Technical Panel
of the
Nebraska Information Technology Commission
Wednesday, September 17, 2003 - 9:00 a.m.
Nebraska State Office Building, Lower Level A
301 Centennial Mall South
Lincoln, Nebraska

AGENDA

Meeting Documents:
Click the links in the agenda
or click here for all documents (1 MB)

1. Roll Call and Meeting Notice

2. Public Comment

3. Approval of Minutes* - August 13, 2003

4. Technical Architecture

   - Recommendation to the NITC*

Groupware Architecture	Blocking Unsolicited Bulk E-Mail / "SPAM"	Comment 1: Alternate Version Comment 2
	Blocking E-Mail with Attachments	Comment 1 Comment 2 Comment 3
E-Government Architecture	Internet GOV Domain Naming Convention	Comment 1
Security Architecture	Wireless Local Area Network Guidelines	
	Remote Access Guidelines	

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

   - Accessibility Architecture Work Group
   - CAP
   - Security Architecture Work Group
   - Statewide Synchronous Video Network Work Group
   - Wireless Project
   - NIS

6. Other Business

7. Next Meeting Date

   Wednesday, October 8, 2003

8. Adjourn

* Denotes Action Item

NITC and Technical Panel Websites: http://www.nitc.state.ne.us/
Meeting notice posted to the NITC Website: 15 AUG 2003 (Revised meeting date and location posted 20 AUG 2003.)
Meeting notice posted to the Nebraska Public Meeting Calendar: 15 AUG 2003
Agenda posted to the NITC Website: 15 SEP 2003

TECHNICAL PANEL

Nebraska Information Technology Commission
Wednesday, August 13, 2003, 9:00 a.m.
Varner Hall, 3835 Holdrege Street
Lincoln, Nebraska

PROPOSED MINUTES

MEMBERS PRESENT:

Mike Beach, Nebraska Educational Telecommunications
Steve Henderson (alt. for Brenda Decker, Department of Administrative Services, State of Nebraska)
Christy Horn, University of Nebraska
Kirk Langer, Lincoln Public Schools, K-12 Representative
Steve Schafer, Chief Information Officer, State of Nebraska
Walter Weir, Chief Information Officer, University of Nebraska

CALL TO ORDER, ROLL CALL, AND MEETING NOTICE

Mr. Weir called the meeting to order at 9:07 a.m. All members were present at the time of roll call. A quorum existed to conduct official business. The meeting notice was posted to the NITC Website and the Nebraska Public Meeting calendar websites on July 11, 2003. The agenda was posted to the NITC Website on August 8, 2003.

PUBLIC COMMENT

Gene Hand introduced Don Gray as a new staff member with the Public Service Commission.

APPROVAL OF JULY MINUTES

Mr. Langer moved to approve the July 9, 2003 minutes as presented. Mr. Beach seconded the motion. Roll call vote: Beach-Yes, Henderson-Yes, Horn-Yes, Langer-Yes, Schafer-Yes, and Weir-Yes. Motion was carried by unanimous vote.

TECHNICAL ARCHITECTURE - Recommendation to the NITC

Groupware Architecture - Use of Computer-based Fax Services by State Government Agencies

The document was posted for the 30-day comment period. There were no comments.

Mr. Beach moved to recommend that the NITC adopt the Use of Computer-based Fax Services by State Government Agencies. Ms. Horn seconded the motion. Roll call vote: Weir-Yes, Schafer-Yes, Langer-Yes, Horn-Yes, Henderson-Yes, and Beach-Yes. Motion was carried by unanimous vote.

TECHNICAL ARCHITECTURE - Set for Public Comment

Groupware Blocking Unsolicited Bulk E-mail/"SPAM"

This is on the agenda to be discussed at the State Government Council meeting tomorrow. Discussion occurred regarding Lotus Notes, SPAM blocking and legitimate e-mail, K-12 efforts in SPAM blocking, staff optioning out of SPAM blocking software, and blocking E-mail with attachments.

Mr. Schafer moved that the draft document, Groupware-Blocking Unsolicited Bulk E-mail/"SPAM," be posted for the 30-day comment period. Mr. Henderson seconded the motion. Roll call vote: Henderson-Yes, Horn-Yes, Langer-Yes, Schafer-Yes, Weir-Yes, and Beach-Yes. Motion was carried by unanimous vote.

Groupware - Blocking E-mail with Attachments

This is on the agenda to be discussed at the State Government Council meeting tomorrow. It was suggested to include a statement providing alternative methods for transmitting documents.

Mr. Langer moved that the draft document, Groupware-Blocking E-mail with Attachments, be posted for the 30-day comment period. Mr. Beach seconded the motion. Roll call vote: Schafer-Yes, Langer-Yes, Horn-Yes, Henderson-Yes, Beach-Yes and Weir-Yes. Motion was carried by unanimous vote.

E-Government Architecture – Internet GOV Domain Naming Convention

This is on the agenda to be discussed at the State Government Council meeting tomorrow. It is stated in the standards process that any deviation must be approved by the Division of Communications.

Ms. Horn moved that the draft document, E-Government Architecture–Internet GOV Domain Naming Convention, be posted for the 30-day comment period. Mr. Schafer seconded the motion. Roll call vote: Horn-Yes, Henderson-Yes, Beach-Yes, Weir-Yes, Schafer-Yes, and Langer-Yes. The motion carried by unanimous vote.

Security Architecture–Wireless Local Area Network Guidelines

This is on the agenda to be discussed at the State Government Council meeting tomorrow. More state agencies are utilizing wireless technology. The document is a result of the efforts of the Security Work Group. The guidelines were developed by researching what other state's are doing. NIST (National Institute on Standards Technology) was a resource.

It was recommended to be more specific about the Registration of Wireless Devices and to include a training recommendation prior to the use of wireless technology. Another recommendation was to provide an additional paragraph regarding HIPPA not being addressed in the document as well as a warning regarding additional security requirements.

Mr. Beach moved that the draft document, Security Architecture–Wireless Local Area Network Guidelines, be posted for the 30-day comment period. Mr. Schafer seconded the motion. Roll call vote: Langer-Yes, Schafer-Yes, Weir-Yes, Beach-Yes, Henderson-Yes, and Horn-Yes. The motion carried by unanimous vote.

Security Architecture–Remote Access

This is on the agenda item to be discussed at the State Government Council meeting tomorrow.

Ms. Horn moved that the draft document, Security Architecture–Wireless Local Area Network Guidelines, be posted for the 30-day comment period. Mr. Langer seconded the motion. Roll call vote: Henderson-Yes, Beach-Yes, Schafer-Yes, Weir-Yes, Langer-Yes, and Horn-Yes. Motion was carried by unanimous vote.

TECHNICAL ARCHITECTURE–Scheduled for Review

Minimum Workstation Configuration Guidelines for K-12 Public Education

Ms. Horn moved to adopt the revised Minimum Workstation Configuration Guidelines for K-12 Public Education. Mr. Langer seconded the motion. After discussion regarding the changes to the document, Mr. Becker offered a friendly amendment to the motion to make the document a "resource document" rather than a guideline or standard. Ms. Horn and Mr. Langer accepted the amendment. The motion now reads:

Ms. Horn moved to adopt the revised Minimum Workstation Configuration Guidelines for K-12 Public Education and that the document become a resource document. Mr. Langer seconded the motion. Roll call vote: Beach-Yes, Weir-Yes, Henderson-Yes, Schafer-Yes, Horn-Yes, and Langer-Yes. Motion was carried by unanimous vote.

Minimum Workstation Configuration Guidelines

Discussion occurred regarding technical support. It was recommended to include a statement regarding IT technical support and additional costs. It was by group consensus that the statement be included in both documents.

Mr. Schafer moved to adopt the revised Minimum Workstation Configuration Guidelines and that the document become a resource document. Mr. Weir seconded the motion. Roll call vote: Henderson-Yes, Horn-Yes, Langer-

Yes, Schafer-Yes, Weir-Yes, and Beach-Yes. Motion was carried by unanimous vote.

REGULAR INFORMATION ITEMS AND WORK GROUP UPDATES (as needed)

Accessibility, Christy Horn. The Gallup Corporation has contacted UNL for assistance regarding the accessibility of their web site. Teachers College is working with Kent Hendrickson to provide closed captioning for the handicap.

CAP, Steve Schafer. There is a meeting tomorrow, August 14th. The bids for Phase II are due today. Evaluation team is in place for review of the bids. Mr. Weir has staff working on the business plan. Mr. Schafer is making changes in the Customer Service Manual to include Public Service Commission's eligibility information.

Ms. Horn left the meeting at 10:35 a.m.

Security Work Group, Steve Schafer. The work group has not met since early July. The Security Assessment consultant has completed their work. Reports specific to agencies are available to them via the state Guardian website. There will also be a general report that will be available soon. There is funding left from the original grant that may be used for vulnerability assessment. Mr. Weir reported that the University is in the process of hiring a person to be responsible for security related issues.

