NDLC
NORTH DAKOTA LEGISLATIVE COUNCIL
1945 75 2020
Years

North Dakota Legislative Management
Meeting Minutes
21.5124.03000

INFORMATION TECHNOLOGY COMMITTEE

Thursday, June 4, 2020

Representative Corey Mock, Chairman, called the meeting to order at 9:30 a.m.

Members present: Representatives Corey Mock, Glenn Bosch, Shannon Roers Jones, Nathan Toman, Don Vigesaa; Senators Kyle Davison, Merrill Piepkorn, Larry J. Robinson, Shawn Vedaa, Terry M. Wanzek; Citizen Member Shawn Riley

Member absent: Representative Robin Weisz

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

It was moved by Senator Robinson, seconded by Representative Vigesaa, and carried on a voice vote that the minutes of the October 24, 2019, meeting be approved as distributed.

CYBERSECURITY

Cybersecurity Defense Ability

Mr. Kevin Ford, Chief Information Security Officer, Information Technology Department, presented information (Appendix B) regarding North Dakota's cybersecurity status, including the ability of the state to defend against cybersecurity attacks. He said the Information Technology Department (ITD) has conducted an assessment of the cybersecurity maturity and risk of state agencies and political subdivisions. He said preliminary results indicate many cities, counties, and K-12 school districts have critical cybersecurity risk, meaning those entities likely will experience unauthorized access to information technology (IT) systems and networks and likely will encounter successful ransomware and malware attacks. He said counties likely will recover successfully from cybersecurity attacks, while cities and school districts may have difficulties recovering from cybersecurity attacks. He said a successful recovery is considered re-establishing services quickly after a cybersecurity attack but the entity may experience lost data or other damages due to malware or ransomware used in the cybersecurity attack.

Mr. Ford said the judicial and legislative branches are considered to have high cybersecurity risk, meaning those branches likely will experience unauthorized access to IT systems and networks and may encounter successful ransomware and malware attacks. He said the judicial and legislative branches are very likely to recover from cybersecurity attacks.

Mr. Ford said ITD and other executive branch agencies that have unified IT resources are considered to have low cybersecurity risk, meaning those agencies may experience unauthorized access to IT systems and networks but likely will not encounter successful malware or ransomware attacks. He said these agencies are very likely to recover from cybersecurity attacks.

Mr. Ford said data from the assessment of the North Dakota University System's cybersecurity maturity and risk is being collected and is not available at this time.

Cybersecurity Insurance

Mr. Ford presented information (Appendix C) regarding state and political subdivision cybersecurity insurance policies.

Mr. Ford said the state has a cybersecurity insurance policy that insures all state government agencies in the event of a cybersecurity or ransomware attack but the policy does not cover counties, cities, school districts, or other political subdivisions. He said the policy includes a $250,000 deductible and provides coverage of up to $5 million of damages in the event of a successful cybersecurity attack. He said damages the policy will cover include operational costs to reconnect systems and services, notifying impacted individuals or agencies of the attack, and the cost of affected individuals or agencies enrolling in credit monitoring services. He said the policy will not pay for the loss of data or value.

Mr. Ford said the state cybersecurity policy provides for an additional $5 million of coverage if the state is held liable if other entities that rely on the statewide technology access for government and education network (STAGEnet) experience a successful cybersecurity attack.

Mr. Ford said political subdivisions are insured through the North Dakota Insurance Reserve Fund, which includes no deductible and will cover costs associated with an information breach, but will not cover damages from cybersecurity events.

In response to a question from Chairman Mock, Mr. Ford said the state's cybersecurity insurance policy is written and held by a private insurance company.

COVID-19 Pandemic

Mr. Ford presented information (Appendix D) regarding cybersecurity trends resulting from the Coronavirus (COVID-19) pandemic. He said the COVID-19 pandemic has increased cybersecurity attacks worldwide. He said the state also has experienced increases in cybersecurity attacks primarily due to the increase in state employees working from home using networks not designed to protect state government information.

In response to a question from Representative Bosch, Mr. Ford said cybersecurity attacks have continued to increase since April 15, 2020, but at a slower rate than experienced from March 8, 2020, to April 15, 2020. He said the number of unaddressed security incidents has increased from approximately 3,800 on March 8, 2020, to approximately 8,000 at the end of May 2020.

