NORTH DAKOTA LEGISLATIVE MANAGEMENT

Minutes of the

LEGISLATIVE AUDIT AND FISCAL REVIEW COMMITTEE JOINT MEETING WITH INFORMATION TECHNOLOGY COMMITTEE

Thursday, January 29, 2015
Roughrider Room, State Capitol
Bismarck, North Dakota

Representative Gary Kreidt, Chairman, Legislative Audit and Fiscal Review Committee, called the meeting to order at 3:30 p.m. along with Representative Robin Weisz, Chairman, Information Technology Committee.

Legislative Audit and Fiscal Review Committee members present: Representatives Gary Kreidt, Jeff Delzer, Ron Guggisberg, Patrick R. Hatlestad, Jerry Kelsh, Keith Kempenich, Andrew G. Maragos, Bob Martinson, Corey Mock, Chet Pollert, Dan Ruby, Jim Schmidt, Robert J. Skarphol, Wayne Trottier; Senator Judy Lee

Legislative Audit and Fiscal Review Committee members absent: Representatives Wesley R. Belter, Marvin E. Nelson; Senators Ralph Kilzer, David O'Connell, Terry M. Wanzek

Information Technology Committee members present: Representatives Robin Weisz, Corey Mock, Mark S. Owens, Roscoe Streyle, Blair Thoreson, Nathan Toman; Senators Joe Miller, Larry J. Robinson; Citizen Member Mike Ressler

Information Technology Committee members absent: Senators Randall A. Burckhard, Richard Marcellais, Donald Schaible

Others present: See Appendix A

NORTH DAKOTA UNIVERSITY SYSTEM'S TECHNOLOGY SECURITY AUDIT AND VULNERABILITY ASSESSMENT

At the request of Chairman Kreidt, Mr. Donald LaFleur, State Auditor's office, presented information regarding the audit report for the North Dakota University System's technology security audit and vulnerability assessment. Mr. LaFleur said the Legislative Assembly appropriated $100,000 during the 2013-15 biennium to conduct a technology security audit and vulnerability assessment of the University System.

At the request of Chairman Kreidt, Mr. Erik Wallace, Principal Architect, Enterprise Security and Protection, TeleCommunication Systems, representing L.R. Kimball, presented information (Appendix B) regarding the audit report for the University System's technology security audit and vulnerability assessment. Mr. Wallace said the colleges and universities included as part of the audit include Bismarck State College, Dakota College at Bottineau, Dickinson State University, Lake Region State College, Mayville State University, Minot State University, North Dakota State College of Science, North Dakota State University, University of North Dakota, Valley City State University, Williston State College, and University System offices in Fargo, Bismarck, and Grand Forks. He said the University System provides information technology resources to more than 47,000 students and 11,000 faculty and staff members on a daily basis. He said information technology security is essential to help campuses comply with both state and federal laws and regulations, which include protecting sensitive information including education records, personally identifiable information, credit card data, and financial aid records.

Mr. Wallace said 12 findings were considered critical or high based on the common vulnerability scoring system. The schedule below summarizes the 12 findings and related recommendations.

Findings	Recommendation
Unsupported operating systems	• Move from unsupported versions of operating systems to supported versions. • Unsupported systems which may not be changed or if the cost would be too high should provide depth strategies to mitigate risk to the system, which includes shutdown of ports and applications not required, limit of access to the machine, and segregating the machine if possible. • If an unsupported system is required, a waiver should be provided and a defense strategy outlined for protection of the machine and the attached networks.

Findings	Recommendation
Missing software patch or required upgrade	• Ensure each campus runs vulnerability assessment software to determine required patches and to provide prioritization associated with patching. • Apply all applicable hardware, software, and application patches within a reasonable time period based on the severity of the issue. • Ensure a patch management program is in place which is tracking systems affected and timeline to resolution. • Evaluate commercial available patch management products to expedite patching and updates.
Easily guessed or default credentials	• Create a password policy which includes password management-related requirements. • Protect passwords from attacks which capture passwords, which includes the use of HTTPS for web password submission, or the use of multi-factor authentication. • Configure password mechanisms to reduce successful password guessing. • Determine requirements for password expiration based on security and usability. • Ensure systems do not include default or "out-of-box" user and password settings.
Unsupported web server	• Evaluate the need for the web server. • Upgrade the web server to a supported release. • If the web server is no longer supported, provide a web server which is supported and will meet the requirements of the application.
Well-known internal network assessment exploits	• Patch all systems found with internal network exploits with an appropriate vendor-supported patch. Common internal network exploits include "Heartbleed," "Shellshock," and the "Intelligent Platform Management Interface Cipher Suite Zero."
Publicly accessible web applications	• Systems with web applications or appliances should be disabled if not required and should not be publicly accessible. • Ensure systems are not setup with default user or administrator credentials.
Firewall and network address translation	• Install and configure a routing firewall to provide network address translation to networks so they are not publicly facing. • Implement a multi-faceted security effort.
Cross-site scripting	• Input should be validated as strictly as possible on arrival and input which fails the validation should be rejected, not sanitized. • User input should be HTML-encoded at any point when copied into application responses.
Clear text password	• Replace HTML (HTTP) web services with an HTTPS version when data must be protected. • Replace unsecured services with secured Secure Shell service. • Add training for user awareness.
Session token in URL	• Applications should use alternative mechanisms for transmitting session tokens.
SQL injection	• Use queries with parameters for all database access.
Serialized object in HTTP message	• Do not pass serialized objects into request parameters.