Statewide Synchronous Video Network Work Group, Mike Beach. Preliminary round one recommendations include the following:

1. Recommend a State-level Internet Protocol (IP) network that maintains a satisfactory, user-defined Quality of Service for interactive distance learning, telemedicine, videoconferencing and date.

2. Recommend two contracts at the local level; one for procurement and maintenance of connective terminal hardware and another one for transport.

3. If the authority does not already exist, recommend to the NITC that it work with the Public Service Commission to draft clarification language that allows providers to offer different service rates for public and private entities.

4. If the authority does not already exist, recommend to the NITC that it work with Legislature to authorize a discounted rate for public entities for data services within flexibly provisioned bandwidth.

5. Recommend to the NITC that it work with the Legislature and the Public Service Commission to provide a one-time capital investment, compliant with NITC technical standards, for the replacement or upgrade of equipment at existing sites when current contracts expire or are re-negotiated.

The work group has other informational documents on the NITC website. Technical Panel members were asked to provide input and/or suggestions on the document. The final recommendations will be presented to the Technical Panel at the September meeting for adoption for final approval by the NITC. Mr. Beach was commended on his efforts.

Wireless. No report. Mr. Schafer stated that he attended their meeting and the group had passed several resolutions and are moving forward. Much of the work has been done through sub-committees.

NIS. No report. Mr. Schafer stated that progress is being made on the punch list. A post-implementation team has been established.

OTHER BUSINESS

NEXT MEETING DATE AND ADJOURNMENT

The next meeting of the NITC Technical Panel will be held on Wednesday, September 10th at 9:00 a.m. at Varner Hall in Lincoln, Nebraska.

Mr. Langer moved to adjourn the meeting. Mr. Henderson seconded the motion. All were in favor. Motion was carried by

voice vote.

The meeting was adjourned at 11:15 a.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by Rick Becker of the Office of the CIO/NITC.

NEBRASKA INFORMATION TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

XX-XXX Blocking Unsolicited Bulk E-Mail / "SPAM"

Category	**Groupware**
Title	**Blocking Unsolicited Bulk E-Mail / "SPAM"**
Number	**XX-XXX**

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:** _____ .....**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.

Status	☐ Adopted	☑ Draft	☐ Other:_____
Dates	Date: August 8, 2003 Date Adopted by NITC: Other:		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

1.0 Guideline

Agencies shall be allowed to evaluate and implement methods for blocking SPAM e-mail, even if some legitimate messages are blocked. Most e-mail should be accepted. Allowing the unhindered flow of legitimate state correspondence is a primary consideration of this standard. Minimum guidelines for State agencies implementing SPAM blocking methods are:

1. Must notify the e-mail originator that their message was blocked and say why.
2. Should notify e-mail originator, when possible, of alternative methods for delivering legitimate mail.
3. Should notify e-mail originator, when possible, of how to resume sending email to the state without being blocked.
4. Should not block a high volume of legitimate incoming e-mail.
5. Should not place an undue burden on Nebraska citizens for legitimate communications with the state.

2.0 Purpose and Objectives

The need for the state to access information on the Internet also allows for access from entities on the Internet into the state infrastructure, unless precautions are implemented. This guideline addresses the burden on state resources due to unsolicited bulk e-mail (UBE), spam and how state agencies may address the issue. (The term "spam" is used to denote mass unsolicited mailings, .) Agencies cannot expect to "solve" all problems that arise from bulk e-mail, only mitigate them. Policy recommendations for generally acceptable bulk e-mail practices are not addressed in this document. Agencies should use these recommendations when developing policies concerning what outside e-mail to accept.

Unsolicted email (SPAM) creates a significant drain of technical and operational resources. In 2003, the state will receive an estimated 2 million SPAM messages for approximately 12,000 employees using email. These numbers will likely continue to rise. SPAM email needs to be reduced to the extent possible without adding excessive costs or exceptional risks to normal flow of legitimate email.

2.1 Overview

The terms spam, unsolicited bulk e-mail (UBE), and unsolicited commercial e-mail (UCE) all refer to the mass posting of e-mail messages.

Any automated means of sorting out spam from e-mail messages sent by citizens, vendors, or other state agencies will result in the rejection of some valid e-mail. Agencies should take special effort to ensure that citizens can conveniently contact state agencies for official business. Blocking legitmate e-mail communication with the state should be minimized.

The goal of this guideline is not to eliminate all forms of bulk e-mail but instead to move part of the burden of dealing with unsolicited e-mail from the recipient to systems administrators. These guidelines should encourage professionalism among

e-mailers, allowing state workers to identify official correspondence more easily while not cutting off access to all bulk e-mail.

2.2 Conforming E-Mail

Most e-mail should be accepted. E-mail that conforms to the following guidelines should not be rejected without good cause. These guidelines on conforming e-mail help administrators as well as recipients to establish a chain of responsibility for the e-mail, and aid automated re-direction or deletion when appropriate. Non-conformance to these guidelines does not imply the agency must necessarily reject the message, but senders who repeatedly send non-conforming e-mail are recognized as unnecessarily adding to the administrative burden of the state's e-mail systems. In general, state agencies should accept bulk e-mail that meets the following minimum requirements.

(1) The sender is identifiable and can be contacted by e-mail. The e-mail contains a valid e-mail address for the sender of the message. If the originator of the message is not the same as the person or company actually sending the message, valid e-mail contact information for both is present.
Valid return addresses allow state workers to respond to e-mail directly, if appropriate, without resorting to the phone, postal mail, or any other method that may be unavailable or inconvenient. Phone numbers and/or postal addresses may be included in addition to the e-mail reply addresses.

(2) The sender discloses how the means of obtaining the e-mail address. The message contains a statement on how the sender obtained the recipient's e-mail address. State agencies and their workers have an interest in how the e-mailer obtained the e-mail address, and this is a vital part of the "chain of responsibility" required of bulk e-mailers. Details of how the addressee got on the list can be given by including lines such as the following within the body of the e-mail message: "This e-mail list was derived from your attendance at the Fall COMDEX conference."

(3) The recipient must "OPT-IN" before being sent any repeat mailings. If the e-mailing was unsolicited, then this must be a one-time-only mailing. A recipient who does not want to receive addition mailings on a topic must not be forced to perform any action. Any repeat mailings can only be as the result of an explicit action on the part of the recipient, such as a request for additional information or to be added to a list.

(4) The sender identifies the e-mail address the message was sent to. Whether for a single mailing or for an opt-in list, the sender must include within the body of the message a statement identifying the full e-mail address the message is being sent to, such as: This message was sent out to: joe.smith@state.ne.us This inclusion allows users and administrators to keep track of e-mail that might pass through multiple computers, aliases, or internal agency e-mail lists before reaching the final recipient, and to help identify e-mail being sent to persons no longer employed by the agency or no longer working in the same capacity.

(5) The recipient is informed how to be removed from the mailing list. The recipient must be informed how to be removed from the mailing list within the body of the message. Just because a recipient doesn't want to be on a particular list does not imply they want to refuse all unsolicited e-mail. The remove instructions must distinguish between being removed from the current list, and all lists maintained by the sender. Merely directing the recipient to a general "list of people who don't want to be on lists" is not sufficient to comply with this guideline.

(6) The message is "reasonably targeted" to the addressee. An unsolicited e-mail should only be sent to someone who might reasonably, in high percentage, be interested in reading the message. See the definitions of "targeted", "narrowed", and "indiscriminate" e-mail lists, below.

2.3 Examples of E-Mail That Should Be Rejected

(1) E-mail that cannot be traced to a valid source computer. When the apparent originating computer of an e-mail has no name, or an invalid name, such as when that computer's name does not appear in the Domain Name System (DNS) database of computer names, that e-mail may be rejected. As with any other rejection criteria, e-mail senders with legitimate state business may be denied access because their computer is merely miss-configured, or because of some temporary outage within the DNS database. Invalid source addresses, however, are the mainstay of senders who don't wish to be properly identified, and this is one area where many illegitimate senders can be eliminated.

(2) E-mail relayed without permission. E-mail that was relayed without permission through another computer in an effort to disguise its origin or to place the burden and expense of e-mail delivery upon another computer may be rejected out of hand.

(3) E-mail from addresses or domains posted on the state's subscribed black list. E-mail that is received from sources that have a history of delivering spam. This list of sources are provided to the state through a subscribed service.

2.4 Methods for Blocking SPAM

SPAM Blocking techniques have costs, effectiveness, and usage issues to consider. Agencies may investigate and use the following methods:

DNS Reverse Name Look-up - Blocks SPAM from the most troublesome SPAM producers. This method is easy to implement but has the greatest risk of blocking legitimate email. IT is very difficult for Email senders to understand or fix problems.

