North Dakota Legislative Council
Prepared for the Information Technology Committee
LC# 23.9046.01000
August 2021

STATE AND LOCAL GOVERNMENT CYBERSECURITY - BACKGROUND MEMORANDUM

Section 15 of Senate Bill No. 2021 (2021) (appendix) provides for a study during the 2021-22 interim regarding costs incurred by the Information Technology Department (ITD) to deliver core technology services and cybersecurity services to state agencies and political subdivisions. The study must consider the feasibility and desirability of political subdivisions paying their share of the cost of these services. The Legislative Management has assigned the responsibility for this study to the Information Technology Committee.

INFORMATION TECHNOLOGY SERVICES

The Information Technology Department provides information technology (IT) services to state agencies and political subdivisions, including computer hosting, software development, direct bill-back services, network services, and telephone services. During fiscal year 2020, ITD received $75.5 million in revenue from state agencies and political subdivisions, of which 49 percent was for computer hosting services, 22 percent was for software development services, 14 percent was for network services, 9 percent was for direct bill-back services, 5 percent was for telephone services, and 1 percent was for other services. Revenue received by ITD was primarily from the Department of Human Services (42 percent), Department of Transportation (13 percent), and Department of Public Instruction (7 percent).

CYBERSECURITY FUNDING

The 2021 Legislative Assembly added $19,486,225 for ITD cybersecurity initiatives for the 2021-23 biennium, of which $6,500,000 is considered one-time funding from the federal Coronavirus Relief Fund and $12,986,225 is considered ongoing funding from the general fund and ITD operating service fund. The Legislative Assembly also authorized the addition of 29 full-time equivalent (FTE) cybersecurity positions, 17 of which relate to state cybersecurity and 12 FTE to local cybersecurity. Of the total, 23 FTE cybersecurity positions are funded from the general fund and 6 of the local FTE cybersecurity positions are funded from the ITD operating fund. Additional cybersecurity funding approved for the 2021-23 biennium is as follows:

	FTE	General Fund	Special Funds	Federal Funds	Total
Salaries and wages	29.00	$5,840,142	$1,523,515	$0	$7,363,657
Operating expenses		5,251,534	240,000	6,500,000	11,991,534
Capital assets		131,034	0	0	131,034
Total	29.00	$11,222,710	$1,763,515	$6,500,000	$19,486,225

In addition to funding added by the 2021 Legislative Assembly, ITD's 2021-23 biennium base budget included $5.8 million for cybersecurity salaries and wages, of which $2.3 million is from the general fund and $3.5 million is from special funds, for 20 FTE cybersecurity positions and 3 temporary positions. A total of 49 FTE cybersecurity positions are authorized for the 2021-23 biennium.

The 2019 Legislative Assembly appropriated one-time funding of $15.4 million for cybersecurity operating expenses, of which $11.4 million was from the general fund and $4 million was from the strategic investment and improvements fund. The Legislative Assembly also appropriated $2.3 million of ongoing funding from the general fund for 8 new FTE cybersecurity positions.

SELECT CYBERSECURITY-RELATED STATUTES

Audits of Computer Systems

North Dakota Century Code Section 15-10-44.2 provides any auditor hired to conduct audits of the State Board of Higher Education and the entities under the control and supervision of the board may conduct a review and assessment of any computer system or related security system of the State Board of Higher Education or any entity under the control and supervision of the board. A review and assessment under this section may include an

assessment of system vulnerability, network penetration, any potential security breach, and the susceptibility of the system to cyber attack or cyber fraud.

Section 54-10-29 provides the State Auditor may conduct a review and assessment of computer systems and related security systems. Computer systems subject to this section include the computer systems of a state agency or political subdivision that is subject to audit by the State Auditor. Tests conducted in connection with this review and assessment may include an assessment of system vulnerability, network penetration, potential security breach, and susceptibility to cyber attack or cyber fraud. The State Auditor may procure the services of a specialist in information security systems or other contractors deemed necessary in conducting a review under this section.

Powers and Duties of the Information Technology Department

Section 54-59-05 relates to the powers and duties of ITD, which includes the department shall:

- Advise and oversee cybersecurity strategy for all executive branch state agencies, including institutions under the control of the state board of higher education, counties, cities, school districts, or other political subdivisions. For purposes of this subsection, the department shall consult with the attorney general on cybersecurity strategy; and
- Advise and consult with the legislative and judicial branches regarding cybersecurity strategy.

