OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

Minnesota State Colleges and Universities

Wireless Network Security Audit

September 8, 2005 **05-48**

Financial Audit Division

The Office of the Legislative Auditor (OLA) is a professional, nonpartisan office in the legislative branch of Minnesota state government. Its principal responsibility is to audit and evaluate the agencies and programs of state government (the State Auditor audits local governments).

OLA's Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division also investigates allegations that state resources have been used inappropriately.

The division has a staff of approximately forty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

Consistent with OLA's mission, the Financial Audit Division works to:

- Promote Accountability,
- Strengthen Legislative Oversight, and
- Support Good Financial Management.

Through its Program Evaluation Division, OLA conducts several evaluations each year.

OLA is under the direction of the Legislative Auditor, who is appointed for a six-year term by the Legislative Audit Commission (LAC). The LAC is a bipartisan commission of representatives and senators. It annually selects topics for the Program Evaluation Division, but is generally not involved in scheduling financial audits.

All findings, conclusions, and recommendations in reports issued by the Office of the Legislative Auditor are solely the responsibility of the office and may not reflect the views of the LAC, its individual members, or other members of the Minnesota Legislature.

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 651-296-1235 (voice), or the Minnesota Relay Service at 651-297-5353 or 1-800-627-3529.

All OLA reports are available at our Web Site: http://www.auditor.leg.state.mn.us

If you have comments about our work, or you want to suggest an audit, investigation, or evaluation, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Dr. James McCormick, Chancellor
Minnesota State Colleges and Universities

We have conducted an information technology audit of wireless computer networks deployed across the Minnesota State Colleges and Universities (MnSCU) system. The scope of our audit focused on wireless network security controls used to protect the integrity and confidentiality of MnSCU business and academic data. The Report Summary highlights our overall conclusion. Our specific audit objective and conclusions are contained in Chapter 2 of this report.

Wireless technology has become an important part of business for the majority of MnSCU's colleges and universities, extending the range of traditional wired computers by providing MnSCU students, faculty, and staff with access to wireless-enabled devices and laptops. However, wireless technology is new and fast-changing; posing a heightened risk of unauthorized access to computer systems and data. We found that MnSCU wireless networks were not thoroughly planned and, as a result, several institutions had significant security weaknesses. We recommend that MnSCU disable all wireless networks that lack strong authentication and encryption controls.

We would like to thank staff from the Office of the Chancellor and the individual colleges and universities for their cooperation during this audit.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: June 17, 2005

Report Signed On: September 2, 2005

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651/296-4708 • Fax: 651/296-4712
E-mail: auditor@state.mn.us • TDD Relay: 651/297-5353 • Website: www.auditor.leg.state.mn.us

Minnesota State Colleges and Universities
Wireless Network Security Audit

Table of Contents

Audit Participation

The following members of the Office of the Legislative Auditor prepared this report:

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Brad White, CPA, CISA	Audit Manager
Neal Dawson, CPA, CISA	Auditor-in-Charge
Eric Wion, CPA, CISA, CISSP	Auditor
John Kelcher	Auditor

Exit Conference

We discussed the findings and recommendations in this report with the following officials of the Minnesota State Colleges and Universities on August 29, 2005:

Laura King	Vice Chancellor – Chief Financial Officer
Ken Niemi	Vice Chancellor – Chief Information Officer
John Asmussen	Executive Director – Internal Auditing
Beth Buse	Deputy Director – Internal Auditing
Bev Shuft	Security Director
John Ladwig	Security Specialist

Minnesota State Colleges and Universities
Wireless Network Security Audit

Report Summary

Key Conclusion:

The Minnesota State Colleges and Universities (MnSCU) did not adequately plan and secure its wireless computer networks. Many wireless networks had security weaknesses, some of which were significant. We recommend that MnSCU disable all wireless networks that lack strong authentication and encryption controls.

Findings:

- MnSCU did not adequately plan and secure many of its wireless networks. (Finding 1, page 8)
- Controls to authenticate users and encrypt wireless data transmissions were weak or nonexistent at several colleges. (Finding 2, page 9)
- Most colleges did not functionally segment their wired and wireless networks to better protect computer systems and data. (Finding 3, page 10)
- Several colleges do not have controls to protect their networks from insecure computers that connect to them. (Finding 4, page 11)
- Several colleges did not adequately monitor their systems and wireless networks. (Finding 5, page 11)

Audit Scope:

Wireless network security controls as of June 2005

Selected Audit Areas:
Wireless networks used by MnSCU universities, colleges, and the Office of the Chancellor

Background:

Almost all of MnSCU's colleges and universities have deployed wireless networks. Wireless networks extend the range of traditional wired networks by using radio waves to transmit data through the air to wireless-enabled devices, such as laptop computers or personal digital assistants (PDAs). While wireless networks offer many potential benefits, including flexibility and mobility, they also introduce significant security risks, such as unauthorized access to computer systems and data. Appropriate controls are needed to mitigate risks and protect the integrity, confidentiality, and availability of MnSCU's computer systems and data.