White list - Blocks almost all SPAM, but is difficult to implement and confusing for external email senders to understand. Many Email senders will refuse to add their ID to a state white list.

Blacklist - Likely to block 60% of SPAM but is likely to block a small percentage of legitimate email. It is fairly easy to implement, email senders are notified the mail was blocked, and many know what a blacklist is.
Router Blocking - Looks at a manually prepared list of site domain names or IP addresses to block. This method only blocks specific email known to be a problem. This method may not impact the worst SPAM producers. It is easy to implement, but is manually intensive to maintain. Users may not understand the cryptic message sent by a router.
Filtering - May block a significant number of SPAM Messages at a fairly low cost. Some legitimate messages may be blocked. It is fairly easy to implement. Users will see a customized message from most systems. One type of filtering is "Content Filtering". It involves searching for text in body, subject, or the sender information. Another type of filtering is "Blocking", which is based on the number of addresses in the recipients field. It can also use the file extension name or the size of memo.
Personal Rules - User creates rule to delete from in-box. The cost is high, because each individual has to learn how to set up rules. Usually, rules are not very effective against the worst SPAM producers.

2.5 Other Resources

The Internet Mail Consortium (IMC) has published several reports on the problem. "Unsolicited Bulk Email: Mechanisms for Control" (http://www.imc.org/ube-sol.html) lists the technical and legal solutions being discussed and how they affect Internet mail users. "Unsolicited Bulk Email: Definitions and Problems" (http://www.imc.org/ube-def.html) provides precise definitions of UBE and spam issues.

The Coalition Against Unsolicited Commercial Email (http://www.cauce.org/) is also a source of information.

3.0 Definitions

3.1 Targeted e-mail list

A "targeted" e-mail list is a collection of e-mail addresses where the sender may reasonably expect that all or nearly all of the addressees will be interested in the solicitation. An example of this would be a list of conference attendees, where the conference host may reasonably assume that past attendees will be interested in notification about future, similar conferences. Targeted lists are generally acceptable.

3.2 Narrowed e-mail list

A "narrowed" e-mail list is a collection of addresses that can be expected to contain a higher-than-average percentage of addressees interested in the solicitation. An example of this would be the use of a list of computer conference attendees to send a solicitation for the purchase of computer cabling services. While such conference attendees may be more likely than the general population to have an interest in such a solicitation, such a broad solicitation might be an unreasonable transfer of costs from the sender to the recipient when only a small percentage of the total recipients

are likely to be interested, even though that percentage is higher than would be found on an indiscriminate list.

3.3 Indiscriminate e-mail list

An "indiscriminate" list is one where the sender would have little or no reasonable expectation that the addressee would have more interest in the solicitation than the general population. An example of this would be the sending of a notification of "investment opportunities" to e-mail addresses culled randomly from posters to Usenet newsgroups. "UBE/Spam" e-mail is identified most often with indiscriminate e-mail. The sending of solicitations to state workers as part of a indiscriminate e-mail list is almost always unacceptable.

4.0 Responsibility

Information Management Services Division may investigate and implement methods for the mail routing server, which IMServices supports. Other agencies may elect to share this service or set up their own.

5.0 Related Policies, Standards and Guidelines

Nebraska Information Technology Commission, Individual Use Policy:
http://www.nitc.state.ne.us/tp/workgroups/security/policies/individual_use_policy.pdf

State of Nebraska Acceptable Use Policy of State Data Communications Network,
http://www.doc.state.ne.us/policies/datausage.html

Blocking Unsolicited Bulk E-mail / "SPAM"
Comment 1: Alternate Version

Glen Riedel

09/05/2003 02:23 PM

To: Rick Becker/DASCIO/NEBRLN@NEBRLN
cc: State SPAM Workgroup, Lotus_Administration_Voting_Agencies, Lotus_Notes_Collaboration_Steering_Commitee
Subject: SGC Blocking Unsolicited Bulk E-Mail

Rick:

Here is the final version of the State Spam Workgroup's document on Blocking Unsolicited Bulk Email.

Please use it to replace the existing version that was presented to the NITC - Technical Panel.

Please let me know if there are any upcoming meetings that this will be discussed so I can answer any questions that may arise.

Thanks!

Glen Riedel, CNE
Senior IS Analyst
Nebraska Dept of Insurance
402.471.4432

NEBRASKA INFORMATION TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

XX-XXX Blocking Unsolicited Bulk E-Mail / "Spam"

Category: Groupware

Title: **Blocking Unsolicited Bulk E-Mail / "Spam"**

Number: **XX-XXX**

Applicability

☑ **State Government Agencies,** excluding Higher Education ..... **Standard**

☐ **State Government Agencies, all ..... 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.

Status: ☐ Adopted ☑ Draft ☐ Other:_____

Dates

Date: September 5, 2003

Date Adopted by NITC:

Other:

Prepared by: Technical Panel of the Nebraska Information Technology Commission

Authority: Neb. Rev. Stat. § 86-1506(6)

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

1.0 Technical Standard

Agencies shall be allowed to evaluate and implement methods for blocking Unsolicited Bulk Email (UBE) or spam in relation to their changing email needs, even if some legitimate e-mail is blocked. State Agencies that choose to adopt UBE blocking methods must meet these minimum standards.

1. Agencies must periodically review blocked email statistics to determine its effectiveness and to help reduce the non-delivery of legitimate email.

2. UBE blocking methods must attempt to send notification to legitimate originators of blocked email with the following information:
   a. The email was blocked.
   b. Possible reasons for non-delivery and information on how to restore legitimate communications.
   c. List of alternate methods of communication that maintains reasonable levels of convenience and places no undue hardship on the sending or receiving party.
   d. Links to related state statutes, standards, or guidelines used.

Cost sharing - Where feasible, agencies should work to pool resources to reduce costs to Nebraska. Agencies seeking to purchase UBE-blocking tools should consult with DASIMS managers.

Knowledge sharing - A public web site should be created to share State of Nebraska research on UBE issues.

2.0 Purpose and Objectives

This standard addresses the burden on state resources due to UBE and how state agencies may address the issue. Agencies cannot expect to "solve" all problems that arise from UBE, only mitigate them.

UBE creates a significant drain of technical and operational resources. In 2003, the state will receive an estimated 2 million UBE messages for approximately 12,000 employees using e-mail. These numbers will likely continue to rise. UBE needs to be reduced to the extent possible without adding excessive costs or exceptional risks to normal flow of legitimate e-mail.

2.1 Overview

The terms spam and Unsolicited Bulk E-mail (UBE) both refer to the mass receipt of e-mail messages that are usually inappropriate for state operations.

Any automated means of sorting out UBE from e-mail messages sent by the public, vendors, or other state agencies will typically result in the rejection of some valid e-mail. Agencies should take special effort to ensure that the public can conveniently contact state agencies for official business. Blocking legitmate e-mail communication with the state should be minimized.

2.2 Other Resources

The Internet Mail Consortium (IMC) has published several reports on the problem. “Unsolicited Bulk Email: Mechanisms for Control” (http://www.imc.org/ube-sol.html) lists the technical and legal solutions being discussed and how they affect Internet mail users. “Unsolicited Bulk Email: Definitions and Problems” (http://www.imc.org/ube-def.html) provides precise definitions of UBE and spam issues.

The Coalition Against Unsolicited Commercial Email (http://www.cauce.org/).

The State of Nebraska UBE resource web site (www.ims.nol.org/spam).

3.0 Definitions

3.1 Spam - A common term for UBE is "spam", although that term encompasses a wider range of intrusive transmissions. For instance, the term "spam" originated in the realm of Usenet news, not email. There, individuals cannot request or refuse bulk email, although some newsgroups explicitly permit or encourage its inclusion as a part of the group charter. For further information, see RFC2635 at the Internet Engineering Task Force, http://www.ietf.org.

3.2 UBE - Unsolicited Bulk Email, or UBE, is Internet mail ("email") that is sent to a group of recipients who have not requested it. A mail recipient may have at one time asked a sender for bulk email, but then later asked that sender not to send any more email or otherwise not have indicated a desire for such additional mail; hence any bulk email sent after that request was received is also UBE.

4.0 Applicability

Agencies with their own mail servers can utilize the standard UBE filtering methods provided by the State Internet email gateway. To reduce duplication costs, agencies should consider utilizing the State Internet email gateway before implementing their own.

5.0 Responsibility

Information Management Services Division may investigate and implement UBE filtering methods on the State Internet e-mail gateway, which IMServices supports. Other agencies may elect to share this service.

6.0 Related Policies, Standards and Guidelines

Nebraska Information Technology Commission, Individual Use Policy:
http://www.nitc.state.ne.us/tp/workgroups/security/policies/individual_use_policy.pdf

State of Nebraska Acceptable Use Policy of State Data Communications Network,
http://www.doc.state.ne.us/policies/datausage.html

Blocking Unsolicited Bulk E-mail / "SPAM"
Comment 2

Dennis Burling
IT Manager
NE Environmental Quality
402.471.4214

Blocking email

section 2.2 number 3 second sentence, should read ....receive additional email.....