2021 CYBERSECURITY-RELATED LEGISLATION

House Bill No. 1314 - Cybersecurity Incidents

This bill established Chapter 54-59.1 related to requirements for executive branch state agencies and political subdivisions to disclose cybersecurity incidents to ITD. The bill provides for immediate and ongoing disclosure requirements to ITD, requires ITD to establish and make known methods to securely disclose cybersecurity incidents to ITD, and requires ITD to report to the Legislative Management all disclosed cybersecurity incidents reported to ITD pursuant to Chapter 54-59.1. The department is required to ensure all reports of disclosed cybersecurity incidents are communicated in a manner that protects victims of cybersecurity incidents, prevents unauthorized disclosure of cybersecurity plans and strategies, and adheres to federal and state laws regarding protection of cybersecurity information. The bill provided the legislative and judicial branches may disclose cybersecurity incidents to ITD.

House Bill No. 1395 - COVID-19 Funding

This bill provided a $61.9 million 2019-21 biennium appropriation to ITD from the federal Coronavirus Relief Fund for costs related to cybersecurity, telework, and digital government initiatives in response to the Coronavirus (COVID-19) pandemic. The bill includes an exemption authorizing ITD to continue the funding into the 2021-23 biennium. Of the total, ITD anticipates spending $29.6 million on cybersecurity expenses to address an increase in security incidents related to the COVID-19 pandemic, including contractor support, additional software and licenses, staff training, and on-call third-party support for large-scale incidents.

House Bill No. 1417 - Memorandums of Understanding

This bill amended Section 54-59-05 regarding the powers and duties of ITD to allow ITD to enter a memorandum of understanding with state and local government entities for the purposes of ensuring the confidentiality, availability, and integrity of state information systems and data, including consulting, developing cybersecurity strategy, prevention of cybersecurity incidents, and response strategies to cybersecurity incidents. The bill allows ITD to charge an amount equal to the cost of the services rendered by ITD to agencies that receive federal or special funds. Section 18 of Senate Bill No. 2021 declared House Bill No. 1417 an emergency measure.

Senate Bill No. 2007 - Veterans' Home IT

Section 5 of this bill amended Section 54-59-05 to exclude IT of the Veterans' Home from being required to be provided by, supervised by, and regulated by ITD. Section 6 of the bill amended Section 54-59-22 to exclude email, file and print administration, database administration, application server, and hosting services of the Veterans' Home from being required to be provided by ITD.

Senate Bill No. 2021 - Information Technology Department

This bill includes appropriations for ITD, as well as transfers, exemptions, Legislative Management studies, and legislative intent. Section 6 of the bill further amended Section 54-59-05 to remove a requirement established in Section 5 of Senate Bill No. 2007 to require ITD to consult with the Veterans' Home regarding cybersecurity strategy.

INFORMATION TECHNOLOGY SECURITY AUDIT
2019-21 Biennium

In Senate Bill No. 2004 (2019), the Legislative Assembly appropriated $450,000, of which $150,000 is from the general fund and $300,000 is from other funds, to the State Auditor's office to contract with consultants to test IT systems security, including vulnerability testing, of ITD and the North Dakota University System, pursuant to Sections 15-10-44.2 and 54-10-29.

During the 2019-20 interim, the State Auditor contracted with a third-party cybersecurity consulting and auditing vendor, Secure Yeti, to conduct an IT security audit of ITD and the University System. In March 2021, the State Auditor and Secure Yeti reported the results of the audit to the Information Technology Committee. The University System's Core Technology Services and the 11 higher education institutions were included in the audit. Of the 13 physical locations between ITD and the University System, 6 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. The audit of ITD included testing at the Capitol.

The purpose of the audit was to assess the security of IT in state government and identify potential vulnerabilities in the state network, systems, and applications. 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. 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 STAGEnet when users access a website or system on STAGEnet.

The audit consisted of a phishing campaign in which 698 phishing emails were sent to nonhigher education email addresses, of which 76, or 11 percent, successfully phished users into clicking risky links or content. The audit included 730 phishing emails being sent to higher education email addresses, of which 199, or 27 percent, successfully phished users into clicking risky links or content. The University System responded within 5 minutes of the first phishing emails sent and ITD responded within 3 minutes. The University System and ITD were aware of the vulnerabilities identified in the audit and both organizations indicated the key findings in the audit report will not require significant network, system, or process changes to mitigate potential risks and vulnerabilities.

