connectivity between/among the sites. This includes controlling the network and endpoint hardware and bandwidth necessary to cause a successful connection.

1.1.1 Standards for hardware control system

A system should be able to control all hardware in a network and be capable of linking into all the other systems listed in this standard to enable the following:

1.1.1.1 Browser-based access
1.1.1.2 Locate devices by IP address (both static and DHCP)
1.1.1.3 Locate devices by MAC address
1.1.1.4 Facilitate far-end control in endpoint devices with the capability
1.1.1.5 Display a call list that is understood by non-techs using plain English site description
1.1.1.6 Have a defined quality of service
1.1.1.7 Hardware and software systems must work such that the scheduling system is available for use at least 99.9% of the time
1.1.1.8 The system should not require reset/reboot more often than once per week
1.1.1.9 Have a minimum of a one-year warranty
1.1.1.10 Annual maintenance fees after the warranty has run out should not exceed 10% of original purchase price
1.1.1.11 Keep automated log data that may be defined by and searched in ways to be defined by the system administrator(s) with multiple possible search definitions
1.1.1.12 Maintain security in ways that can be defined by system administrators including:

1.1.1.12.1 Keeping log information secure
1.1.1.12.2 Limiting access to an event
1.1.1.12.3 Turning encryption on/off in endpoint devices with the capability
1.1.1.12.4 Identifying security capability to system administrators and event coordinators by site
1.1.1.12.5 Provide an identity management system that allows for multiple levels of user access as defined by system administrators

1.1.1.13 Facilitate ad hoc events by users with permission from system administrators

1.1.1.14 Facilitate scheduled events by users with permission from system administrators

1.1.1.15 Be capable of controlling all specific equipment used in the network (CODECs, routers, switchers, MCUs, firewall systems, etc.)

1.1.1.16 Facilitate various types of events
1.1.1.16.1 Broadcast to all
1.1.1.16.2 Broadcast to some
1.1.1.16.3 2-way point-to-point
1.1.1.16.4 2-way multipoint
1.1.1.16.5 A combination of broadcast and 2-way

1.2 Event logging component

If a system coordinator has a requirement to track information about events some mechanism would have to be in place. This may include knowing the number of people at a site, the minutes an event runs at any given site, or the number of events a specific organization schedules.

1.2.1 Standards for event logging system

A system should be able to automatically store data and permit reports and be capable of linking into the all the other systems listed in this standard to include the following:

1.2.1.1 Browser-based access

1.2.1.2 Store data in an ODBC compliant relational database

1.2.1.3 Provide fields for logging various pieces of information
1.2.1.3.1 minutes a site is available/not available
1.2.1.3.2 minutes a site is used
1.2.1.3.3 number of event attendees
1.2.1.3.4 type of event as defined by system administrators
1.2.1.3.5 number of sites per event

1.2.1.4 Permit system administrator defined fields (no fewer than 64)

1.2.1.4.1 Definable by site, groups of sites, and groups of groups

1.2.1.5 Related GUI entry for call setup as defined by system administrators

1.2.1.5.1 Physical site location

1.2.1.5.2 Local contact and facility arrangement info

1.2.1.5.2.1 Costs, availability, site rules

1.2.1.5.2.2 ADA options available

1.2.1.5.3 Searchable criteria for describing or accessing spaces

1.2.1.5.4 Must have a GUI that is understandable in plain English

1.2.1.6 Facilitate search to know what facilities are in conflict or are often in conflict

1.2.1.6.1 number of conflicts for a given site over a specific amount of time

1.2.1.7 Accommodate a facility “wait” list / availability queue

1.2.1.7.1 If a facility is already confirmed for an event, it should log who has requested the same facility then auto notify the requester(s) if the event causing the conflict is cancelled

1.2.1.8 Account for billing charges per event/location and total bill generation after the event

1. 3 Facilities coordination component

If an event will include locations for which more than one person/organization has responsibility, then some mechanism must exist for coordinating use of facilities. There may be technical or administrative limits as to the number or types of sites that can participate in any given event. This could be as simple as users coordinating times over the telephone or through e-mail, but for some applications there may be a greater need for pre-scheduling and coordination among multiple administrators.

1.3.1 Standards for facilities coordination system

A system should enable access to facilities based on defined permissions, resolve conflicts based on pre-determined policies and be capable of linking into all the other systems listed in this standard to include the following:

1.3.1.1 Browser-based access

1.3.1.2 System editable user access

1.3.1.2.1 Activate a facility such that it is known to the system and to system users

1.3.1.2.2 Building level admin such that the facilities at a specific location can set policies for that site and permit use by others
1.3.1.2.3 Regional admin (organization / geo-political) such that a group of facilities can set policies for all related sites and permit use by others
1.3.1.2.4 Sys admin (configuration) such that technical system setup, operation and maintenance may be conducted
1.3.1.2.5 Sector admin such that groups of groups of facilities can set policies for all related sites and permit use by others
1.3.1.2.6 Room request such that any designated site user or administrator may request access to a facility they do not already have rights to schedule
1.3.1.2.7 Participant access defaults
1.3.1.2.7.1 All denied unless specifically permitted
1.3.1.2.7.2 All permitted unless specifically denied
1.3.1.2.8 User account directory service with definable permissions for each account

1.3.1.3 Types of coordination
1.3.1.3.1 Event posting to inform others of possible access
1.3.1.3.2 Site joining to allow other to access
1.3.1.3.3 Ad hoc to allow immediate activation of unscheduled events
1.3.1.3.4 Pre-planned events that may occur once or cyclically
1.3.1.3.5 Inter network coordination to permit interaction of sites both within and outside a controlled network
1.3.1.3.6 Intra network coordination to permit interaction of sites within a controlled network
1.3.1.3.7 Administrator defined bandwidth prioritization to minimize network bottlenecks
1.3.1.3.8 Administrator defined asset prioritization to minimize system conflicts
1.3.1.3.9 Site-requested bandwidth speed

1.3.1.4 Facilities information to be posted
1.3.1.4.1 Identify technology available by site
1.3.1.4.2 Physical site location
1.3.1.4.3 Local contact and facility arrangement info
1.3.1.4.3.1 Costs, availability, site rules
1.3.1.4.3.2 ADA options available

1.3.1.5 Event information to be posted
1.3.1.5.1 Definable credit type
1.3.1.5.2 Definable student type
1.3.1.5.3 Event/course prerequisites

1.3.1.5.4 Event/course descriptions
1.3.1.5.5 Teacher / event leader / presenter
1.3.1.5.6 Materials needed
1.3.1.5.7 Event coordinator info
1.3.1.5.8 Target audience
1.3.1.5.9 Mapquest-like link

1.4 People coordination component

If a specific location is to be used this implies that operational people may need to be dedicated to cause successful events. Since there will be a variety of site designs and operations, then there will be a variety of the demand of staff time. Likewise each facility will have limits on how many people can attend at any one location. Finally, there may be limitations as to the total number of event participants allowed.