NEBRASKA INFORMATION TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

xx-xxx Blocking E-mail with Attachments

Category	**Groupware Architecture**
Title	**Blocking E-Mail with Attachments**
Number	**XX-XXX**

Applicability

☑ **State Government Agencies**
- ☑ All.....**Guideline**
- ☐ 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.

Status	☐ Adopted	☑ Draft	☐ Other:_____
Dates	Date: August 13, 2003 Date Adopted by NITC: Other:		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

1.0 Technical Guideline

1.1 Blocking E-Mail with Attachments

E-mails that include attachments with certain extensions should be blocked at the SMTP gateway. Setting up the blocking criteria at the SMTP gateway will stop incoming Internet mail with those attachments from being delivered. The blocking will also stop outgoing Internet mail with those attachments from being sent. If any of the extensions listed below are detected, the e-mail will be deleted and a standard non-delivery report (NDR) will be returned to the sender stating that the e-mail was not delivered. Inter-Agency mail going through a SMTP gateway with the extensions listed below will be blocked. All other attachments should be allowed to pass through and agencies can determine what other safeguards to activate on their mail servers.

Extensions to be blocked at the SMTP server:

scr - screensaver	bas - basic
bat - batch	cmd - command
com - command, executable	cpl - control panel applet
exe - executable program	inf - set up
msi - install control file	msp - probably a windows installer patch
mst - windows installer transform	reg - Microsoft registry
vbs - visual basic	pif - windows program information file
wsf - Windows Script File	

1.2 Alternative Methods for Receiving Files

If an individual needs to receive an attachment with one of the extensions above, the sender can be asked to rename the file extension. For example, Proposal.exe.ForSue

Other alternatives for transmitting files should also be considered, including FTP; Web-based document retrieval; and document repositories.

2.0 Purpose and Objectives:

It is important to take steps to protect our environment against the threat of viruses. Attachments with certain extensions are often used in virus attacks because of their execution access and the amount of damage they can cause.

3.0 Definitions

N/A

4.0 Applicability

State Government Agencies – Agencies using E-mail are encouraged to follow this guideline.

5.0 Responsibility

Anyone running a State SMTP Gateway should consider following this guideline.

6.0 Related Policies, Standards and Guidelines

(http://www.nitc.state.ne.us/standards/)

Security Policies – Information Security Management

Blocking E-Mail with Attachments
Comment 1

Ron Ritchey
09/02/2003 11:10 AM

To: Rick Becker/DASCIO/NEBRLN@NEBRLN
Subject: Re: Blocking E-Mail with Attachments - Final Draft

Blocking attachments in email are usually handled in two different ways. One is blocking the entire message if it has an unwanted attachment and the other is to remove any unwanted attachments before passing the message through. This document only discusses the first so we should probably add a section that talks about the latter. I would suggest the following additions. I didn't change the blocking e-mail with attachments section. Just included with my changes.

1.0 Technical Guideline

Attachments with specific extensions should not be allowed into the State network and mail systems. There are two standard ways to accomplish this. The first is to block any message that contains specific attachments from being delivered. The second is to remove any attachment with the unwanted extension before allowing the memo into the State.

Blocking E-Mail with Attachments

E-mails that include attachments with certain extensions should be blocked at the SMTP gateway. Setting up the blocking criteria at the SMTP gateway will stop incoming Internet mail with those attachments from being delivered. The blocking will also stop outgoing Internet mail with those attachments from being sent. If any of the extensions listed below are detected, the e-mail will be deleted and a standard non-delivery report (NDR) will be returned to the sender stating that the e-mail was not delivered. Inter-Agency mail going through a SMTP gateway with the extensions listed below will be blocked. All other attachments should be allowed to pass through and agencies can determine what other safeguards to activate on their mail servers.

Removing Attachments Before Delivery

If the process of "**Blocking E-Mail with Attachments**" is not used, an agency can strip the unwanted attachment before allowing it to be delivered.

Here are some additional extensions that Symantic recommends blocking.
ade – Microsoft access project extention

adp – Microsoft access project	asp – active server pages
chm – compiled HTML help file	crt – security certificate
hlp – windows help file	hta – HTML application
js – JScript	ins – internet communications settings
jse – JScript encoded file	isp – internet communications settings
lnk – shortcut	mdb – Microsoft access application
mst – visual test source file	mde – Microsoft access MDE database
pcd – photo CD image	msc – Microsoft common console document
sct – Windows script component	shb – document short cut

shs – shell script object
vb – VBScript
vsd – visio drawing
vst – targa bitmap file
ws – wordstar file
wsf – windows script file
url – Internet shortcut (Uniform Resource Locator)
vbe – VBScript encoded file
vss – Visual sourcesafe file
vsw – visio workspace file
wsc – windows script component
wsh – windows scripting host settings

Blocking E-Mail with Attachments
Comment 2

Ron Ritchey

08/21/2003 02:56 PM

To: Rick Becker/DASCIO/NEBRLN@NEBRLN
cc:
Subject: Fw: blocking e-mail with attachments

I haven't been able to review this entire document, but the part that suggests renaming a document to Proposal.exe.ForSue could get blocked by some systems because they don't look at just the extension, they look for .exe anywhere in the file name. ProposalEXE.ForSue should work. Zipping and sending in a zip file should work as well, unless we want to try to block attachments in zip files. Some software can do and some can not.

Blocking E-Mail with Attachments
Comment 3

Dennis Burling
IT Manager
NE Environmental Quality
402.471.4214

Just a couple of quick comments for you....

Blocking email comments

I still disagree with the list for blocking email attachments. While the sending and receiving of a virus is a problem, it will not take long for those that wish to send a virus to use a new extension and have it sent anyway.

Also, there is no proposal under the alternate methods for the zipping of files and sending with a zip extension. Would this not be another possibility?

NEBRASKA INFORMATION TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

XX-XXX Internet GOV Domain Naming Convention

Category	**E-Government**
Title	**Internet GOV Domain Naming Convention**
Number	**XX-XXX**

Applicability

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

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

☑ **Other:** Local Government Entities ..... **Standard**

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

Status	☐ Adopted ☑ Draft ☐ Other:_____
Dates	Date: August 13, 2003 Date Adopted by NITC: Other:

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

1.0 Technical Standard

State agencies must use the Nebraska.gov and ne.gov domain names, in addition to any other Internet domain names, assigned to a computer which hosts their primary web site or home page. The naming convention for state agencies appears in §2.5 below.

Local governments choosing to utilize the .gov address must follow the naming convention set forth in § 2.6 below.

2.0 Purpose and Objectives

2.1 Overview

The State of Nebraska is the owner of the Nebraska.gov and ne.gov domains. The use of these domains to date has been primarily for the Nebrask@ Online state portal and second-level portals (NOL for Business, State Employees, Education and Citizens). The purpose of these guidelines is to provide for consistent use of the Nebraska.gov and ne.gov domains by state agencies and local government. For purposes of illustration, the proposed guidelines listed below are shown using ne.gov, but would also apply to nebraska.gov.

2.2 Background

The Federal Networking Council and the Internet Engineering Task Force (IETF) delegated jurisdiction of the Internet GOV (dot-gov) domain to the federal General Services Administration (GSA) in 1997. On March 28, 2003, the GSA published a final rule for making the dot-gov domain available to state and local governments. The final rule (41 CFR Part 102-173) addresses the registration of second-level domain names used in the Internet GOV domain. This registration process assures that the assigned domain names are unique worldwide. Only federal agencies, state governments, local governments, and Native Sovereign Nations may use the Internet GOV domain.

2.3 Who Authorizes Domain Names?

For State and local governments, GSA will accept authorization from appropriate state or local officials. For States, GSA will accept authorization from the Office of the Governor or designee. The Governor has designated the state's Division of Communications (DOC) to be the official registrant for Internet domain names on behalf of the State of Nebraska. This includes the www.state.ne.us and the dot-gov domain names. By agreement with the DOC, Nebrask@ Online will accept requests for assignment of domain names under the Nebraska.gov and ne.gov domains.

For local government, GSA will accept registrations from the mayor (for cities or towns), county commissioner (for counties) or highest ranking IT official. For third-level domain names using Nebraska.gov or ne.gov, the DOC and Nebrask@ Online will accept requests from the highest ranking elected official or the appropriate administrator for the local government entity.

2.4 Is There a Registration Charge for Domain Names

The DOC and Nebrask@ Online will not charge a fee to register third-level domain names for Nebraska.gov and ne.gov.