This page intentionally left blank.

Chapter 1. Introduction

The Minnesota State Colleges and Universities (MnSCU) contracts with the Office of the Legislative Auditor to conduct selected audits for its system of colleges and universities. In planning our information technology audit, we met with MnSCU management to identify important information technology areas needing assessment. We jointly decided to focus the audit on wireless network security controls since MnSCU's use of wireless technology is relatively new, widespread, and may pose significant risks if not properly secured.

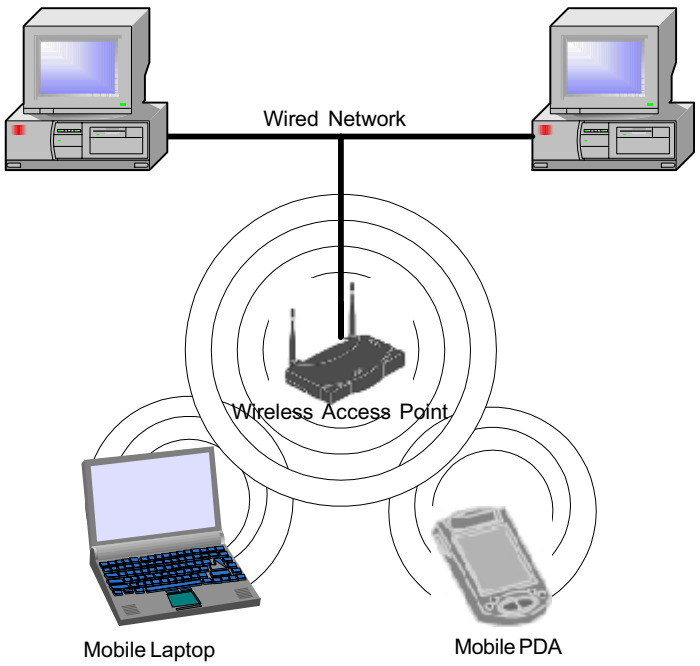
Overview

This information technology audit assessed the adequacy of security controls over the wireless networks deployed by MnSCU colleges, universities, and the Office of the Chancellor. Providing wireless access to computer systems and data for students, staff, and faculty has become an important part of business for nearly every MnSCU institution. In fact, only 2 of 37 campuses reported they had not used any wireless networks.[1] The Office of the Chancellor had no wireless networks in its Saint Paul offices.

Wireless networks extend the range of traditional wired networks by using radio waves to transmit data through the air over relatively short distances, such as across an office building or college campus. In basic terms, wireless networks are comprised of two types of equipment: access points and wireless-enabled devices, such as laptop computers and personal digital assistants (PDAs). As depicted in Figure 1-1, an access point is physically wired to a conventional wired network while broadcasting wireless radio signals. Anyone with a wireless-enabled device within range of the signal can connect to the access point and possibly access the local wired network and the computer systems and data on it.

[1] The Minnesota State Colleges and Universities (MnSCU) is comprised of the Office of the Chancellor and 32 colleges and universities. However, additional campus locations include Hibbing, Itasca, Mesabi Range, Rainy River, and Vermillion which make up a consortium called the Northeast Higher Education District. Also, Northwest Technical College at Bemidji is aligned with Bemidji State University.

Figure 1-1
Example of a Wireless Network



Source: Auditor Prepared

Wireless networks offer colleges several benefits, including more flexibility, mobility, and easier installation. Faculty, staff, or students can access computer systems and data throughout a campus without having to be physically located in a particular office or classroom. Wireless networks are also easier and quicker to install and may result in cost savings since wires do not have to be installed throughout buildings or between buildings.

Despite the potential benefits offered by wireless networks, they also introduce significant risks. These risks include those associated with wired networks, such as worms, viruses, software vulnerabilities, and unauthorized access attempts, plus additional risks that are unique to wireless networks. Wireless networks are known to be vulnerable to several different types of compromises in security. For example, inadequately secured transmissions are susceptible to eavesdropping, impersonation, and other attacks since data is broadcast over radio waves.

