Legislative Council
600 East Boulevard Avenue, Bismarck, ND 58505

North Dakota Legislative Management
Meeting Minutes
23.5011.03000

INFORMATION TECHNOLOGY COMMITTEE

Thursday, March 4, 2021
Brynhild Haugland Room, State Capitol
Bismarck, North Dakota

Representative Corey Mock, Chairman, called the meeting to order at 8:00 a.m.

Members present: Representatives Corey Mock, Glenn Bosch, Shannon Roers Jones, Nathan Toman, Don Vigesaa; Senators Kyle Davison, Joan Heckaman, Merrill Piepkorn, Shawn Vedaa; Citizen Member Shawn Riley

Members absent: Representative Robin Weisz; Senator Terry M. Wanzek

Others present: Allen H. Knudson, Legislative Council, Bismarck
See Appendix A for additional persons present.

It was moved by Senator Davison, seconded by Representative Vigesaa, and carried on a voice vote that the minutes of the September 30, 2020, meeting be approved as distributed.

INFORMATION TECHNOLOGY SECURITY AUDIT

Mr. Joshua C. Gallion, State Auditor, presented information (Appendix B) regarding the information security audit of the Information Technology Department (ITD) and North Dakota University System. He said his office contracted with a third party vendor, Secure Yeti, to conduct the audit.

Mr. Casey Bourbonnais, Lead Technical Tester, Secure Yeti, presented information (Appendix C) regarding the information security audit of ITD and the University System. He said ITD, the University System's Core Technology Services, and the 11 higher education institutions were included in the audit. He said 6 of the 13 physical locations were tested during the audit, including ITD, Core Technology Services, University of North Dakota, Valley City State University, Bismarck State College, and Dickinson State University. He said the audit of ITD included testing at the Capitol.

Mr. Bourbonnais said the purpose of the audit was to assess the security of information technology in state government and identify potential vulnerabilities in the state network, systems, and applications. He said the audit revealed 128 vulnerabilities, of which 5 were considered critical risk, 57 were high risk, 33 were medium risk, and 33 were low risk. He said of the 95 critical, high, and medium risk vulnerabilities, 10 key findings were identified and related to the following:

- Intrusion monitoring, detection, and response;
- Insecure legacy protocols;
- Insecure password policies;
- Critical University System data center infrastructure is not adequately protected by physical barriers;
- Misconfigured wireless networks;
- Unauthenticated simple mail transfer protocol (email) relay, remote shell, and phishing;
- Externally exposed network resources;
- Patching and configuration management; and
- The need to display an acceptable use policy for the statewide technology access for government and education network (STAGEnet) when users access a website or system on STAGEnet.

Mr. Bourbonnais said the audit consisted of a phishing campaign in which 698 phishing emails were sent to non-higher education email addresses, of which 76, or 11 percent, successfully phished users into clicking risky links or content. He said 730 phishing emails were sent to higher education email addresses, of which 199, or 27 percent, successfully phished users into clicking risky links or content. He said ITD and the University System responded quickly to the phishing emails, as ITD responded within 3 minutes and the University System responded within 5 minutes of the first phishing emails sent. He said the phishing campaign at the University System was conducted for a longer period of time than the ITD phishing campaign.

Mr. Bourbonnais said ITD and the University System were aware of the vulnerabilities identified in the audit. He said ITD and the University System indicated the key findings in the audit report will not require significant network, system, or process changes to mitigate potential risks and vulnerabilities.

In response to a question from Mr. Riley, Mr. Bourbonnais said ITD has the resources available to respond to the risks identified in the audit, but there are communication processes and delays between ITD and other agencies that have prevented timely responses to those risks. He said the University System does not have the resources to respond to the risks identified in the audit.

In response to a question from Chairman Mock, Mr. Bourbonnais said without proper physical barriers to protect critical University System data center infrastructure, it is possible the data center may not be considered a Tier III data center, which is a data center with redundant and dual-powered servers, storage, and network equipment.

No further business appearing, Chairman Mock adjourned the meeting at 8:55 a.m.

____

Levi Kinnischtzke
Senior Fiscal Analyst

ATTACH:3