Mr. Ford said the amount of state data on the dark web has increased 2,087 percent in 2020 and there are more than 17,500 state data records on the dark web. The dark web is a decentralized network of Internet sites not accessible to the general public which often provides access to illegal activities and stolen data. He said the dark web contains approximately 13,284 North Dakota K-12 data records, which is an increase of an average of 1,205 percent in 2020 compared to 2019. He said the dark web contains approximately 685 North Dakota county data records, which is an increase of an average of 400 percent in 2020 compared to 2019. He said the dark web contains approximately 735 North Dakota city data records, which is an increase of an average of 1,200 percent in 2020 compared to 2019.

In response to a question from Representative Toman, Mr. Ford said a portion of the state and political subdivision data on the dark web may have been obtained prior to the COVID-19 pandemic, but is now being used due to significant increases in the value of stolen data on the dark web.

In response to a question from Representative Vigesaa, Mr. Shawn Riley, Chief Information Officer, Information Technology Department, said health care organizations have been the most targeted entities during the COVID-19 pandemic, as well as educational and law enforcement organizations.

Network Cybersecurity Requirements

Mr. Ford presented information (Appendix E) regarding cybersecurity and minimum security requirements for state and political subdivisions using STAGEnet. He said ITD is establishing standards for government and educational entities to access STAGEnet, including default blocking of macros, removing unnecessary administrative rights on user devices, using multifactor authentication, ensuring proper data backups, using artificial intelligence to reduce ransomware risk, and requiring entities to report security events to ITD. He said ITD is forming a cybersecurity steering committee for state agencies and political subdivisions, which will include participation from the University System, City of Fargo, and representatives of other cities, counties, school districts, the legislative and judicial branches, and tribal entities.

In response to a question from Chairman Mock, Mr. Ford said ITD has strategic cybersecurity authority for political subdivisions but no authority to enforce compliance with ITD's cybersecurity requirements. He said ITD can provide guidance and documentation to political subdivisions regarding cybersecurity minimum standards and best practices for access to STAGEnet, but because ITD does not have the authority to enforce the standards and practices or monitor compliance with ITD guidance, political subdivisions may choose whether the requirements will be implemented at the local level. He said ITD does not provide guidance to political subdivisions regarding physical access controls to IT equipment and systems, but that is an important component of data security.

In response to a question from Chairman Mock, Mr. Ford said ITD provides cybersecurity awareness training for political subdivisions and tests political subdivision exposure to phishing attacks.

In response to a question from Representative Bosch, Mr. Ford said it is unknown whether new legislation is necessary regarding political subdivision use of STAGEnet but clarification may be needed regarding statutes related to ITD's authority to enforce STAGEnet minimum requirements.

In response to a question from Representative Bosch, Mr. Ford said some political subdivisions welcome the cybersecurity advice of ITD while other political subdivisions do not. He said ITD has concerns regarding small political subdivisions that do not have dedicated IT or cybersecurity personnel.

In response to a question from Representative Bosch, Mr. Riley said other states do not have a comprehensive state network similar to STAGEnet. He said other states have requested political subdivisions coordinate cybersecurity initiatives at the local government level, independent of state government. He said these approaches have not been successful.

COVID-19 RELIEF FUNDING

Cybersecurity

Mr. Ford presented information (Appendix F) regarding planned uses of $17 million of federal COVID-19 relief funding approved for cybersecurity, including third-party cybersecurity contract information, ongoing costs of new cybersecurity initiatives after COVID-19 relief funding is spent, and how new cybersecurity initiatives will affect state agency budgets.

Mr. Ford said of the $17 million approved for cybersecurity from the state's allocation from the federal Coronavirus Relief Fund, 61 percent will be used to purchase cybersecurity tools, 28 percent will be to provide cybersecurity services, 9 percent will be for staff training and education, and 2 percent will be for additional cybersecurity contract work. He said after the federal cybersecurity funding is used, there will be an ongoing operational cost of approximately 15 percent, or $2.6 million, to maintain the new cybersecurity initiatives.