Wireless technology has rapidly evolved over the past several years. Initially the technology was extremely insecure and, as a result, other mechanisms were needed to provide adequate security.

Audit Approach

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. These standards require that we obtain an understanding of internal controls relevant to the audit objectives.

For information technology audits, we obtain evaluation criteria from the *Control Objectives for Information and Related Technology* (COBIT). Published by the IT Governance Institute, COBIT includes high-level and detailed control objectives, grouped in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring. To evaluate controls over specific technologies, we relied on information published by the developers of those products. Finally, we used publications distributed by recognized security experts, such as the National Institute of Standards and Technology.

Information technology audits frequently include the review of sensitive security data that is legally classified as *not public* under the Minnesota Data Practices Act. In some cases, to protect state resources and comply with the Minnesota Data Practices Act, we must withhold security-related details from our publicly-released reports. When these situations occur, we communicate all pertinent details to agency leaders in a confidential document. For this audit, we issued a separate, *not public* document to the management of the MnSCU Office of the Chancellor.

This page intentionally left blank.

Chapter 2. Wireless Network Security Controls

Chapter Conclusions

Minnesota State Colleges and Universities (MnSCU) did not adequately plan and secure its wireless computer networks. Many college wireless networks had significant security weaknesses including deficiencies in authentication, encryption, segmentation, and monitoring controls. We recommend that MnSCU disable all wireless networks that lack strong authentication and encryption controls.

Most MnSCU colleges and universities provide some form of wireless access to their students, administrators, faculty, and staff, but the purpose varied. For example, some institutions provided wireless access to the Internet only, while others used it to provide access to college computer systems and data. Although wireless security controls varied at each college, we found that schools that had been using wireless the longest were generally further along in developing good controls.

Each MnSCU university or college is responsible for the day-to-day management and security of its own computer networks, including wireless networks. Though these critical duties are delegated to each college, the Office of the Chancellor retains overall responsibility and authority for the protection of information assets. To fulfill these responsibilities, the Office of the Chancellor has been developing a security program that includes a small security unit and a security policy, standards, and guidelines that colleges and universities must follow. However, limited resources have made development of a comprehensive security program slow and difficult to accomplish. The Office of the Chancellor developed a draft security policy, but it has not yet been finalized and approved by the MnSCU Board of Trustees. While several security standards and guidelines have been developed, much work remains.

Audit Objective

We designed our audit work to answer the following question:

- Did MnSCU design and implement wireless network security controls to protect computer systems and maintain the integrity and confidentiality of data housed in them?

To address this objective, we surveyed information technology staff at the Office of the Chancellor and at each college and university. The survey was used to identify the purpose of any wireless networks deployed and the controls implemented to secure them. After reviewing the initial survey and clarifying responses, we conducted onsite visits at ten locations. During

each onsite visit, we interviewed key information technology and security professionals who oversee the wireless networks and related systems controls. We relied upon inquiries and observations to determine whether certain controls were implemented and, in some cases, used computer-assisted audit tools to test selected controls.

Current Findings and Recommendations

1. MnSCU did not adequately plan and secure many of its wireless networks.

MnSCU did not take the necessary steps to adequately plan and secure the wireless networks deployed across its system of colleges and universities. The Office of the Chancellor did not assess wireless technology risks, nor did it develop any wireless-specific policies, standards, or guidelines for colleges to follow. Also, it did not develop a comprehensive strategy to ensure colleges comply with security policies, standards, and guidelines. As a result, each institution independently implemented its wireless networks with little oversight. In many cases, colleges hired consultants because they lacked the necessary knowledge or personnel to implement wireless technology. Historically, each college and university has been responsible for its own computer networks. However, most institutions also did not conduct formal risk assessments, nor document detailed policies, standards, or guidelines for adequately securing their wireless networks.

We believe that insufficient planning ultimately led to the security weaknesses described in Findings 2 through 5. When questioned, several colleges indicated they lacked adequate staffing, making it extremely difficult to properly manage and secure their wireless networks. Management should not adopt new technologies and services, like wireless, if they can not ensure those services are properly managed and secured. If not addressed, security weaknesses could jeopardize the integrity, confidentiality, and availability of MnSCU's computer systems and data.