In response to a question from Representative Streyle, Mr. Wallace said input would be needed from the University System including all the campuses to determine a best approach method for consolidation of operational security. In addition, he said, the University System along with the campuses could determine common policies and procedures for all campuses to improve information technology security.

In response to a question from Representative Skarphol, Mr. Wallace said most of the findings and recommendations have been addressed. He said many of the corrections were made onsite during the audit.

In response to a question from Representative Streyle, Mr. Wallace said external security testing should be done on an annual basis.

COMMENTS BY UNIVERSITY SYSTEM REPRESENTATIVES

At the request of Chairman Kreidt, Dr. Lisa Feldner, Vice Chancellor for Information Technology and Research, North Dakota University System, provided comments regarding the University System's technology security audit and vulnerability assessment. Dr. Feldner said the University System is reviewing and rewriting existing policies and adding new policies. She said existing policies were not up-to-date. She said training sponsored by the State Auditor's office is being provided for staff. She said the Core Technology Services staff is required to have security training and similar training for all campus staff would be beneficial.

In response to a question from Representative Streyle, Dr. Feldner said the University System is currently accessing common security policies and procedures. She said policies and procedures are not common across all campuses, which has been difficult to enforce.

Chairman Weisz adjourned the meeting of the Information Technology Committee subject to the call of the chair at 4:30 p.m.

PERFORMANCE AUDIT UPDATE - USE OF TUITION WAIVERS AND STUDENT STIPENDS AT THE UNIVERSITY SYSTEM INSTITUTIONS

At the request of Chairman Kreidt, Mr. Jason Wahl, State Auditor's office, presented information regarding an update on the status of the performance audit on the use of tuition waivers and student stipends at University System institutions. Mr. Wahl said various inconsistencies at the campuses has caused additional work for the State Auditor's office which has resulted in delays with the audit process. He said the audit will take longer than anticipated. He said the State Auditor's office anticipates completing the audit report before the end of the 2015 legislative session. If additional delays prevent the completion of the final audit prior to the end of this session, he said, a preliminary report will be provided. He said a final report would be provided when the audit is complete.

In response to a question from Representative Hatlestad, Mr. Wahl said the performance audit will allow the State Auditor's office to provide the committee with additional information on tuition waivers.

Chairman Kreidt directed the State Auditor's office to inform the institutions included in the audit that their assistance is crucial for the timely completion of the audit prior to the close of the 2015 legislative session.

PROPOSED PERFORMANCE AUDIT OF SELECTED UNIVERSITIES' DEVELOPMENT FOUNDATIONS

Representative Skarphol proposed that the State Auditor's office conduct a performance audit of certain universities' development foundations. He said the performance audit is intended to assist in the rebuilding of a positive relationship between the Legislative Assembly and the University System.

Senator Lee questioned the need for a performance audit of the universities' development foundations at this time.

Representative Skarphol said the development foundations are valuable to the universities. He said a performance audit will provide an opportunity to document the value of the development foundations to the universities.

In response to a question from Senator Lee, Mr. Wahl said he anticipates the performance audit could begin in June or July 2015 unless the State Auditor's office is required by law to complete other performance audits.

Mr. Wahl asked for clarification on the development foundations that are to be included in the audit. Representative Skarphol said the audit should include the largest blended component unit that provides both academic and ancillary contributions in support of the University of North Dakota, North Dakota State University, and Dickinson State University.

It was moved by Representative Skarphol, seconded by Representative Trottier, and carried on a roll call vote that, pursuant to North Dakota Century Code Section 54-10-01, the State Auditor conduct performance audits of the development foundations at the University of North Dakota, North Dakota State University, and Dickinson State University for fiscal years 2012, 2013, and 2014. As part of the Dickinson State University Foundation audit, the State Auditor may, to the extent possible, review information available from recent receivership and audit activities. The audits are to include the largest blended component unit at each university that provides both academic and ancillary contributions in support of the university. Representatives Kreidt, Hatlestad, Kempenich, Maragos, Martinson, Nelson, Pollert, Ruby, Schmidt, Skarphol, and Trottier voted "aye." Representatives Guggisberg, Kelsh, and Mock and Senator Lee voted "nay."

COMMITTEE DISCUSSION AND STAFF DIRECTIVES

It was moved by Representative Maragos, seconded by Representative Skarphol, and carried on a roll call vote that, pursuant to Section 54-35-02.2, the committee accept the performance audit report of the University System's technology security audit and vulnerability assessment. Representatives Kreidt, Guggisberg, Hatlestad, Kelsh, Kempenich, Maragos, Martinson, Mock, Nelson, Pollert, Ruby, Schmidt, Skarphol, and Trottier and Senator Lee voted "aye." No negative votes were cast.

Chairman Kreidt said he anticipates the next Legislative Audit and Fiscal Review Committee meeting to be at the end of the 2015 legislative session or shortly after the session is adjourned.

No further business appearing, Chairman Kreidt adjourned the Legislative Audit and Fiscal Review Committee meeting at 5:00 p.m.

____

Michael C. Johnson
Fiscal Analyst

____

Allen H. Knudson
Legislative Budget Analyst and Auditor

ATTACH:2