2.5 What is the Naming Convention for State Agencies?

State agencies shall use the (agency abbreviation).ne.gov format shown below for their home page. In addition, state agencies may use one or more of the following formats for third-level names within the Nebraska.gov and ne.gov domains:

(Agency Abbreviation).ne.gov	(Example: DAS.ne.gov)
(Partial Agency Name).ne.gov	(Example: AdministrativeServices.ne.gov)
(Division Name).ne.gov	(Example: CommunicationsDivision.ne.gov)
(Program Name).ne.gov	(Example: NVCN.ne.gov)

DOC and Nebrask@ Online will use the following rules to resolve potential conflicts between agencies:

2.5.1 First priority shall go to the commonly used agency abbreviation.

2.5.2 Second priority shall go to the program name, if it is in wide use or has the potential to be widely used by the general public or a large number of constituents of the program.

DOC and Nebrask@ Online will have exclusive use of extensions to the second-level domain names. Examples include www.ne.gov/citizen and www.ne.gov/business.

2.6 What is the Naming Convention for Local Government?

The format for third-level domain names for cities is www.cityname.ne.gov. (Example: www.lincoln.ne.gov)

The format for third-level domain names for counties is www.countynamecounty.ne.gov. (Example: www.lincolncounty.ne.gov)

The format for other local governments will incorporate either the description or acronym of the type of political subdivision into the third-level name. (Examples: www.lowerplattesouthNRD.ne.gov; www.lincolnpublicschools.ne.gov.)

Local governments may request other formats, if they do not conflict with other domain names or have the potential to create confusion. For example, www.lpsnrd.ne.gov might be acceptable, but www.lps.ne.gov would cause confusion.

DOC and Nebrask@ Online will use the following rules to resolve potential conflicts among political subdivisions or between political subdivisions and state agencies:

2.6.1 First priority shall go to the formats described above for state agencies, cities and counties;

2.6.2 Second priority shall go to the name that is in wide use or has the potential to be widely used by the general public or a large number of constituents;
2.6.3 Third priority shall go to the entity, which is first to request a third-level domain name.

3.0 Definitions

3.1 Domain

Domain is a region of jurisdiction on the Internet for naming assignment.

3.2 Domain Name

Domain name is a name assigned to an Internet server. Typically, one would apply this name to a domain name server. A domain name locates the organization or other entity on the Internet. The dot gov part of the domain name reflects the purpose of the organization or entity. This part is called the Top-Level domain name. The Second-Level Domain name to the left of the dot gov maps to a readable version of the Internet address. **Nebraska.gov** is a second-level domain name. The Third-Level Domain name maps to the left of the Second-Level Domain name. **Lincoln.ne.gov** is an example of a Third-Level Domain Name. The Domain Name server has a registry of Internet Protocol (IP) address numbers that relate to the readable text name.

3.3 Domain Name Server

Domain name server is the computer that provides pointers from the domain name to the actual computers.

3.4 Dot-gov

Dot-gov refers to domain names ending with a ".gov" suffix. The Internet GOV domain is another way of expressing the collection of dot-gov domain names.

3.5 Internet GOV Domain.

Internet GOV Domain refers to the Internet top-level domain "dot-gov" operated by the federal General Services Administration for the registration of U.S. government-related domain names. In general, these names reflect the organization names in the Federal Government and non-Federal governmental entities in the United States. These names are now being used to promote government services and increase the ease of finding these services.

4.0 Related Policies, Standards and Guidelines

Federal Management Regulation, Internet GOV Domain, Final Rule – 41 CFR Part 102-173 (http://www.nic.gov/final_rule_102.html).

Internet GOV Domain Naming
Comment 1

To: State Government Council and Technical Panel
From: Lotus Administrators Workgroup
Subject: Internet GOV Domain Naming Convention
Date: September 8, 2003

The Lotus Administrators Workgroup has concerns regarding the passing of the Internet GOV Domain Naming Convention standard that will require the use of **nebraska-dot-gov (nebraska.gov)** and **ne-dot-gov (ne.gov)**. It seems that there is already a widely used standard at the State of Nebraska, which is the domain of **state-dot-ne-dot-us (state.ne.us)**. Adding or changing to another domain will bring complications and confusion to the Internet community.

The standard of 'state.ne.us' is a simple standard based on political geography (RFC 1480) and has been widely accepted by a good majority of the state. Anyone accessing a web site of 'state.ne.us' will know that they are receiving information from Nebraska State Government. To include city and county examples, the city of Lincoln is using 'ci.lincoln.ne.us' and the county of Lincoln is using 'co.lincoln.ne.us'. The 'ci' and 'co' identify city and county government in much the same way that 'state' identifies state government. By using this naming convention, there is a very high probability that I can directly access any city, county, or state government just by entering their most logical web address. This standard allows for uniqueness and very low conflict in domain name assignments.

It is our understanding that by adding 'ne.gov' as a standard, new web sites or web sites that are using 'state.ne.us' can use 'ne.gov'. Since cities and counties will be authorized to register under 'ne.gov' on a first-come-first-serve basis (i.e. 'lincoln.ne.gov' or 'max.ne.gov'), the Internet user will not know if they are getting information from either city, county, or state government. There would also be the possibility that 'max.ne.gov' is a server at the state therefore eliminating the city of Max the opportunity in its use.

Implementing 'ne.gov' seems very simple, but the manageability and costs can be quite high. As we see agencies adopting this new standard, other agencies already using 'state.ne.us' will want to change to 'ne.gov'. Requests for changing email addresses will also be made. While the cost of changing to 'ne.gov' would be minimal for the smaller agencies (say less than 100 employees), the costs of changing the larger agencies (say Health and Human Services) can be quite large and we believe this has not been taken into consideration. Currently, over 65 percent of the state employees are using 'state.ne.us' in their email address. Eventually, the Governor will demand that a single standard be used and the monies will need to be spent to change either one way or the other.

Although the Lotus Notes Administrators workgroup is always open to new ideas and changes to making electronic operations and communications at the State of Nebraska easier and more efficient. In this specific instance, it was agreed that the costs and risks of adding this change to an already established and generally accepted domain naming convention outweighed any substantial immediate short-term benefits that could be gained.

If you have any questions or comments on this document, please contact:

Glen Riedel, Lotus Administrator
NE Dept of Insurance
402.471.4432
griedel@doi.state.ne.us

NEBRASKA INFORMATION TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

XX-XXX Wireless Local Area Network Guidelines

Category	**Security Architecture**
Title	**Wireless Local Area Network Guidelines**
Number	**XX-XXX**

Applicability

☑ **State Government Agencies**
- ☐ All.....**Not Applicable**
- ☑ Excluding higher education institutions.....**Standard (§1.1) and 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:_____
Dates	Date: August 13, 2003 Date Adopted by NITC: Other:		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard and Guidelines

STANDARD (For state government agencies only, excluding higher education institutions.)

1.1 Registration of Wireless Devices

- Registration of access clients is not required unless the same device is configured as an access point.
- All wireless network access points should be registered with the network manager for that entity. State agencies must register Wireless Local Area Networks with IMServices. Self-registration will be available through the IMServices web site (www.ims.state.ne.us). The registration process will identify: a) the physical location of the network, b) the security/firewall technologies being deployed, and c) the types of services or information that is available through the wireless LAN. IMServices reserves the right to disable network access for a device, server or LAN if adequate security for a wireless connection is not in place. Wireless services that fall within the definition of campus connection, MAN or WAN must be purchased through the Division of Communications to comply with State statutes.
- 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.
- Only approved and registered access points will be deployed within state agencies. Unapproved (rogue) devices should be removed from service.

GUIDELINES

1.2 Management and Security of Access Points

- *Physical Security*: Access points should be properly secured within a safe, adequately monitored area to prevent unauthorized access and physical tampering. Devices should not be placed in easily accessible public locations.
- *Configuration Management*: All wireless access points should be secured using a strong password. Passwords should be changed at least every six months. Administrators should ensure all vendor default usernames and passwords are removed from the device. Administration of the device should be prohibited from the wireless network.
- *Rogue Wireless LANS*: Network managers for each entity should 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.

1.3 Broadcast Security and Encryption

- Agencies deploying wireless technology should adhere to minimum encryption standards, and follow best practices for secure installations.

1.4 Access to Systems and Data

- Agencies and other entities connected to the state's network must employ adequate security to protect other systems and data connected to the state's network.
- Once authenticated to an access point, users should 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-- should 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 should be deployed to separate the wireless network from the internal wired network.
- As the technology permits, wireless networks should employ a combination of layered authentication methods to protect sensitive, proprietary, and patient information.

1.5 Naming Conventions

- Final device names are assigned 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.

1.6 Disruption and Interference

- All newly deployed wireless technologies should satisfy all existing and future standards as required by law or established by the NITC or the Information Management Services Division pertaining to use and security of the state's network.
- An entity's network manager should resolve any conflicts between wireless devices. Priority is granted to fully supported and registered installations, except in the case of medical, safety, or emergency devices, as appropriate. For state agencies, excluding higher educational institutions, IMServices will resolve any conflicts between wireless devices, in coordination with affected agencies.