Recommendations

- *The Office of the Chancellor and individual institutions should conduct formal risk assessments and develop wireless-specific policies, standards, and guidelines to adequately mitigate risks. Each college and university should assess whether it has sufficient staff and resources to properly manage and secure its wireless networks.*

- *The Office of the Chancellor should develop a comprehensive plan to ensure its colleges and universities comply with system security policies, standards, and best practices on an ongoing basis.*

2. Controls to authenticate users and encrypt wireless data transmissions were weak or nonexistent at several colleges.

Authentication and encryption controls did not exist or were weak at several colleges. Authentication controls help ensure that the person requesting wireless access is authorized to have such access. They also provide accountability by allowing computer activities to be traced back to a particular person. The most common authentication controls require a person to provide a valid user account name and password. Encryption controls convert readable text or data into a format that cannot be read by an unauthorized person. This primarily ensures that *not public* data is safeguarded and not inappropriately disclosed. Strong encryption controls are particularly important with wireless data transmissions because they prevent eavesdropping by hackers. Of the ten locations visited, nine had insecure wireless networks that made it relatively easy for anyone to gain unauthorized access to their internal computer networks or for wireless data to be captured and read:

- Four institutions had no wireless authentication and encryption controls.

- Five institutions had wireless networks with strong authentication and encryption controls; however, the controls could be circumvented by other wireless networks they had on campus that did not adequately authenticate users or encrypt data transmissions.

The above results and college survey responses suggest these weaknesses are relatively common across MnSCU. We feel that MnSCU should disable all wireless networks that do not adequately authenticate users and encrypt transmissions until strong controls can be designed, tested, and implemented. Failure to have such controls could lead to someone gaining unauthorized access to MnSCU's computer systems and jeopardize the integrity and confidentiality of its data.

Finally, many colleges allow unauthenticated or anonymous wireless access, but restrict it to the Internet only. Therefore, anyone within range of the wireless networks can use the college's network to access the Internet without identifying themselves. While this may be highly convenient for legitimate users, it may also expose MnSCU to potential liabilities should a student, hacker, or anyone else use the college's Internet connection to commit an illegal act. Several college technology managers strongly agreed that their colleges should not provide such anonymous access, and alternatively, others felt it was appropriate. At the time of the audit, the Office of the Chancellor had not developed a policy or standards to adequately address this issue.

Recommendations

- *MnSCU should ensure appropriate controls are used to authenticate users and encrypt traffic on all wireless networks. It should disable wireless networks that provide access to internal computer systems without strong authentication and encryption controls.*

- *The Office of the Chancellor should develop a policy and standards to address anonymous wireless Internet access and implement appropriate controls.*

3. Many colleges did not functionally segment their wired and wireless networks to better protect computer systems and data.

Many colleges did not functionally segment their networks to improve security. Typically, segments are created based upon user or computer functions. For example, administrators may be placed in a different segment than students. Similarly, computers running business applications or containing sensitive data may be placed in a different segment than a computer containing public data. Wireless networks should also be isolated or segmented. Network segmentation improves control by only allowing appropriate traffic in or out of each segment. For example, students would be prevented from accessing the segment containing critical administrative applications and data. Segmentation also helps prevent the spread of malicious software such as viruses, worms, and trojans.

Generally, we found that once a user gained access to a college's computer networks, such as through wireless access, they were able to move throughout the networks and could attempt to access any information on them. At one campus, for example, anyone connected to the college's wired or wireless network could attempt to access the computer and database containing *not public* data that the college retrieved from MnSCU's central administrative systems. Although other security mechanisms may prevent unauthorized access, colleges should segment networks and limit access to only those who need it. In another example, an academic department at one campus installed a wireless access point for educational purposes. The access point did not provide any authentication or encryption controls, and it was directly connected to the college's internal computer network. It was not segmented to prevent unauthenticated wireless users from accessing the rest of the network.

We were told that in higher education it is not uncommon for colleges to allow faculty, in computer science or other academic departments, to manage their own computers. One MnSCU college estimated it had between 60 and 100 computers that were not under the direct control of its information technology professionals. This creates a very problematic scenario for college management, since there is little assurance that those computers are secure. To protect college computer systems and data, these computers should be segmented and not allowed access into critical segments.

The Office of the Chancellor recently hired a consultant to develop security guidelines for MnSCU computer networks. The consultant's report provided colleges with guidance on several matters, including network segmentation to improve security. We think segmentation creates a good foundation for strong security, but the biggest challenge will be to implement the recommendations at each college and university. Some colleges, particularly smaller ones, may struggle because it will take significant staff resources to accomplish the recommendations. In some cases, colleges may also need to purchase additional hardware.