1.4.1 Standards for people coordination system

A system should enable interaction of people based on policies set by system administrators and be capable of linking into all the other systems listed in this standard to include the following:

1.4.1.1 Browser-based access
1.4.1.2 Allow for multiple permission levels
- 1.4.1.2.1 View schedules
- 1.4.1.2.2 Request systems/facilities
- 1.4.1.2.3 Approve systems/facilities use

1.4.1.3 Provide information about instructor/facilitator and their availability
1.4.1.4 Allow for predetermined maximum number of attendees
1.4.1.5 Track and display count of committed attendees
1.4.1.6 Track and display remaining permitted attendees
1.4.1.7 Allow for predetermined maximum number of sites
1.4.1.8 Track and display count of committed sites
1.4.1.9 Track and display remaining permitted sites

1.5 Event clearinghouse component

As system users see a need for pre-scheduled events coordinated among a large number of facilities and administrators, the concept of a virtual location for brokering of events becomes attractive. Such a clearinghouse could serve as a way that event coordinators might let others know the specifics of events they are planning (a certain class with a specific sort of content will be offered on a certain schedule for a certain period of time or a specific event will happen one time on a specific day at a specific time).

Such a clearinghouse could also serve as a way for interested parties to find events that meet their specific needs (a school administrator has a certain number of students who need a specific class that is not offered locally). Availability might also include information about participant or site number limitations (the total seats/sites in the class/event, the number requested/registered so far and the number remaining of the total).

1.5.1 Standards for an event clearing house system

A system should enable online interaction for publishing of event information and be capable of linking into all the other systems listed in this standard to include the following:

- 1.5.1.1 Browser-based access
- 1.5.1.2 Posting of one-time single events
- 1.5.1.3 Posting of sequenced or cyclical events
- 1.5.1.4 Posting of costs to participate in an event
- 1.5.1.5 Permit system administrator defined fields (no less than 256)
- 1.5.1.6 Provide for automated multiple time zone accommodation
- 1.5.1.7 Posting of multiple standard bell schedules related to formal educational events
- 1.5.1.8 Permitting or excluding view of encrypted/secured events such that those with permission may see that the events are available and those without permission won't even be able to know that these events are taking place
- 1.5.1.9 Posting of all, part or none of the information defined in the standards in this document as defined by system administrators
- 1.5.1.10 Use an ODBC compliant relational database
- 1.5.1.11 System administrator defined search/reporting capability
- 1.5.1.12 Posting of facility group affiliation
- 1.5.1.13 Provide for automated email notification of site requests/confirmations
  - 1.5.1.13.1 Events offered
  - 1.5.1.13.2 Events needed
  - 1.5.1.13.3 Event outages
  - 1.5.1.13.4 Event conflicts
- 1.5.1.14 Provide for automated site schedule generation to include
  - 1.5.1.14.1 Events offered
  - 1.5.1.14.2 Events needed
  - 1.5.1.14.3 Event outages
  - 1.5.1.14.4 Event conflicts
- 1.5.1.15 Provide for event cancellation "drop dead" date policies for events to include automated email notifications
  - 1.5.1.15.1 Minimums not met

1.5.1.15.2 Facilities conflict not resolved
1.5.1.15.3 Email notification

1.5.1.16 Provide for links to asynchronous event-related material (eLearning)

1.5.1.17 Provide for automated billing

1.5.1.18 Provide for post event evaluations as defined by system administrators

2.0 Purpose and Objectives

The purpose of this standard is to establish and define the needs for scheduling to be addressed when purchasing and maintaining scheduling coordination systems.

2.1 Background

The State of Nebraska is about to exceed 300 IP-based videoconferencing facilities within the sectors of K-12 education, higher education, informal education, telehealth, and state agencies. In order for any particular entity to be able to connect to any other particular entity (within or outside their subsector), some software system is required to complete the connection, maintain the connection, and to list the directory of participating entities.

The standards expressed herein is a product of a meeting that took place on February 3, 2006, with input from over 20 representatives from the NITC Technical Panel's Statewide Synchronous Video Work Group, coming from institutions all across the State. It is this unselfish dedication to achieving a common good that makes such a software system possible.

When describing scheduling of teleconferencing events there is a variety of descriptive language expressed by those who use the technology. Depending on how "scheduling" is defined, the need may be described on a continuum from "not needed" to "locally coordinated" to "centrally coordinated".

2.2 Objective

The objective of this standard is to enable all existing and future synchronous distance learning and videoconferencing facilities in Nebraska to achieve interoperability and maintain an acceptable quality of service through scheduled and ad hoc event coordination.

3.0 Applicability

These standards apply to synchronous distance learning and videoconferencing facilities as follows:

- If utilizing state-owned or state-leased communications networks:

- Any synchronous distance learning facility or videoconferencing application which utilizes state-owned or state-leased communications networks must comply with the scheduling standards listed in Sections 1.1 through 1.5; or
- The entity must provide, or arrange for, coordination on their behalf through some other entity with the stated capability.

- If using state funding:

  - All **new** facilities or applications receiving state funding must comply with the scheduling standards listed in Sections 1.1 through 1.5.
  - All **existing** facilities or applications receiving state funding for ongoing operations must convert to the standards listed in Sections 1.1 through 1.5 as soon as fiscally prudent or upon renewal of any existing scheduling system service contract, whichever comes first.

- These standards **do not apply** to the following entities:

  - University of Nebraska (relating to the university's academic research mission)
  - Any entity which applies for, and receives, an exemption.

General Statement on Applicability
The Governing board or chief administrative officer of each organization is responsible for compliance with these standards. The NITC will consider adherence to technical standards as part of its evaluation and prioritization of funding requests

3.1 Exemption
Exemptions may be granted by the NITC Technical Panel upon request by an agency or education entity.

3.1.1 Exemption Process
Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion; federal government requirements; or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 521 S. 14th Street, Suite 301, Lincoln, NE 68508). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the NITC Technical Panel may be appealed to the NITC.

4.0 Responsibility

An effective program for scheduling standards compliance involves cooperation of many different entities. Major participants and their responsibilities include:

1. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate quality of service and uniformity for information systems through adoption of policies, standards, and guidelines.
2. Technical Panel Statewide Synchronous Video Work Group. The NITC Technical Panel, with advice from the Statewide Synchronous Video Work Group, has responsibility for recommending scheduling standard policies and guidelines and making available best practices to operational entities.
3. Agency and Institutional Heads. The highest authority within an agency or institution is responsible for interoperability of information resources that are consistent with this policy. The authority may delegate this responsibility but delegation does not remove the accountability.
4. Information Technology Staff. Technical staff must be aware of the opportunities and responsibility to meet the goals of interoperability of information systems.