In response to a question from Chairman Mock, Mr. Ford said ITD's 2021-23 biennium budget request related to cybersecurity had not been developed prior to requesting funding from the state's allocation from the Coronavirus Relief Fund. He said it is possible a portion of the funding requested from the state's allocation from the Coronavirus Relief Fund may have been requested during the 2019 legislative session.

In response to a question from Chairman Mock, Mr. Riley said it is unknown whether ITD will request a general fund appropriation for the $2.6 million of ongoing expenditures for cybersecurity or if the funding will be paid by state agencies when billed by ITD for services provided.

In response to a question from Senator Robinson, Mr. Riley said ITD will provide information regarding the department's 2021-23 biennium budget request at a future committee meeting.

In response to a question from Senator Robinson, Mr. Riley said salaries for state cybersecurity professionals are not competitive with salaries offered to cybersecurity professionals in the private sector. He said ITD employs personnel in nine states to help recruitment of IT personnel by offering remote working and flexible work schedules.

Mr. Riley said of the $17 million allocated for cybersecurity, $5.6 million is for cybersecurity tools and software, $3.5 million is for professional services for the deployment of the tools and software, $3.5 million is for staff augmentation for cyber operations, $2 million is for third-party incident response to fraud and other pandemic-related cybersecurity issues, $1.6 million is for cybersecurity training and education, and $800,000 is for multifactor authentication costs to eliminate simple phishing attacks.

In response to a question from Representative Bosch, Mr. Riley said ITD has worked closely with the Secretary of State regarding a request for $3 million of federal funding to address cybersecurity concerns related to elections.

Telework

Mr. Riley presented information (Appendix G) regarding planned uses of $23.87 million of federal COVID-19 relief funding approved for telework, including telework equipment purchased. He said ITD moved more than 7,000 state employees to telework in 2 days in an effort to reduce the risk of COVID-19 infection but many state employees do not have adequate IT equipment to effectively work remotely. He said ITD assisted all state government agencies, including higher education, as well as many political subdivisions to ensure state employees were able to work remotely. He said ITD redirected 40 employees working in other IT areas to assist state employees experiencing IT issues while working remotely. He said ITD expanded virtual private network capabilities to improve remote connection to STAGEnet for state employees. He said while some agencies are beginning to bring a portion of staff back to office locations, other agencies are continuing to work remotely due to lack of adequate space for employees to social distance in an office environment.

Mr. Riley said of the $23.87 million allocated for telework, $10.52 million is for the cost of purchasing telework equipment, such as computers, conference room equipment, network and server equipment, and hardware for system administration. He said the remaining $13.35 million will be spent on researching ways for state government to work differently as a result of the pandemic ($4.5 million), professional services for enterprise service management software ($4 million), the cost of software licenses and training for remote support tools ($3.2 million), and Microsoft Office 365 licensing expansion to enable telework voice capabilities, improve document management, and enhance data analytics ($1.65 million).

In response to a question from Representative Toman, Mr. Riley said state systems and data can be secure while employees work remotely, but the state structure was not designed for remote working. He said the funding provided from the state's allocation from the Coronavirus Relief Fund will help establish a secure telework structure for remote working.

In response to a question from Chairman Mock, Mr. Riley said applications developed by ITD related to the COVID-19 pandemic and contact tracing have been shared with other states at no cost.

Digital Government

Mr. Riley presented information (Appendix H) regarding planned uses of $26.75 million of federal COVID-19 relief funding approved for digital government initiatives, including services to be offered by a digital government enterprise call center, how the funding will be used to automate manual processes for state agencies, and information regarding the digital government assessment. He said ITD is deploying software throughout the state while continuing unification, strategic redesign, and COVID-19 initiatives. He said ITD will use temporary resources, including contracting with vendors, to complete as much of the initiatives as possible.

Mr. Riley said of the $26.75 million of federal COVID-19 relief funding approved for digital government initiatives, $11 million will be for automation processes to quickly build software to improve citizen experience, improve business workflow, and provide efficiencies. He said $6 million is for a COVID-19 unified data platform to reduce or eliminate manual data collection, primarily in State Department of Health systems. He said $5.25 million is for resources to establish an enterprise call center to replace individual agency-specific call centers. He said $4.5 million is for digital services to replace paper and in-person interactions.