2.0 Background

2.1 Purpose and Objectives

In some situations, wireless technology offers important advantages in terms of convenience, flexibility and cost savings over other types of networking. A major disadvantage of wireless technology is its inherent security risks. If not deployed properly, a wireless local area network (LAN) offers open access to everyone in the vicinity who has a wireless card in his or her PC, laptop, Personal Digital Assistant (PDA), wireless messaging devices or other computing devices.

The purpose of these guidelines is to encourage wise decisions regarding whether and how to implement wireless technology. The primary source of these guidelines is the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce, which has issued Special Publication 800-48, "Wireless Network Security 800.11, Bluetooth and Handheld Devices," November 2002. A full copy of this publication is available at: (http://csrc.nist.gov/publications/nistpubs/index.html).

NIST Special Publication 800-48 is 119 pages long. It 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, which is incorporated into these guidelines by reference. The following guidelines copy the executive summary and the checklist in NIST SP 800-48 that specifically pertain to wireless LANs. Parts of the Executive Summary and most of Section D are based on the National Institutes of Health Wireless Network Policy.

As a final cautionary note, the ease and convenience of setting up wireless LANs should not outweigh the responsibility of every agency to consider the "security needs of other agencies or institutions connected to the network".

In addition to following the NIST SP 800-48, any public entity implementing wireless technology should notify that entity's network manager before connecting the wireless device to the entity's network. State government agencies, excluding higher educational institutions, must comply with notification procedures established by the Division of Communications and the Information Management Services Division, as described in Section 1.1.

These general guidelines do not replace or supercede any specific standards and procedures of operational entities, which have responsibility for managing communications networks.

2.2 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. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders.

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, launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

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.

This document provides an overview of wireless networking technologies and wireless handheld devices most commonly used in an office environment and with today's mobile workforce. This document seeks to assist agencies in reducing the risks associated with 802.11 wireless local area networks (LAN), Bluetooth wireless networks, and handheld devices.

These guidelines recommend the following actions:

1. Agencies should be aware that maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. Moreover, it is important that agencies assess risks more frequently and test and evaluate system security controls when wireless technologies are deployed.

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

3. Agencies should be aware of the technical and security implications of wireless and handheld device technologies.

4. Agencies should carefully plan the deployment of 802.11, Bluetooth, or any other wireless technology.

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

6. Agencies should be aware that physical controls are especially important in a wireless environment.

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

8. In addition, firewalls and other appropriate protection mechanisms, such as intrusion detection systems should be employed.

3.0 Definitions

3.1 **Access Point**. 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 need to communicate or share resources.

3.2 **Campus Connection**. (to be defined)

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 within a limited geographical area, such as a military base, is commonly referred to as a campus area network. 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, such as nationwide, 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 **Personal Digital Assistant (PDA)**. A handheld computer that serves as an organizer for personal information. It generally includes at least a name-and-address database, a to-do

list, and a note taker. PDAs are pen-based and use a stylus to tap selections on menus and to enter printed characters. The unit may also include a small on-screen keyboard that is tapped with the pen. Data are synchronized between a user's PDA and desktop computer by cable or wireless transmission.

3.6 **Smart Card**. A credit card with a built-in microporcessor and memory that is used for identification or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times.

3.7 **Virtual Private Network**. A means by which certain authorized individuals (such as remote employees) can gain secure access to an organization's intranet by means of an extranet (a part of the internal network that is accessible via the Internet).

3.8 **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. Note 1: WANs may include physical networks, such as Integrated Services Digital Networks (ISDNs), X.25 networks, and T1 networks. Note 2: A metropolitan area network (MAN) is a WAN that serves all the users in a metropolitan area. WANs may be nationwide or worldwide.

3.9 **Wireless Application Protocol (WAP)**. A standard for providing cellular telephones, pagers, and other handheld devices with secure access to e-mail and text-based Web pages.

3.10 **Wired Equivalent Privacy (WEP)**. Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

4.0 Applicability

These guidelines are intended to be useful to all public entities that are developing their own security policies and procedures for wireless networks. They specifically apply to state government agencies, excluding higher educational institutions.

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 authority may delegate this responsibility but delegation does not remove the accountability.

5.2 **Agency Information Officer**. The Agency Information Officer or delegate must notify the Division of Communications and the Information Management Services Division before implementing a wireless system.

5.3 **Information Management Services Division (IMServices)**. IMServices shares responsibility with the Division of Communications for the security of the state's network. State agencies must register Wireless Local Area Networks with IMServices. Self-registration will be available through the IMServices web site (www.ims.state.ne.us). IMServices reserves the right to disable network access for a device, server or LAN if adequate security for a wireless connection is not in place.

5.4 **Division of Communications (DOC)**. DOC shares responsibility for the security of the state's network with IMServices. Wireless services that fall within the definition of campus

connection, MAN or WAN, must be purchased through the Division of Communications to comply with State statutes.

6.0 Related Policies, Standards and Guidelines

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 NIST Wireless Network Security Special Publication 800-48 (http://csrc.nist.gov/publications/nistpubs/index.html)

7.2 National Institutes of Health (NIH) Wireless Network Policy, January 24, 2003, (http://www1.od.nih.gov/oma/manualchapters/management/2807/)

7.3 Information Management Services Division, "Network Security Standards" (Draft, February 11, 2003), www.ims.state.ne.us.

APPENDIX

Wireless LAN Security 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. Most of the recommendations are "best practices", which all agencies should be followed. Items marked as "Should Consider" might provide a higher level of security, but should be weighed against other considerations.

Management Recommendations

Status	Recommendation
	1. Develop an agency security policy that addresses the use of wireless technology, including 802.11.
	2. Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.
	3. Perform a risk assessment to understand the value of the assets in the agency that need protection.
	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).
	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.
	6. Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.
	7. Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).
	8. Complete a site survey to measure and establish the AP coverage for the agency.
	9. Take a complete inventory of all APs and 802.11 wireless devices.
	10. Ensure that wireless networks are not used until they comply with the agency's and the state's security policies.
	11. Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
	12. Place APs in secured areas to prevent unauthorized physical access and user manipulation.

Technical Recommendations

Status	Recommendation
	13. Empirically test AP range boundaries to determine the precise extent of the wireless coverage.
	14. Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends).
	15. Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people.
	16. Restore the APs to the latest security settings when the reset functions are used.
	17. Change the default SSID in the APs.
	18. Disable the broadcast SSID feature so that the client SSID must match that of the AP. (Should Consider)

	19. Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.
	20. Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference.
	21. Understand and make sure that all default parameters are changed.
	22. Disable all insecure and nonessential management protocols on the APs.
	23. Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy feature.
	24. Ensure that encryption key sizes are at least 128-bits.
	25. Make sure that default shared keys are periodically replaced by more secure unique keys.
	26. Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).
	27. Install antivirus software on all wireless clients.
	28. Install personal firewall software on all wireless clients.
	29. Disable file sharing on wireless clients (especially in untrusted environments).
	30. Deploy MAC access control lists. (Should Consider)
	31. Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.
	32. Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications. (Should Consider)
	33. Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.
	34. Fully test and deploy software patches and upgrades on a regular basis.
	35. Ensure that all APs have strong administrative passwords.
	36. Ensure that all passwords are being changed regularly.
	37. Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI. (Should Consider)
	38. 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.
	39. Use static IP addressing on the network. (Should Consider)
	40. Disable DHCP. (Should Consider)
	41. Enable user authentication mechanisms for the management interfaces of the AP.
	42. Ensure that management traffic destined for APs is on a dedicated wired subnet.
	43. Use SNMPv3 and/or SSL/TLS for Web-based management of APs.

Operational Recommendations

Status	Recommendation
	44. 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.
	45. Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.
	46. Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information. (Should Consider)

	47. Consider other forms of authentication for the wireless network such as RADIUS and Kerberos. (Should Consider)
	48. Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity. (Should Consider)
	49. Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity. (Should Consider)
	50. Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features. (Should Consider)
	51. Enable utilization of key-mapping keys (802.1X) rather than default keys so that sessions use distinct WEP keys.
	52. Fully understand the impacts of deploying any security feature or product prior to deployment.
	53. 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. (Should Consider)
	54. Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features. (Should Consider)
	55. 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.
	56. If the access point supports logging, turn it on and review the logs on a regular basis.

NEBRASKA INFORMATION TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

XX-XXX Remote Access Guidelines

Category	**Security Architecture**
Title	**Remote Access Guidelines**
Number	**XX-XXX**

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:_____
Dates	Date: August 8, 2003 Date Adopted by NITC: Other:		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

1.0 Guidelines

1.1 All home networks connected to the Internet via a broadband connection should have some firewall device installed. Personal software firewalls installed on each computer are useful and effective, but separate, dedicated, and relatively inexpensive hardware firewalls that connect between the broadband connection and the telecommuter's computer or network can provide greater protection. Organizations should consider using both personal and hardware firewall devices for high-speed connections. When both a software personal firewall and a separate device are in operation, the organization can screen out intruders and identify any rogue software that attempts to transmit messages from the user's computer to an external system.