5.0 Related Documents

5.1 Statewide Synchronous Video Work Group Charter:
http://www.nitc.state.ne.us/tp/workgroups/video/charter.pdf

5.2 Glossary of Technical Terms
http://www.nitc.state.ne.us/itc/citizens/glossary.htm

Nebraska Information
Technology Commission

STANDARDS AND GUIDELINES

Web Cookie Policy

Category	**E-Government Architecture**
Title	**Web Cookie Policy**
Number	

Applicability

☑ **State Government Agencies**
- ☑ All ..... **Policy**
- ☐ Excluding _____ ..... **Not Applicable**

☐ **State Funded Entities -** All entities receiving state funding for matters covered by this document..... **Not Applicable**

☐ **Other:** _____ ..... **Not Applicable**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of _____.
Guideline - Adherence is voluntary.
Policy - A high-level set of principles and acceptable procedures.

Status	☐ Adopted ☑ Draft ☐ Other:_____
Dates	Date: April 11, 2006 Date Adopted by NITC: Other:

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Policy

Nebraska.gov and state agencies may use cookies to store user information subject to the following:

1.1 Permanent Cookies

1.1.1 Will not contain personal identifying information (e.g. names, date of birth, social security number, hint answers).

1.1.2 May be used to save personalized web site settings (e.g. font size, color, text type, etc.).

1.1.3 May include an expiration date if appropriate.

1.2 Session Cookies

1.2.1 Will be erased when a user's web browser session ends or the user logs out of the application.

1.2.2 Will only be accessible to the specific application(s) in use.

1.3 Any use of cookies can be made known to the user through the use of appropriate browser settings.

1.4 The Web Cookie Policy is available on the State Portal.

2.0 Purpose and Objectives

The purpose of this policy is to establish guidance for the use of web cookies on web sites, web pages, and web applications created by State of Nebraska agencies, boards and commissions.

3.0 Definitions

3.1 Web Cookie

Any technique of saving state or tokens stored on a user's computer to be exchanged between a web browser and a web server is considered a cookie (an example of an additional type of cookie is a PIE - Persistent Identification Element).

3.2 Web Page

A document stored on a server, consisting of an XHTML file and any related files for scripts and graphics, viewable through a web browser or the World Wide Web. Files linked from a web page such as Word (.doc), Portable Document Format (.pdf), and Excel (.xls) files are not web pages, as they can be viewed without access to a web browser.

3.3 Web Site

A set of interconnected web pages, usually including a homepage, generally located on the same server, and prepared and maintained as a collection of information by a person, group or organization.

3.4 Web Application

An application that is accessed with a web browser over a network such as the Internet or an intranet.

4.0 Applicability

This policy shall apply to all State of Nebraska agencies, boards and commissions.

Nebraska Information
Technology Commission

STANDARDS AND GUIDELINES

Wireless Local Area Network Standard

Category	**Security Architecture**
Title	**Wireless Local Area Network Standard**
Number	

Applicability

☑ **State Government Agencies**
- ☐ All.....**Not Applicable**
- ☑ Excluding higher education institutions..... **Standard**

☐ **State Funded Entities -** All entities receiving state funding for matters covered by this document.....**Not Applicable**

☑ **Other:** All Public Entities.....**Guideline**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval (see Section 4.1).
Guideline - Adherence is voluntary.

Status	☐ Adopted	☐ Draft	☑ Other: Reviewed
Dates	Date: March 17, 2006 (Draft Revisions) Date Adopted by NITC: September 30, 2003 Other:		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

Executive Summary

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs.

In additional to the inherent risks associated with any wired network, wireless technology introduces several unique vulnerabilities. Since wireless signals are radio transmissions, they can be intercepted by suitable radio receiving devices, sometimes even devices operating outside the intended service area. If data transmissions are not encrypted or are inadequately encrypted, the intercepted data can be read and understood in a matter of seconds. Any data transmission sent through the wireless network is at risk, including correspondence, usernames and passwords, financial data, and other sensitive information. Because wireless transmissions circumvent traditional perimeter firewalls, those existing protections established to prevent unauthorized access are ineffective. Advances in wireless signaling technology may increase transmission distances, further exacerbating the problem of unauthorized reception. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

Also, since wireless network devices operate using radio signals, their proliferation within an area can lead to Radio Frequency Interference (RFI) among these devices and other radio devices using the same frequency bands.

The purpose of this standard is to ensure that only registered and secure WLANs are deployed by state government agencies. This standard provides the following:

1. State agencies must register WLANs, including each Access Point (AP) that connects to the state private network, with the Division of Communications (DOC). [Section 1.1]

2. State agencies must provide for proper management and security of WLANs. [Section 1.2]

3. Provides for resolution of conflicts between wireless devices. [Section 1.3]

4. Requires compliance with other network standards. [Section 1.4]

5. Provides a list of general recommendations for agencies implementing WLANs. [Section 1.5]

Source Notes: A source for portions of the original version of this document and the Division of Communication's Wireless Access Point Checklist was *Special Publication 800-48, "Wireless Network Security 800.11, Bluetooth and Handheld Devices,"* November 2002 published by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. A full copy of that publication is available at http://csrc.nist.gov/publications/nistpubs/index.html. NIST Special Publication 800-48 provides a detailed overview of wireless technology, wireless LANs, wireless personal area networks ("Bluetooth" technology), and wireless handheld devices. Anyone implementing any of these types of wireless systems should read the entire report. Parts of the document were also based on the National Institutes of Health, Wireless Network Policy.

1.0 Standard

This standard applies to state agencies which deploy a Wireless Local Area Network (WLAN).

Wireless services that fall within the definition of Campus Connection, Metropolitan Area Network (MAN), or Wide Area Network (WAN) must be purchased through DAS Information Technology Services (ITS) to comply with state statutes.

1.1 Registration of Wireless Devices

State agencies must register WLANs, including each Access Point (AP) that connects to the state private network, with the Division of Communications (DOC).

1.1.1 Registration

Self-registration is available through a DOC form on the ITS website (See Section 7.1). The registration process will identify: contact information; WLAN device information, including the manufacturer, model, and physical location; and the security/firewall technologies being deployed. Registration should occur prior to deployment.

1.1.2 Review and Approval

The DOC will contact the registering agency after reviewing the registration information.

1.1.3 Naming Convention

Final device names are assigned by the DOC during the registration process to avoid conflicts and confusion, and to aid in incident response and in identifying and locating wireless devices. If technology allows for the broadcast of a device name, standardized names should appear in the broadcast description, along with any unique identifiers assigned to the unit.

1.1.4 Unregistered (Rogue) and Unsecured Devices

Only approved WLANs and access points will be deployed within state agencies. Unregistered (rogue) devices will be removed from service.