Recommendation

- *The Office of the Chancellor should work with individual institutions to devise a plan and timeline to properly segment and secure each college and university network. The plan should address academic computers not under the direct control of campus information technology professionals.*

4. Several colleges do not have controls to protect their networks from insecure computers that connect to them.

Several colleges did not have controls that would prohibit insecure computers from connecting to their wireless networks. In a wireless environment, an increasingly prevalent threat that colleges face is that insecure computers can connect to and compromise college networks. Computers can quickly become insecure if software is not updated or patched in a timely manner, anti-virus software is not running or is out of date, or personal firewalls are not used or are configured improperly. Allowing insecure computers to connect to a college's network can lead to disastrous consequences from viruses, trojans, and worms.

While a college may be able to provide reasonable assurance that its own computers are secure, they have virtually no control over computers, such as laptops, owned by students or others who may connect them to the college's computer networks. As a result, controls are needed to scrutinize computers attempting to access the college's computer networks and quarantine those deemed insecure. By quarantining an insecure computer, a college may prevent a virus or other malicious software from spreading across its computers and other devices on its computer network.

Recommendation

- *MnSCU should develop controls to protect its computer networks from insecure computers.*

5. Several colleges did not adequately monitor their systems and wireless networks for intrusion attempts, unauthorized access points, and known security exploits.

Several colleges did not have effective controls to detect and promptly respond to security-related events, such as unauthorized wireless access attempts made by hackers. Intrusion detection systems are one solution commonly used to detect unauthorized access attempts. Although the best controls are those that prevent inappropriate or malicious events from happening, it is virtually impossible to design flawless preventative controls. Since time is of the essence when under attack, an organization must have defined incident response procedures. Organizations that do not have effective procedures may fail to discover they are insecure until extensive damage is done.

Several colleges also did not have effective controls to prevent or promptly detect unauthorized wireless access points that connect to the college's computer network. Fourteen colleges reported they had no such controls, and an additional nine schools reported weak manual controls. Unauthorized access points are almost always insecure, providing anyone easy access into an organization's computer network. The best monitoring controls are automated and continual and typically rely on existing authorized wireless access points to act as 'sensors' and report when they identify any unknown wireless device. The effectiveness of this control may be limited, however, if colleges do not have wireless access points that provide complete coverage spanning the entire campus. In this case, the college may have to supplement its automated controls with other manual controls such as frequently walking throughout the campus using a computer and software to identify wireless access points. During our on-site visits, we identified two unauthorized access points that college technology staff were not aware of. In both cases, the wireless access points were installed by faculty members and allowed anyone open access to the college's computer networks.

Finally, most campuses did not run vulnerability assessment software to search for commonly known security weaknesses. Vulnerability scanners are special software packages that probe systems to find exploitable security weaknesses. An example of one such weakness is a commercial product flaw that causes a computer program to perform an unauthorized operation. Since hackers take advantage of these exploits, it is important to find and correct them as quickly as possible. Vendors that provide vulnerability scanners update their products frequently to include the most recent security exploits. We think that the Office of the Chancellor should make ongoing vulnerability assessments and reporting a requirement for all of its colleges and universities.

Recommendation

- *MnSCU should develop effective monitoring controls to detect and respond to security-related events in a timely manner, including:*

  -- *procedures and tools, such as intrusion detection systems, to identify unauthorized access attempts;*

  -- *methods to prevent and promptly detect unauthorized wireless access points connected to the college's networks; and*

  -- *periodic scans of its networks and computers to search for security weaknesses commonly exploited by hackers.*

OFFICE OF THE CHANCELLOR
500 WELLS FARGO PLACE
EAST SEVENTH STREET
ST. PAUL, MN 55101-4946
PH 651.296.8012
FX 651.297.5550
www.mnscu.edu

Minnesota
STATE COLLEGES
& UNIVERSITIES

September 2, 2005

James R. Nobles
Legislative Auditor
Office of the Legislative Auditor
Centennial Building 658 Cedar Street
St. Paul MN 55155

Dear Mr. Nobles,

The purpose of this letter is to respond to the Wireless Network Security Audit that your office recently completed. We jointly decided to focus this audit on wireless networks in order to assess wireless security across the system. We appreciate the efforts of the audit staff and their interest in working with us to improve our technical security environment.