1.2 Web browsers should be configured to limit vulnerability to intrusion. Web browsers also represent a threat of compromise and require additional configuration beyond the default installation. Browser plugins should be limited to only those required by the end user. Active code (such as ActiveX or Java) should be disabled or used only in conjunction with trusted sites. The browser should always be updated to the latest or most secure version. Privacy is always a concern with web browsers. The two greatest threats to this privacy are the use of cookies and monitoring of web browsing habits of users by third parties. Cookies can be disabled or selectively removed using a variety of built-in web browser features or third-party applications.

1.3 Operating system configuration options should be selected or disabled as appropriate to increase security. The default configuration of most home operating systems is generally inadequate from a security standpoint. File and printer sharing should almost always be disabled. The operating system and major applications should be updated to the latest and most secure version or patch level. All home computers should have an anti virus program installed and configured to scan all incoming files and e-mails. The anti virus program should have its virus database updated on a regular basis. Another concern for many telecommuters is the surreptitious installation of spyware by certain software applications. This spyware, while usually not intended to be malicious, reports information on users (generally without their knowledge) back to a third party. This information could be general information about their system or specifics on their web browsing habits. A variety of programs are available for detecting and removing this spyware..

1.4 Selection of wireless and other home networking technologies should be in accordance with security goals. Several home networking technologies are available for telecommuters who wish to connect their home PCs together to share resources. Some of these technologies are the same as their office counterparts (e.g., Ethernet), and others are designed specifically to meet the needs of telecommuters (e.g., phone- and power-line networking). While most of these technologies can be made relatively secure, some represent a threat to security of both the home network and, sometimes, the office network. In particular, wireless networking has vulnerabilities that should be carefully considered before any installation.

1.5 Public entities should provide telecommuting users with guidance on selecting appropriate technologies, software, and tools that are consistent with the agency network and with agency security policies. Users have many approaches to choose from in establishing an off-site office. Sophisticated technologies such as virtual private networks (VPNs) can provide a high level of security, but are more expensive and complex to implement than other solutions. Whenever practical, agencies should provide telecommuting users with systems containing pre-configured security software and necessary hardware. If

possible, agency security administrators should update and maintain the systems as well, to minimize reliance on users who are not specialists in security features. (It is not always financially or logistically practical for agencies to provide users with pre-configured systems, and this recommendation should not be taken as a requirement of this publication.) Many users, particularly if they do not require interactive access to agency databases, can obtain an adequate degree of security at very low cost and with little additional software, easing burdens on both the user and system administrators at the central computing system. The benefits and risks of telecommuting are here to stay. Computing resources and access to office networks while on the road or working from home is too valuable for most organizations or employees to give up. While there will always be risks associated with remote access to an organization's resources, most of these risks can be mitigated through careful planning and implementation. By the same token, even though broadband connections generally represent a greater threat than dial-up connections, the threat can be reduced through careful configuration and the judicious use of the security tools and techniques discussed in this document.

2.0 Background

2.1 Purpose and Objectives

This document sets forth policies and guidelines for acquiring and managing resources used for remote access to the state's network. The following guidelines copy the Executive Summary and other information from the National Institute Standards and Technology (NIST) Special Publication, 800-46, "Security for Telecommuting and Broadband Communications". A full copy of this publication is available at: (http://csrc.nist.gov/publications/nistpubs/index.html).

Anyone implementing remote access should read the entire NIST Special Publication, 800-46, which is incorporated into these guidelines by reference.

These general guidelines do not replace or supercede any specific standards and procedures of operational entities, which have responsibility for managing communications networks.

2.2 Executive Summary

Telecommuting has become a popular trend in the workplace. As employees and organizations employ remote connectivity to corporate and government networks, the security of these remote end points becomes increasingly important to the overall security of a network. Accompanying and contributing to this trend is the explosive growth in the popularity of broadband connections for telecommuters. These developments complicate the process of securing organizational and home networks. This document assists organizations in addressing security issues by providing recommendations on securing a variety of applications, protocols, and networking architectures. Recommendations in this publication are designed for State government agencies, educational institutions and other public entities, but may be useful to commercial organizations and home users as well. Home broadband architectures face a variety of threats that, while present on dial-up connections, are easier to exploit using the faster, always-on qualities of broadband connections. The relatively short duration of most dial-up connection makes it more difficult for attackers to compromise telecommuters dialed-up to the Internet. "Always on" broadband connections provide attackers with the speed and communications bandwidth necessary to compromise home computers and networks. Ironically, as governmental and corporate organizations have hardened their networks and become more sophisticated at protecting their computing resources, they have driven some malicious entities to pursue other targets of opportunity. Telecommuters with broadband connections are these new targets of opportunity both for

their own computing resources and as an alternative method for attacking and gaining access to government and corporate networks.

State agencies and their employees can take a variety of actions to better secure their telecommuting and home networking resources.

3.0 Definitions

3.1 Access Point. 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 need to communicate or share resources.

3.2 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 within a limited geographical area, such as a military base, is commonly referred to as a campus area network. 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, such as nationwide, is commonly called a wide area network (WAN).

3.3 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.

3.4 Personal Digital Assistant (PDA). A handheld computer that serves as an organizer for personal information. It generally includes at least a name-and-address database, a to-do list, and a note taker. PDAs are pen-based and use a stylus to tap selections on menus and to enter printed characters. The unit may also include a small on-screen keyboard that is tapped with the pen. Data are synchronized between a user's PDA and desktop computer by cable or wireless transmission.

3.5 Smart Card. A credit card with a built-in microprocessor and memory that is used for identification or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times.

3.6 Virtual Private Network. A means by which certain authorized individuals (such as remote employees) can gain secure access to an organization's intranet by means of an extranet (a part of the internal network that is accessible via the Internet).

3.7 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. Note 1: WANs may include physical networks, such as Integrated Services Digital Networks (ISDNs), X.25 networks, and T1 networks. Note 2: A metropolitan area network (MAN) is a WAN that serves all the users in a metropolitan area. WANs may be nationwide or worldwide.

3.8 Wireless Application Protocol (WAP). A standard for providing cellular telephones, pagers, and other handheld devices with secure access to e-mail and text-based Web pages.

3.9 Wired Equivalent Privacy (WEP). Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

4.0 Applicability

These guidelines are intended to be useful to all public entities that are developing their own security policies and procedures for remote access. They specifically apply to state government agencies, excluding higher educational institutions.

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 authority may delegate this responsibility but delegation does not remove the accountability.

5.2 **Agency Information Officer**. In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest-ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies, including disaster recovery planning for information technology.

5.3 **Agency Security Officer**. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for preparing a disaster recovery plan for information technology. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan for information technology.

6.0 Related Policies, Standards and Guidelines

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 National Institute Standards and Technology (NIST) Special Publication, 800-46, “Security for Telecommuting and Broadband Communications”. A full copy of this publication is available at: (http://csrc.nist.gov/publications/nistpubs/index.html).

APPENDIX

A. Home Computer Security Checklist

1. **Anti Virus Software --** Anti virus application is installed and is configured to:
   a. Start with the boot of the operating system.
   b. Run in the background and automatically scan all incoming files.
   c. Enable web browser protection, if available.
   d. Automatically update the virus signature database weekly.
   e. Schedule it to be run at least weekly to scan all hard drive files.
   f. Attempt to recognize unknown viruses, if available.
2. **Spyware Removal Tools**
   a. Install and run a spyware removal tool to identify and eliminate (as appropriate) spyware.
   b. On a monthly basis, update and run spyware removal tool, again eliminate discovered spyware if appropriate.
3. **Firewall**
   a. A firewall is an application that is employed to monitor and limit dangerous packets from entering a network, providing the capability to:
   b. Log all suspicious traffic (this is generally true for default installs).
   c. Examine log on a periodic basis.
   d. Block traffic to ports that support services that should not be accessible from the Internet (e.g., NetBIOS, Telnet, etc.).
   e. Automatically lock out network access to the host when network connectivity is not required (e.g., when the screensaver activates or computer is inactive for a fixed period of time).
   f. Notify the user when an application attempts to make an outbound connection.
   g. Medium to high level of security (e.g., “paranoia level”).
4. **Encryption Software**
   a. Ensure that appropriate encryption software is being used.
5. **Securing the Operating System**
   a. Secure or disable file and printer sharing.
   b. Ensure that the latest operating system patches are installed.
   c. Use a password protected screensaver to lock it during periods of inactivity.
   d. Where appropriate use a BIOS password to restrict who is able to start the system.
   e. Turn your system off when it is not being used.
6. **Securing Wireless Networks**
   a. Place wireless base station away from outside walls in order to minimize transmission of data outside of building.
   b. Use additional encryption beyond WEP (VPN, PGP, etc.).
   c. Enable 128-bit WEP encryption.
   d. Change SSID to a hard to guess password.
   e. Enable additional authentication schemes supported by your wireless base station.
   f. Disable broadcasts of SSID in the wireless base station beacon message.
   g. Disable SNMP or change the SNMP community strings to a hard-to-guess password.
   h. Install personal firewall on all wireless clients.
7. **Online Security Assessment**
   a. An online security assessment has scanned the current configuration (including the firewall).
   b. All major vulnerabilities identified by the assessment have been corrected and confirmed by a rescan.
8. **Securing Web Browsers**
   a. Browser(s) configured to limit or disable plugins.
   b. Browser(s) configured to limit ActiveX, Java, and JavaScript.