Network managers for the DOC will incorporate procedures for scanning and detecting unregistered (rogue) wireless devices and access points. This requires a full understanding of the topology of the network. It also requires performing periodic security testing and assessment, including randomly timed security audits to monitor and track wireless and handheld devices. ITS reserves the right to disable network access for a device, server or LAN if adequate security is not in place.

1.2 Management and Security

1.2.1 Physical Security

Access points must be properly secured within a safe, adequately monitored area to prevent unauthorized access and physical tampering. Devices will not be placed in easily accessible public locations.

1.2.2 Configuration Management

All wireless access points must be secured using a strong password. Passwords will be changed at least every six months. Administrators must ensure all vendor default user

names and passwords are removed from the device. Administration of the device will be prohibited from the wireless network.

1.2.3 Authentication and Encryption

Authentication and encryption is required on all WLANs (see options listed on the registration form for details).

1.2.3.1 Access to Systems and Data

- Agencies and other entities connected to the state's network must employ adequate security measures to protect other systems and data connected to the state's network.
- Once authenticated to an access point, users will either be routed outside the state's firewall(s), or authenticated to the network. Just as with a wired network, state network authentication--whether enterprise-wide or agency-specific-- must satisfy prescribed login/password combinations prior to using enterprise or agency-specific resources that are not normally accessible by nodes outside the state's firewall(s).
- Access control mechanisms such as firewalls must be deployed to separate the wireless network from the internal wired network.
- As the technology permits, wireless networks will employ a combination of layered authentication methods to protect sensitive, proprietary, and patient information.

1.2.4 Risk Management

Agencies using wireless systems must develop general risk mitigation strategies for access points, users, and client devices such as virus protection, password standards, and other preventative measures.

1.3 Disruption and Interference

For state agencies, the DOC will resolve any conflicts between wireless devices in coordination with the affected agencies. Priority is granted to fully supported and registered installations, except in the case of medical, safety, or emergency devices, as appropriate.

1.4 Compliance with Other Network Standards

Agency WLANs must satisfy all existing and future standards pertaining to use and security of the state's network as required by law or established by the Nebraska Information Technology Commission or ITS.

1.5 General Recommendations for Agencies Implementing WLANs

1.5.1 Agencies must not undertake wireless deployment until they have examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of operations. Agencies should perform a periodic risk assessment and develop a security policy before purchasing wireless technologies, because their unique security requirements will determine which products will be considered for purchase.

1.5.2 Agencies must be aware of the technical and security implications of wireless and handheld device technologies.

1.5.3 Agencies must carefully plan the deployment of 802.11, Bluetooth, or any other wireless technology.

1.5.4 Agencies must be aware that security management practices and controls are especially critical to maintaining and operating a secure wireless network.

1.5.5 Agencies must be aware that physical controls are especially important in a wireless environment.

1.5.6 Agencies must enable, use, and routinely test the inherent security features, such as authentication and encryption that exist in wireless technologies.

1.5.7 Where appropriate, agencies must employ protection mechanisms, such as firewalls and intrusion detection systems will be employed.

1.5.8 State agencies must assure all Federal, State, and agency compliance regulations are addressed prior to implementing wireless technology.

1.5.9 Agencies must educate wireless users in wireless security measures and controls to protect information resources they are accessing.

1.5.10 Agencies must utilize the DOC's Wireless Access Point Checklist (see Section 7.3).

2.0 Purpose and Objectives

The purpose of this standard is to ensure that only registered and secure WLANs are deployed by state government agencies.

3.0 Definitions

3.1 Access Point (AP)
A hub or interconnect device on a Local Area Network (LAN) that supports wireless (IEEE 802.11x) devices such as laptops, PDA's, etc. In some cases, the Access Point constitutes a stand-alone LAN where only a few wireless devices that are needed to communicate or share resources.

3.2 Campus Connection
Any building with high-speed access (at least 10Mb) to the 501 building.

3.3 Local Area Network (LAN)
A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. For State agencies, LANs are defined as restricted to rooms or buildings. An interconnection of LANs over a city-wide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas is commonly called a wide area network (WAN).

3.4 Metropolitan Area Network (MAN)

A data communications network that (a) covers an area larger than a local area network (LAN) and smaller than a wide area network (WAN), (b) interconnects two or more LANs, and (c) usually covers an entire metropolitan area, such as a large city and its suburbs.

3.5 Strong Password

A strong password must be a minimum of 8 characters, and possess 2 of the 3 following attributes.

- Must contain at least one (1) numeric,
- Must contain both upper and lowercase letters,
- Must contain special characters (!@#$%^&*{}).

3.6 Wide Area Network (WAN)

A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and is usually spread over a larger geographic area than that of a LAN.

4.0 Applicability

This standard applies to state agencies, excluding higher education institutions, which deploy a Wireless Local Area Network (WLAN).

Wireless services that fall within the definition of Campus Connection, Metropolitan Area Network (MAN), or Wide Area Network (WAN) must be purchased through DAS Information Technology Services (ITS) to comply with state statutes.

4.1 Exemption

Exemptions may be granted by the NITC Technical Panel upon request by an agency.

4.1.1 Exemption Process

Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion, federal government requirement, or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 521 S 14th Street, Suite 301, Lincoln, NE 68508). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the Technical Panel may be appealed to the NITC.

5.0 Responsibility

5.1 Agency and Institutional Heads

The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs, including disaster recovery plans for information technology. The Agency must notify the DOC before implementing a wireless system. Self-registration is available through the ITS website (see Section 7.1). Wireless services that fall within the definition of Campus Connection, MAN or WAN, must be purchased through the ITS to comply with State statutes. The agency authority may delegate this responsibility but delegation does not remove the accountability.

5.2 DAS Information Technology Services Divisions (ITS)

ITS shares responsibility for the security of the state's network. ITS reserves the right to disable network access for a device, server or LAN if adequate security for a wireless connection is not in place.

6.0 Related Documents

6.1 NITC Security Officer Handbook

http://www.nitc.state.ne.us/standards/security/so_guide.doc

6.2 NITC Network Security Policy

http://www.nitc.state.ne.us/standards/index.html

6.3 NITC Incident Response and Reporting Procedures for State Government

http://www.nitc.state.ne.us/standards/index.html

7.0 References

7.1 DOC's Wireless Registration Website

http://wlansupport.ims.state.ne.us/wlan_form.html

7.2 ITS Website

http://its.ne.gov/

7.3 DOC's Wireless Access Approval Process

(LINK TO BE ADDED ~ NITC file URL of appendix)

7.4 DOC's Wireless Access Point Checklist

(LINK TO BE ADDED ~ NITC file URL of appendix)

7.5 NIST Wireless Network Security Special Publication 800-48

http://csrc.nist.gov/publications/nistpubs/index.html

7.6 ITS "Network Security Standards", Draft - February 11, 2003

http://its.ne.gov/

Wireless Access Point Approval Process

1. Review NITC wireless LAN security checklist.
2. Plan wireless installation according to NITC standards.
3. Fill out Wireless Registration Online Form. http://wlansupport.ims.state.ne.us/
4. DOC will verify the Agencies approval of the request.
4. Wait for installation approval from Network Services.
5. Purchase and install equipment
6. Notify Network Services of future replacement or removal of wireless equipment.

Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Wireless Local Area Network Checklist

The table, below, provides a WLAN security checklist. The table presents guidelines and recommendations for creating and maintaining a secure 802.11 wireless network, based on NIST Special Publication 800-48. Items marked 'REQUIRED" must be fulfilled in order to meet the specifications of this standard. Items marked as "Strongly Advise" might provide a higher level of security, but should be weighed against other considerations.

Management

Status	Tasks
REQUIRED	1. Develop an agency security policy that addresses the use of wireless technology, including 802.11.
REQUIRED	2. Maintain a complete inventory of all APs and 802.11 wireless devices.
REQUIRED	3. Ensure that wireless networks are not used until they comply with the agency's and the state's security policies.
Strongly Advise	4. Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become available (prior to purchase).
Strongly Advise	5. Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.
Strongly Advise	6. Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.
Strongly Advise	7. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
Strongly Advise	8. Complete a site survey to measure and establish the AP coverage for the agency.
Strongly Advise	9. Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.
Strongly Advise	10. Perform a risk assessment to understand the value of the assets in the agency that need protection.
Strongly Advise	11. Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
Optional	12. Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).

Technical

Status	Tasks
REQUIRED	13. Change the default SSID in the APs
REQUIRED	14. Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference
REQUIRED	15. Disable all insecure and nonessential management protocols on the APs.
REQUIRED	16. Enable all security features of the WLAN product, including the cryptographic authentication and privacy feature.
REQUIRED	17. Ensure that encryption key sizes are at least 128-bits.
REQUIRED	18. Install antivirus software on all wireless clients.
REQUIRED	19. Ensure that all managed APs have strong administrative passwords.
REQUIRED	20. Enable user authentication mechanisms for the management interfaces of the AP.
Strongly Advise	21. Empirically test AP range boundaries to determine the precise extent of the wireless coverage.
Strongly Advise	22. Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people.
Strongly Advise	23. Restore the APs to the latest security settings when the reset functions are used.
Strongly Advise	24. Understand and make sure that all default parameters are changed.
Strongly Advise	25. Make sure that shared keys are periodically replaced by more secure unique keys.
Strongly Advise	26. Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).
Strongly Advise	27. Install personal firewall software on all wireless clients.
Strongly Advise	28. Deploy MAC access control lists.
Strongly Advise	29. Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.
Strongly Advise	30. Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.
Strongly Advise	31. Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.
Strongly Advise	32. Fully test and deploy software patches and upgrades on a regular basis.
Strongly Advise	33. Ensure that all passwords are being changed regularly.
Strongly Advise	34. Ensure that the “ad hoc mode” for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.
Strongly Advise	35. Ensure that management traffic destined for APs is on a dedicated wired subnet.
Strongly Advise	36. Use SNMPv3 and/or SSL/TLS for Web-based management of APs.
Optional	37. Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends).
Optional	38. Disable the broadcast SSID feature so that the client SSID must match that of the AP.
Optional	39. Validate that the SSID character string does not reflect the agency’s name (division, department, street, etc.) or products.
Optional	40. Disable file sharing on wireless clients (especially in untrusted environments).
Optional	41. Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI.

Optional	42. Use static IP addressing on the network
Optional	43. Disable DHCP.

Operational

Status	Tasks
REQUIRED	44. When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.
Strongly Advise	45. Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.
Strongly Advise	46. Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.
Strongly Advise	47. Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.
Strongly Advise	48. Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.
Strongly Advise	49. Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.
Strongly Advise	50. Fully understand the impacts of deploying any security feature or product prior to deployment.
Strongly Advise	51. Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology.
Strongly Advise	52. If the access point supports logging, turn it on and review the logs on a regular basis.
Optional	53. Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.
Optional	54. Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.
Optional	55. Enable utilization of key-mapping keys (802.1X) rather than default keys so that sessions use distinct keys.
Optional	56. Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features.

Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Information Technology Disaster Recovery Plan Standard

Category	**Security Architecture**
Title	**Information Technology Disaster Recovery Plan Standard**
Number	

Applicability

☑ State Government Agencies

- ☐ **All** ..... Not Applicable
- ☑ **Excluding higher education institutions** ..... Guideline

☐ State Funded Entities - **All entities receiving state funding for matters covered by this document** ..... Not Applicable

☑ Other: **All Public Entities** ..... Guideline

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of _____.
Guideline - Adherence is voluntary.

Status

☐ **Adopted** ☐ **Draft** ☑ **Other: Review**

Dates

Date: April 13, 2006
Date Adopted by Nebraska Information Technology Commission: April 23, 2001
Other:

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard

Each agency must have an Information Technology Disaster Recovery Plan that supports the resumption and continuity of computer systems and services in the event of a disaster. The plan will cover processes, procedures, and provide contingencies to restore operations of critical systems and services as prioritized by each agency. The Disaster Recovery Plan for Information Technology may be a subset of a comprehensive Agency Business Resumption Plan which should include catastrophic situations and long-term disruptions to agency operations.

The Information Technology Disaster Recovery Plan should be effective, yet commensurate with the risks involved for each agency. The following elements, at a minimum, must be included:

- Identification of critical computer systems and services to the agency's mission and business functions.
- Critical systems and services preservation processes and offsite storage strategy and methods to protect storage media.
- Documented dependencies upon other State agency's or entities that support critical systems and services.
- Contingency plans for different types of disruptions to critical systems and services, i.e. hardware failure, etc.
- Information technology responsibilities for implementation and disaster management.
- Procedures for reporting events, as well as escalating an event within an agency.
- Identification of copy distribution and multiple site storage of plan documents.
- Multi-year training, exercising, and improvement plans.
- Annual plan review, revision, and approval process.

2.0 Purpose and Objectives

The purpose of this document is to define, clarify, and standardize Information Technology Disaster Recovery Planning of State government agencies.

2.1 Background

Information Technology Disaster Recovery Plans are based on the following premises:

2.1.1 *Information is an asset.* It has value to the organization and needs to be suitably protected.

2.1.2 *Information resources must be available when needed.* Continuity of information resources and supporting critical systems and services must be ensured in the event of a disruption to business or a disaster.

2.1.3 *Risks to information resources must be managed.* Procedures required to ensure critical systems and services can be recovered and business continuity sustained must be cost effective and commensurate with the value of the assets being protected.