We agree with the wireless security audit findings and recommendations that you suggest in the report. We also feel that these recommendations are timely given the current technology environment and the desire students, faculty and staff have for the flexibility and portability of this technology. We do want to point out that as issues were discovered during the audit, we did take immediate action to improve wireless security and in some cases this included turning individual campus wireless access points off until the networks were either secured or, at a minimum, until access was limited to the Internet. As you are well aware, wireless access is an evolving technology and until recently there has been a lack of industry standards and tools for securing these types of networks. For example, the 802.11i standard for wireless security was ratified in June of 2004; many devices still used at MnSCU predate this standard.

This audit and the actions we have taken are a part of our ongoing efforts to work with individual campuses to implement a comprehensive information security program. Wireless security is one component of information security, and is one of a number of security initiatives currently underway to address system wide security concerns. A cross-functional executive level steering committee was established in 2004 to address system wide security strategies, and is directing the development of a comprehensive, multi-year security program that includes Incident Response, Security Management, Security Practices, Risk Management, Security Technology, and Compliance Monitoring. Security awareness and training are also a part of this program.

We will continue to work with individual colleges and universities to provide an acceptable level of security over information technology resources and data. This effort will include wireless security as well as other system wide security concerns. We look forward to ongoing communication with your staff as we work to resolve the issues raised in your audit findings.

Our response to address the specific audit findings in your report follows.

Sincerely,

/s/ Ken Niemi

Ken Niemi
Vice Chancellor for Information
Technology and CIO
Minnesota State Colleges and Universities

Finding 1: MnSCU did not adequately plan and secure many of its wireless networks.

Historically, each institution has been responsible for the deployment, operations and security of technology located on its campuses. The role of the Office of the Chancellor has been to provide centralized shared data and network services. In response to student and faculty demands for wireless capabilities, campuses implemented wireless technology—an extension of the local area network—using the generally accepted security standards capabilities available at the time of implementation.

The Office of the Chancellor is developing a comprehensive security program which includes procedures and guidelines that address virus protection and patch management, awareness and training, data protection, and access management as well as wireless security. Each campus will be required to establish local procedures to address and manage security concerns on an ongoing basis.

Finding 2: Controls to authenticate users and encrypt wireless data transmissions were weak or nonexistent at several campuses.

When wireless systems were first developed, the only security mechanism available (called WEP) was designed to provide roughly the same level of security as wired networks. Some of the flaws with this mechanism became apparent only after deployment worldwide, and it became clear to the IT industry that this initial security standard was inadequate, and needed replacement. Although the 802.11i standard for wireless security was finally ratified in June of 2004, many hardware devices still used at MnSCU predate this standard, which has required us to work with individual campuses to implement short term alternate security approaches until all the older equipment can be replaced.

We have already taken strong action to mandate that all wireless access to private data or to the servers and networks on which private data resides will be authenticated and encrypted. Several campuses have disabled wireless access until these standards have been met. Each campus will be required to establish local procedures to ensure compliance.

We have provided specific assistance to campuses that have been identified as needing assistance in implementing this mandate. Acceptable methods of encryption and authentication appropriate to accessing private data have been developed and communicated to campuses, and we are providing ongoing technical support and direction to campuses.

Finding 3: Many colleges did not functionally segment their wired and wireless networks to better protect computer systems and data.

The architecture, design and delivery of local area networks are the responsibility of each campus. Each institution has designed its own network, which may or may not have included segmentation. Campuses may have chosen not to include network segmentation due to perceived need, or due to the lack of available technical expertise or financial resources.

In an effort to provide tools to support better network security and performance, the Office of the Chancellor ITS division developed formal network architecture guidelines, including specific guidelines regarding network segmentation. These guidelines were communicated to campus CIO's and technical staff in April, 2005.

Strategies and implementation for efficient network segmentation system wide are being developed and a plan will be completed by the end of this year. Each campus will be required to develop a compliant network.

Finding 4: Several colleges do not have controls to protect their networks from insecure computers that connect to them.

The technology for assessing the security of devices connected to the network may be referred to as security policy enforcement. This technology has only recently become available as a commercial product and still requires significant financial investment and staff resources to implement and manage.

A specific strategy for protecting networks from insecure computers attaching to the network will be developed and an implementation plan established by the first quarter of 2006. Each campus will be required to develop a compliant network.

Finding 5: Several colleges did not adequately monitor their systems and wireless networks for intrusion attempts, unauthorized access points, and known security exploits.

The Office of the Chancellor ITS division is establishing requirements for routine security assessments, including wireless networks. This ongoing assessment process is scheduled to be documented and implemented by the end of this year. Each campus will be required to develop monitoring procedures.