B. Laptop Security Checklist

The need for an explicit laptop security checklist can be illustrated by the fact that, according to Safeware Insurance in 1999, the number of laptop computers stolen outnumbered the number of desktop computers stolen by almost 12 to 1.

1. **Review Home Computer Security Checklist**
   a. Where applicable, the appropriate elements from the home computer security checklist presented previously should be applied to a laptop computer. (Not all elements from home computer security checklist may apply.)
2. **Encryption Software**
   a. Although mentioned above in the home computer security checklist, encryption is vital for protecting sensitive information on a mobile computer. Operating system features such as encrypting file system (EFS) or even discretionary access control (DAC) permissions can provide valuable security for a laptop that is stolen.
   b. Third-party software such as PGP and Norton Internet Security can provide similar levels of protection for laptop data.
3. **Physical Security**
   a. Laptops that spend a majority of their time in two or fewer places should be physically secured with a cable lock.
   b. Cable locks are widely available on the Internet and in computer retail stores.
   c. Almost all major laptop brands contain a slot to attach a lock cable.
   d. Those that do not can have a lock cable glued on.
4. **Set BIOS Password**
   a. Set BIOS password to prompt user every time laptop is powered up.
   b. Check for BIOS updates at least twice a year (or more) to “flash” BIOS.
5. **Use Non-descript carrying case**
   a. Avoid unwanted attention. A leather briefcase or obvious laptop case can attract attention in public places, especially airports, and while on planes.
   b. If traveling with confidential information, pack information or information backup in separate bag from laptop in case of theft.
6. **Identify Laptop with contact information**
   a. Many companies and individuals place decals or markings on the laptop case that are difficult to remove and if done so, indicate obvious tampering.
   b. Record serial number and other identification information about laptop twice, and keep one copy at home or in the office in case of theft. This information can be helpful to authorities searching for the laptop.
7. **Backup all personal data on a regular basis**
   a. In the event that your laptop is stolen, all of your work is essentially useless without a backup of all of your personal data.
8. **Consider purchasing advanced security features**
   a. Should your computing needs or data security warrant it, products that offer increasingly advanced security features such as biometric login, motion sensing, and “Lo-Jack” type location tracking are becoming increasingly cheaper to purchase for laptops.
   b. Software developers are responding to this demand by integrating these new technologies into common tasks of computer usage such as seamlessly logging in to the operating system.

C. Telecommuting Security Checklist

This checklist originally appeared in a Department of Energy publication. Not all items in the list will apply to every organization or telecommuter, but it provides a helpful starting point for an organization or individual to review the security of home computer systems. The checklist also includes considerations for organizations that have telecommuting users who regularly access the organization’s central network.

1. **User Identification and Authorization**
   a. Is the telecommuter authorized by their supervisor/manager to telecommute?

   b. Is the telecommuter authorized by the system owner to access the system(s) remotely?
   c. Does the telecommuter have a unique user ID and password for remote access and for access to sensitive applications?
2. **Access Controls**
   a. Are system access controls in place and functioning to log the identification of each remote access user, device, port, and user activity?
   b. Are system audit logs protected from unauthorized access?
   c. Are banners displayed regarding monitoring for unauthorized access and misuse?
3. **Auditing**
   a. Does the remote access system record alarms and authentication information?
   b. Does the system audit log identify date and time of access, user, origin, success or failure of access attempt?
   c. Are system audit logs retained to support reviews by computer security personnel?
   d. If dial-up access is allowed, does the system record details of access attempts?
4. **Information Availability**
   a. Are Government information assets (hardware, software, data, records) in a physically secure location and protected from theft, fire, smoke, hazardous material, etc.?
   b. Is backup media maintained, secured, and easily retrieved to support established contingency and disaster recovery plans?
   c. Is a physical inventory periodically conducted of Government information assets used for telecommuting?
   d. Can Government information assets be retrieved in the event of employee termination?
   e. Is there a process in place to ensure the most current version of anti virus software is installed on the telecommuting computer?
   f. Are Government information assets adequately secured when not in use by the telecommuter?
   g. Are user IDs and passwords protected from unauthorized use?
5. **Information Confidentiality**
   a. Is Government information protected from unauthorized disclosure (family, friends, eavesdroppers)?
   b. Is encryption used when transmitting sensitive unclassified information?
6. **Remote Access Security Administration**
   a. Is organizational, system administrator, and user responsibility for remote access security defined?
   b. Are justifications for remote access users periodically revalidated to support continued access privileges commensurate with job duties (at least annually)?
   c. Are incident reporting procedures in place to address handling of security breaches?
   d. Is regular system monitoring performed to detect unauthorized access attempts, denial of service, or other security weaknesses?
   e. Is access to network management tools restricted to authorized users?
   f. Is software used for telecommuting legally purchased, and are software-licensing agreements properly maintained?
   g. Are telecommuting equipment hard drives degaussed or overwritten to remove sensitive information in accordance with established best business practices?
7. **Architecture and Network Topology**
   a. Is the telecommuting equipment used interoperable with the computing architecture deployed at the home office?
   b. Does the network adequately separate traffic according to user communities? Does the remote access equipment and system protect the internal trusted network from the external (public) untrusted network?
   c. Are network topology maps documented and kept current?
8. **Education, Awareness, and Enforcement**

a. Are telecommuters and their supervisors trained in the specific risks, threats, vulnerabilities, and proper use of a secure telecommuting environment?
b. Is the telecommuter current on their computer security training?
c. Is the telecommuter aware of the consequences for violation of Condition of Use agreements?

9. **Modem Use**
   a. Is there a single (or otherwise restricted) point of entry via modem into the internal network or server?
   b. Are all dial-up numbers protected from unauthorized disclosure?
   c. Is the telecommuter instructed to disconnect modem connectivity to the home office network or server when not in use?

NITC Technical Panel
Statewide Synchronous Video Work Group

Update and Round One Recommendations
August 13, 2003
Michael Beach, Sponsor

Preliminary Round One Recommendations:

1. Recommend a State-level Internet Protocol (IP) network that maintains a satisfactory, user-defined Quality of Service for interactive distance learning, telemedicine, videoconferencing and data.
2. Recommend two contracts at the local level; one for procurement and maintenance of connective terminal hardware and another one for transport.
3. If the authority does not already exist, recommend to the NITC that it work with the Public Service Commission to draft clarification language that allows providers to offer different service rates for public and private entities.
4. If the authority does not already exist, recommend to the NITC that it work with the Legislature to authorize a discounted rate for public entities for data services within flexibly provisioned bandwidth.
5. Recommend to the NITC that it work with the Legislature and the Public Service Commission to provide a one-time capital investment, compliant with NITC technical standards, for the replacement or upgrade of equipment at existing sites when current contracts expire or are re-negotiated.

Next Steps:

- Distribute first five recommendations to the SSVWG and ask for feedback and modifications by August 6, 2003 (Tom Rolfes).
- Present draft Round One recommendations to the NITC Technical Panel on August 13, 2003 (Mike Beach).
- Research current authority for recommendations #3 and #4 (Gene Hand).
- Begin cost estimations for recommendation #5 (John Horvath, Jeff McCartney)
- Complete survey on each distance learning network by September 30 (SSVWG members)
- Provide briefing to the Public Service Commission on the Statewide Synchronous Video Work Group by August 26, 2003 (Mike Beach, Gene Hand, Brenda Decker).
- Begin discussions with the telecommunication providers about an IP-centric network and flexibly provisioned bandwidth before the end of August 2003 (Steve Schafer, Mike Beach, Brenda Decker, Rick Golden, Gene Hand).
- Present final Round One recommendations to the NITC Technical Panel on September 10, 2003 (Mike Beach)
- Ask for approval of the Round One recommendations by the NITC on September 30, 2003 (Walter Weir).

The next meeting date and location of this work group has not been determined but it will be in September prior to the 30th. Previous Meetings: March 26, May 28, July 30, 2003.