2.2 Objectives

The primary objectives of this Standard are:

2.2.1 To communicate responsibilities for the continuity of government operations;

2.2.2 To establish a plan for restoration of operations following a disaster.

2.2.3 To reduce the risk of loss of state information assets.

2.2.4 To provide a process for the recovery of critical systems and services.

3.0 Definitions

3.1 Agency

Any governmental entity, including state government, local government, or third party entities under contract to the agency.

3.2 Agency Business Resumption Plan

Documents how an agency will continue to function during a disaster.

Note: Items found in an Agency Business Resumption Plan may include, but is not limited to:

- *Business impact analysis, including risk assessment, asset classification, and potential disruption to stakeholders.*

- *Mitigation strategies and safeguards to avoid disasters. Safeguards include, but are not limited to, protective measures such as redundancy, fire suppression, power source protection, and environmental issues.*

3.3 Critical Systems and Services
Those systems, system components (hardware, data, or software), or services that if lost or compromised would jeopardize an agency's ability to continue agency operations.

3.4 Disaster
Any event that threatens or causes the destruction or availability of critical systems and services.

4.0 Applicability

This standard applies to all state government agencies, except Higher Education and those agencies receiving an exemption under Section 4.1. Compliance with Nebraska Information Technology Commission (NITC) standards will be a requirement during consideration of funding for any projects requiring review by the NITC and may be used in audit reviews or budget reviews.

4.1 Exception

Exemptions may be granted by the NITC Technical Panel upon request by an agency.

4.1.1 Exception Process

Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion, federal government requirement; or financial hardship. Requests may be submitted to the Office of the NITC via e-mail or letter (Office of the NITC, 521 S 14th Street, Suite 301, Lincoln, NE 68508). The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the Technical Panel may be appealed to the NITC.

5.0 Responsibility

5.1 NITC

The NITC shall adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. (Neb. Rev. Stat. § 86-516(6))

5.2 Agency and Institutional Heads

The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing disaster recovery/business continuity programs consistent with this standard. The authority may delegate this responsibility but delegation does not remove the accountability.

6.0 Related Documents

6.1 Agency IT Disaster Recovery Plan Standard Content

6.2 Information Security Management Policy

http://www.nitc.state.ne.us/tp/workgroups/security/policies/security_policy.pdf

6.3 Security Breaches and Incident Reporting Policy

http://www.nitc.state.ne.us/tp/workgroups/security/policies/incident_reporting_policy.pdf

State of Nebraska
Agency Comprehensive Information Technology Plan

2004

Due: August 16, 2004

Submit completed plan as an e-mail attachment to:
info@cio.state.ne.us

For an electronic version of this form; instructions; and links to agency IT Plans from 2000 and 2002 go to:
http://www.nitc.state.ne.us/forms/

Agency	
Date	

Form Version: 20040315

1. Agency Contact Information

Person responsible for Information Technology in the agency:

Name	
Phone Number	
E-mail	

Person to contact for additional information about the agency Comprehensive Information Technology Plan:

Name	
Phone Number	
E-mail	

If **this document** is posted on your agency's Web site, please provide the URL for this document:

http://

2. Agency Mission, Goals and Objectives

Describe the mission of the agency. This is a statement of why the agency exists and its fundamental purpose. Describe the primary business goals and objectives for the next five years (or for that timeframe for which they are formally established).

Explain the primary programs or service areas of the agency and whom they impact. This should include primary beneficiaries, partners, and other organizations that have an interest in the agency's activities. Please identify how the organization interacts with these other agencies, local governments, the public, businesses, and other entities. How does the agency promote a customer focus and collaboration with these groups?

Please include the URL, if a fuller explanation of this topic is available on the agency's web site.

3. Current Use of Information Technology

3.A. Existing IT Environment

3.A.1. Applications

Off-the-Shelf Applications
Provide the estimated number of licenses for each of the following applications:

Off-the-Shelf Applications		Number of Licenses (Best estimate, exact number not necessary)	Versions in Use (Optional)
Productivity Suites			
	Microsoft Office Suite		
	Corel WordPerfect Office		
	Other (Specify)		
Internet Browser			
	Microsoft Internet Explorer		
	Netscape / Mozilla		
	Other (Specify)		
Anti-Virus			
	Symantec/Norton		
	McAfee		
	Other (Specify)		
E-mail and Calendaring			
	Microsoft Exchange		
	Lotus Notes		
	Other (Specify)		
Database Management (DBMS)			
IBM DB2 or UDB			
	Client Licenses		
	Server Licenses		
	Mainframe Licenses		
Oracle			
	Client Licenses		
	Server Licenses		
	Mainframe Licenses		
Microsoft SQL Server			
	Client Licenses		
	Server Licenses		
AS/400			
	Licenses		
Other (Specify)			
	Client Licenses		
	Server Licenses		

List any other significant off-the-shelf applications utilized by the agency:

Other Applications
List other significant applications, including custom applications developed for the agency. Include information pertaining to (a) the general purpose of the application; (b) the platform on which it is running; and (c) if a custom applications, development tools used:

3.A.2. Data

Databases
List major databases maintained by the agency and the general purpose of each:

Data Exchange
List the significant electronic data exchanges your agency has with other entities:

3.A.3. Hardware, Operating Systems, and Networks

Hardware
Provide a general description of the elements of the computing environment (mainframe, midrange, PC workstations, etc.).

Desktop Operating System(s)

Operating System	Approximate number of users/licenses
Windows 95, 98, or ME	
Windows NT	
Windows 2000	
Windows XP	
OS/2	
Linux	
Mac OS	
Other (Specify:)	

Networks - LANs and WANs
Provide a general description of the agency's network environment:

Networks – Server Operating System
Indicate the network operating system(s) utilized:

Network Server Operating System	Number of server licenses
Novell Netware	
Windows NT	
Windows 2000	
Windows 2003	
Unix	
Linux	
AS/400	
OS/2 LAN Server	
Other (Specify:)	

3.A.4. Staffing

General Information
Identify, in general terms, the agency personnel resources currently devoted to supporting the items listed in this section (3.A). This should include both personnel whose job titles and description are clearly related to technology, other personnel whose responsibilities relate significantly to technology support regardless of job title, and contract staffing provided to the agency. Please provide an organizational chart, if available, or describe the organizational structure for managing IT related staff.

NIS Tracking
The Nebraska Information System (NIS) includes the capability of tracking personnel service expenditures for staff who are devoted to information technology activities. Have you designated any business units in NIS that are focused on providing information technology services by using Category Code 7 (UDC 00/07)? Or have you used the Time Card Category Code 4 (UDC 06/04) for employees who may need to have their time recorded as I/T related expense?

3.A.5. Other

Please list any other issues relating to your current IT environment:

3.B. Value

Describe and document the tangible and intangible benefits of the agency's investment in information technology.