Chairman Mock and Senator Robinson expressed concern regarding the ongoing use of mainframes by state agencies and encouraged ITD to develop a plan to transition state agency programs off of mainframe technology.

Mr. Riley said ITD is working to remove the two largest agencies, Department of Human Services and Department of Transportation, off the ITD mainframe.

REPORT FROM THE CHIEF INFORMATION OFFICER

Annual Report

Mr. Riley presented (Appendix I) ITD's annual report (Appendix J) pursuant to North Dakota Century Code Section 54-59-19. He said ITD accomplishments during fiscal year 2019 included the IT unification of six state agencies; increases in cybersecurity policy, personnel, and tools; increased usage of the North Dakota Health Information Network (NDHIN); the K-20W Initiative, which is a workforce cybersecurity education initiative; and internal service delivery, automation, and cross-agency collaboration.

Mr. Riley said ITD billed state agencies $64.9 million for IT services during fiscal year 2019, including amounts billed to the Department of Human Services (41 percent), Department of Public Instruction (9 percent), Department of Transportation (7 percent), and Workforce Safety and Insurance (4 percent). Of the IT services billed to state agencies, he said, 39 percent was for computer hosting, 27 percent was for software development, 17 percent was for network services, 11 percent was billed directly to state agencies for work performed, 5 percent was for telephone services, and 1 percent was for other services. He said ITD's 12-month rolling period average turnover rate ranged from a low of 6.46 percent to a high of 9.61 percent during fiscal year 2019.

Distributed Ledger Technology Report

Mr. Riley presented a report (Appendix K) regarding the implementation of distributed ledger technologies pursuant to Section 54-59-02.2. He said ITD has identified multiple potential uses of blockchain technology in state government. He said ITD has built a proof of concept application that allows for citizen data to be verified using blockchain in a mobile application. He said the mobile application could be used for licensing, such as driver's licenses or fishing licenses, and human services programs such as the supplemental nutrition assistance program.

LARGE PROJECT REPORTING

Mr. Riley presented (Appendix L) the quarterly summary status report on large information technology projects for the 4th quarter of 2019 (Appendix M) and the 1st quarter of 2020 (Appendix N) and distributed the following startup and closeout reports (Appendix O) completed from October 2019 through May 2020:

Startup Reports

- Department of Human Services - Budget planning and forecasting system
- Department of Human Services - Eligibility system - Release 3
- Department of Transportation - Driver's license project
- ITD - Palo Alto toolset implementation
- ITD - NDHIN - Phase 2
- Workforce Safety and Insurance - MyWSI enhancement - Release 3
- Department of Environmental Quality - Environmental regulatory software system

Closeout Reports

- Department of Public Instruction - ND Foods 4.0
- ITD - NDHIN - Phase 1
- Workforce Safety and Insurance - MyWSI enhancement - Releases 1 and 2
- Workforce Safety and Insurance - Claims and policy system replacement - Release 6

Other Project Reports

- Secretary of State - File 2.0

Mr. Riley said all large projects are within 20 percent of budget and scheduled completion plans, with exception of the Job Service North Dakota unemployment insurance modernization project and Phase 1 of the Secretary of State's File 2.0 project. He said the unemployment insurance modernization project has been delayed because a consortium with Idaho and Vermont to implement a new unemployment insurance system for all states has been dissolved. He said ITD and Job Service North Dakota are working on a strategy to modernize the unemployment insurance system.

Mr. Riley said no large projects were canceled as a result of the COVID-19 pandemic. He said 12 of the 29 large projects were given new budget or schedule baselines. He said the majority of contract work for large projects continued from remote locations, with the exception of the statewide interoperable radio network project.

OTHER

Mr. Riley distributed information regarding IT unification and reinvention (Appendix P), automation (Appendix Q), coordination of services with political subdivisions and higher education pursuant to Section 54-59-12 (Appendix R), business continuity preparedness (Appendix S), and health information technology (Appendix T).

No further business appearing, Chairman Mock adjourned the meeting at 12:20 p.m.

Levi Kinnischtzke
Fiscal Analyst

ATTACH:20