Secure Yeti reported 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, but the University System does not have the resources to respond to the risks identified in the audit.

Information Technology Security Audit Historical Funding

The following is a summary of funding appropriated to the State Auditor's office to contract with consultants to test state government IT system security:

Biennium	General Fund	Other Funds	Total
2005-07	$100,000		$100,000
2007-09	100,000		100,000
2009-11	150,000		150,000
2011-13	150,000		150,000
2013-15	250,000		250,000
2015-17	250,000	$200,000	450,000
2017-19	0	0	0
2019-21	150,000	300,000	450,000
2021-23	150,000	300,000	450,000
Total	$1,300,000	$800,000	$2,100,000

NETWORK CYBERSECURITY REQUIREMENTS

The 2019-20 Information Technology Committee received information from ITD regarding cybersecurity and minimum-security requirements for state and political subdivisions using the statewide technology access for government and education network (STAGEnet). The Information Technology Department reported efforts were being made to establish 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. The Information Technology Department formed a cybersecurity steering committee for state agencies and political subdivisions, which was expected to 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.

The committee was informed ITD has strategic cybersecurity authority for political subdivisions but no authority to enforce compliance with ITD's cybersecurity requirements. The department provides 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 are implemented at the local level. Concerns related to cybersecurity compliance from political subdivisions were addressed in House Bill No. 1314 (2021).

CYBERSECURITY INSURANCE

The 2019-20 Information Technology Committee received information from ITD and the Risk Management Division of the Office of Management and Budget regarding cybersecurity insurance. The state has a cybersecurity insurance policy that insures all state government agencies, except the Bank of North Dakota, which has its own cybersecurity insurance policy, in the event of a cybersecurity or ransomware attack. The policy does not cover counties, cities, school districts, or other political subdivisions. The Risk Management Division combined other state agency cybersecurity insurance policies into the combined state policy in February 2018.

The state cybersecurity insurance policy includes a $250,000 deductible and provides coverage of up to $5 million of damages in the event of a successful cybersecurity attack. Damages the policy covers 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. The policy does not pay for the loss of data or value.

The state cybersecurity insurance policy provides an additional $5 million of coverage if the state is held liable if other entities that rely on STAGEnet experience a successful cybersecurity attack. The policy cost for fiscal year 2021 is approximately $146,000, which is paid from the risk management fund.

Political subdivisions are insured through the North Dakota Insurance Reserve Fund, which includes no deductible and covers costs associated with an information breach but does not cover damages from cybersecurity events.

STUDY PLAN

The following is a proposed study plan for the committee's consideration in its study regarding costs incurred by ITD to deliver core technology services and cybersecurity services to state agencies and political subdivisions:

1. Receive and review information from representatives of ITD regarding:
   a. Cybersecurity services provided to state agencies and political subdivisions, including network, application, information, operational, disaster recovery, and business continuity services;
   b. Revenue received from state agencies and political subdivisions for IT services provided;
   c. The cost and percentage-share of cybersecurity services provided to state agencies and political subdivisions;
   d. Information regarding cybersecurity targets, threats, concerns, and breaches in state agency and political subdivision systems;
   e. The status of state and local government cybersecurity infrastructure and capacity, including STAGEnet cybersecurity requirements and the effects of House Bill No. 1314 (2021);
   f. The status of the new 29 FTE cybersecurity positions authorized for the 2021-23 biennium, including recruitment of cybersecurity personnel from North Dakota;

g. Updates of cybersecurity spending, including how the funding has been spent and a comparison of state and local cybersecurity spending;

h. Potential alternative cybersecurity funding sources and any proposed legislation needed related to political subdivisions potentially paying their share of cost of government cybersecurity;

i. The effects of changes made in Senate Bill No. 2007 (2021) related to the Veterans' Home IT, including the effect on state and local cybersecurity and STAGEnet; and

j. Any memorandums of understanding entered with state and local government entities as a result of House Bill No. 1417 (2021).

2. Receive and review information from representatives of political subdivisions regarding cybersecurity services provided by ITD, cybersecurity needs, and the feasibility of paying for the local share of government cybersecurity services.
3. Consider the feasibility and desirability of political subdivisions paying their share of the cost of government cybersecurity services.
4. Receive and review information from interested persons regarding the committee's study of state and local government cybersecurity.
5. Develop recommendations and any bill drafts necessary to implement the recommendations.
6. Prepare a final report for submission to the Legislative Management.

ATTACH:1