3.C. Security

Security Policies
Please answer the following questions regarding your agency's efforts to maintain a secure information technology environment. [The questions refer to the Nebraska Information Technology Commission's Security Policies. These policies are available at http://www.nitc.state.ne.us/standards/]

	YES	NO	IN PROGRESS
Has your agency implemented the NITC's Security Policies?			
If your answers to the previous question is NO, has your agency implemented other security policies?			

Agency Contact Information
Please provide contact information for the person responsible for IT security:

Name	
Phone Number	
E-mail	

Narrative
Provide a general description of the agency's efforts to develop and implement a security program:

(NOTE: Agency IT Plans are posted on a state Web server, accessible only from computers on the state network. Agencies have the option of providing security information here, or in the alternative, can submit the information directly to the state CIO and it will not be posted. Contact Steve Schafer at slschafe@notes.state.ne.us or 402-471-4385 to submit your security information in an alternative format.)

3.D. Disaster Recovery and Business Continuity Planning

Definitions. For purposes of this document the term, "Disaster Recovery Plan" refers to preparations for restoring information technology systems following a major disruption. The term, "Business Continuity Plan" refers to preparations for restoring the operational functions of the agency. As used here, disaster recovery is a subset of business continuity, because information technology supports the business functions of the agency.

Questions

	YES	NO	IN PROGRESS
Does your agency have a disaster/emergency recovery plan?			
Does your agency perform regular back-ups of important agency data?			
Does your agency maintain off-site storage of back-up data?			

Narrative
Provide a general description of the agency's efforts regarding disaster recovery and business continuity planning:

3.E. Accessibility (Technology Access for Individuals with Disabilities)

[For more information on accessibility, contact Christy Horn at chorn@nebraska.edu]

	YES	NO
Does your agency include the Nebraska Technology Access Clause in contracts for information technology purchases? [See Neb. Rev. Stat. § 73-205. The Technology Access Clause is available at http://www.nitc.state.ne.us/standards/]		
Does your agency have procedures in place to identify the information technology related requirements of users with disabilities?		
Does your agency provide training opportunities for management, procurement, and technical personnel on how to meet the accessibility needs of users with disabilities?		
Has your agency evaluated its website(s) to ensure accessibility to all persons with disabilities? If yes, what tools were used to evaluate accessibility? ___ http://www.w3.org/WAI/ER/existingtools.html ___ http://www.vischeck.com/ ___ http://www.henterjoyce.com/fs_downloads/jaws_form.asp ___ Other (please specify _____)		

4. Future Uses of Information Technology

4.A. Strategies and Future Direction

This section should summarize the agency's strategies and future direction for information technology within the agency. Topics should include:

- A summary of future changes in uses of technology, which the agency plans to implement.
- A description of the agency's hardware replacement program or strategy.
- An overview of the agency's activities that promote collaboration.
- A discussion of factors and risks that will impact the success of the agency's information technology strategy.
- An overview of plans to implement e-government services.
- Your agency's efforts to retain IT staff, if applicable.

4.B. Information Technology Training

Summarize the agency's efforts to address training needs relating to information technology. This should include:

- Training for users of information technology
- Training for IT staff who develop and support the information technology systems
- List areas/topics for which a training need has been identified by the agency.

4.C. Future IT Projects

List significant information technology projects which are expected to be undertaken by the agency during the next two years.

PROJECT	STATUS (start date, etc.)

4.D. Projects Relating to the NITC's Strategic Initiatives

In creating the Nebraska Information Technology Commission (NITC), the Legislature recognized the need for "developing a statewide vision and strategic plan to guide investments in information technology". Each year, the NITC develops the Statewide Technology Plan that adopts goals and objectives to guide the work of the Commission. The NITC also reviews and prioritizes major information technology projects as part of the biennial budget process. This year, the NITC is proposing several changes to the planning process, in order to give policy makers more information about statewide technology goals. These changes include identifying a list of statewide strategic initiatives, giving agencies an opportunity to address those initiatives in their agency comprehensive information technology plans and biennial budget requests, organizing planning sessions to develop implementation strategies, and preparing a gap analysis for the Governor and Legislature in November.

On March 9, 2004, the NITC adopted a list of eight statewide strategic initiatives. These include (in no order of priority):

1. Statewide Telehealth Network
2. Community IT planning and technology-related economic development
3. Network Nebraska (statewide broadband communications and related services)
4. Statewide Synchronous Video Network
5. E-Learning
6. Enterprise Architecture (for state government agencies)

7. E-Government
8. Security and Business Resumption

A general description of each initiative is available at: http://www.nitc.state.ne.us/forms/.

In this section of the Agency Comprehensive Information Technology Plan, agencies have the option to describe current or proposed activities that would promote one or more of these initiatives. Agencies should also notify Steve Schafer by May 1, 2004, of their interest in these initiatives, in order to be included in any planning sessions this summer.

Although each of these initiatives is important, the NITC does not assume that projects promoting these initiatives are a higher priority than activities supporting agency-specific missions and operations.

STATE OF NEBRASKA
NEBRASKA INFORMATION TECHNOLOGY COMMISSION
AND OFFICE OF THE CIO

AGENCY INFORMATION TECHNOLOGY PLAN

FOR FY 2007-09 BIENNIAL BUDGET

Agency	
Date	

Form Version: DRAFT 20060411
http://www.nitc.state.ne.us/forms/

DRAFT

Notes about this form:

1. **USE.** The *Agency Information Technology Plan* is to be completed by Nebraska state government agencies in advance of the biennial budget process. This is a planning tool for agencies internal use; for review by the Office of the CIO to identify trends and areas for collaboration; and for review by budget analysts. The state CIO is responsible for implementing a "strategic, tactical, and project planning process for noneducation state government information technology that is linked to the budget process" (Neb. Rev. Stat. §86-520(5)) and the Nebraska Information Technology Commission is responsible for adopting "schedules and procedures for reporting needs, priorities and recommended projects" (Neb. Rev. Stat. §86-516(10)). Please note that completion of this plan is not a substitute for inclusion of the agency's project funding needs in the operating request submitted to the DAS-Budget Division.
2. **CONTENTS.** The plan contains four sections:
    - Section 1 is for FY2006-07
        - 1.1. Continuing Current Operations Levels
        - 1.2. Projects Currently Active
        - 1.3. Projects Planned to be Started in FY2006-07
    - Section 2 is for the first year of the biennium, FY2007-08
        - 2.1. Continuing Current Operations Levels
        - 2.2. Projects to be Continued in FY2007-08
        - 2.3. Projects Planned to be Started in FY2007-08
    - Section 3 is for the second year of the biennium, FY2008-09
        - 3.1. Continuing Current Operations Levels
        - 3.2. Projects to be Continued in FY2008-09
        - 3.3. Projects Planned to be Started in FY2008-09
    - Section 4 is for Long Term Plans and Other Information
        - 4.1. Future Plans (Beyond the FY2007-09 Biennium)
        - 4.2. Other Information (A general comment section where agencies can identify issues not captured in another section of the plan. This provides an opportunity to address issues which may, or may not, impact an agency IT budget; such things as known risks, trends, or issues for which there is not currently enough information to be included in the other sections.)
3. **PROJECTS**. The plan asks for information about information technology related "projects." Agencies must use their best judgment in determining what an IT "project" for their agency is. Generally, if an IT related purchase or activity is significant enough to merit specific mention in the agency's budget request, it is a "project."
4. **MULTI-YEAR PROJECTS**. Some projects which will be implemented over multiple years may be listed in more than one section. For example, if Project X is started in the first year of the biennium, it will be listed in Section 2.3.; if Project X will continue into the second year of the biennium, it will then also be listed in Section 3.2.
5. **TABLES**. The plan includes tables for agencies to enter certain costs. Generally, exact figures are not required; best estimates are acceptable. Rows can be added as needed.
6. **OPTIONAL INFORMATION**. Agencies can add comments/narrative to any section of the form as needed. Also, agencies can submit additional documents (including documents in other formats, e.g. Excel spreadsheets) to provide additional information, background or context.
7. **SUBMITTING THE PLAN.** Completed *Agency Information Technology Plans* should be submitted as an email attachment to the Office of the NITC/CIO at the following address: rick.becker@nitc.ne.gov.
8. **DEADLINE.** Completed forms should be submitted by August 16, 2006.
9. **DOWNLOADABLE FORM.** This form is available in Microsoft Word, WordPerfect, and Rich Text Format at http://www.nitc.state.ne.us/forms/. An example of a completed plan is also available.
10. **CHANGES TO THE FORM.** Prior versions of this form included inventory information (number of PCs; software, databases, etc.) and other information about the agency's current use of information technology. The form was revised to focus on the planned future uses of technology by agencies.
11. **PRIOR SUBMITTALS.** All *Agency Information Technology Plans* submitted in 2000, 2002, and 2004 are posted at http://www.nitc.state.ne.us/itc/sg/agencyitplans.htm.
12. **QUESTIONS.** Contact the Office of the NITC/CIO at 402-471-3560 or rick.becker@nitc.ne.gov.

AGENCY CONTACT INFORMATION

Primary Agency IT Contact

(List the person responsible for IT in the agency.)

Name	
Title	
Phone	
Email	

Email Contact List

The Office of the CIO will be updating an email list of agency IT contacts. The list will be used to provide general IT related updates and information to agencies. Use the space below to list any individuals in your agency you would like included on the list:

Name	Title	Email Address

1. Fiscal Year 2006-07 (Currently Budgeted)

1.1. Continuing Current Operations Levels

[This portion of the document describes the elements and associated costs that are associated with maintaining the agency's current Information Technology Operations level. This usually consists of the staff, technical training, hardware, and software necessary to continue providing the same IT services, at the same level, for the agency IT customers (internal and external). If an agency is large enough to have a dedicated IT staff, this section should include line item(s) identifying costs for administration and management of the agency's information technology organization.]

Item	Description	Cost

1.2. Projects Currently Active

[This portion of the document describes the active IT projects that are currently being worked on. It usually contains a description of the project, the current project status, projected completion date and costs versus original planned dates and costs.]

Project Title (include a brief description if not evident from the title)	**Current Status** (including projected completion date and costs versus original planned date and costs)	**FY2006-07 Costs**	**Total Project Cost**

1.3. Projects Planned to be Started in FY2006-07

[This portion of the document describes the IT projects that are planned to start before the end of the current fiscal year. It usually will contain a description of the project, projected completion date and costs.]

Project Title (include a brief description if not evident from the title)	**Projected Completion Date**	**FY2006-07 Costs**	**Total Project Cost**

2. First Fiscal Year of the Biennium (FY2007-08)

2.1. Continuing Current Operations Levels

[This portion of the document describes the elements and associated costs that are associated with maintaining the agency's current Information Technology Operations level. This usually consists of the staff, technical training, hardware, and software necessary to continue providing the same IT services, at the same level, for the agency IT customers (internal and external). If an agency is large enough to have a dedicated IT staff, this section should include line item(s) identifying costs for administration and management of the agency's information technology organization.]

Item	Description	Cost

2.2. Project Planned to be Continued in FY2007-08

[This portion of the document describes the active IT projects that will be worked on in FY2007-08 which were started in a previous fiscal year. It usually will contain a description of the project, projected completion date and costs.]

Project Title (include a brief description if not evident from the title)	**Projected Completion Date**	**FY2007-08 Costs**	**Total Project Cost**

2.3. Projects Planned to be Started in FY2007-08

[This portion of the document describes the IT projects that are planned to be started in FY2007-08. It usually will contain a description of the project, projected completion date and costs.]

Project Title (include a brief description if not evident from the title)	**Projected Completion Date**	**FY2007-08 Costs**	**Total Project Cost**

3. Second Fiscal Year of the Biennium (FY2008-09)

3.1. Continuing Current Operations Levels

[This portion of the document describes the elements and associated costs that are associated with maintaining the agency's current Information Technology Operations level. This usually consists of the staff, technical training, hardware, and software necessary to continue providing the same IT services, at the same level, for the agency IT customers (internal and external). If an agency is large enough to have a dedicated IT staff, this section should include line item(s) identifying costs for administration and management of the agency's information technology organization.]

Item	Description	Cost

3.2. Project Planned to be Continued in FY2008-09

[This portion of the document describes the active IT projects that will be worked on in FY2008-09 which were started in a previous fiscal year. It usually will contain a description of the project, projected completion date and costs.]

Project Title (include a brief description if not evident from the title)	**Projected Completion Date**	**FY2008-09 Costs**	**Total Project Cost**

3.3. Projects Planned to be Started in FY2008-09

[This portion of the document describes the IT projects that are planned to be started in FY2008-09. It usually will contain a description of the project, projected completion date and costs.]

Project Title (include a brief description if not evident from the title)	**Projected Completion Date**	**FY2008-09 Costs**	**Total Project Cost**

4. Long-Term Plans and Other Information

4.1. Long-Term Plans (beyond the FY2007-09 Biennium)

[This portion of the document describes any long range planning for IT projects that are to be started after the FY2007-09 biennium. It usually will contain a description of the project, projected completion date and costs.]

Agency Narrative:

Project Title (include a brief description if not evident from title)	**Projected Completion Date**	**Projected Cost**

4.2. Other

[A general comment section where agencies can identify issues not captured in another section of the plan. This provides an opportunity to address issues which may, or may not, impact an agency IT budget; such things as known risks, trends, or issues for which there is not currently enough information to be included in the other sections.]

Agency Narrative: