17.8014.01000

FISCAL NOTE

Requested by Legislative Council
12/23/2016

Revised
Bill/Resolution No.: HB 1088

1 A. **State fiscal effect:** *Identify the state fiscal effect and the fiscal effect on agency appropriations compared to funding levels and appropriations anticipated under current law.*

	2015-2017 Biennium		2017-2019 Biennium		2019-2021 Biennium	
	General Fund	Other Funds	General Fund	Other Funds	General Fund	Other Funds
Revenues						
Expenditures						
Appropriations						

1 B. **County, city, school district and township fiscal effect:** *Identify the fiscal effect on the appropriate political subdivision.*

	2015-2017 Biennium	2017-2019 Biennium	2019-2021 Biennium
Counties			
Cities			
School Districts			
Townships			

2 A. **Bill and fiscal impact summary:** *Provide a brief summary of the measure, including description of the provisions having fiscal impact (limited to 300 characters).*

This measure would allow OMB to pay from the Risk Management Fund notification and remediation costs following a data breach involving a state entity or the cost of insurance to cover data breach response and remediation costs. Fiscal impact cannot be determined.

B. **Fiscal impact sections:** *Identify and provide a brief description of the sections of the measure which have fiscal impact. Include any assumptions and comments relevant to the analysis.*

Expenditures would be limited to the existing statutory caps contained in NDCC Chapter 32-12.2 and would only be made to the extent the Risk Management Fund could continue to meet current and future liability obligations. The extent to which the Risk Management Fund will experience actuarially projected losses and the extent to which prompt notification and remediation will reduce liability exposures cannot be determined.

3. **State fiscal effect detail:** *For information shown under state fiscal effect in 1A, please:*

A. **Revenues:** *Explain the revenue amounts. Provide detail, when appropriate, for each revenue type and fund affected and any amounts included in the executive budget.*

All state entities are required to participate in the Risk Management Fund by contributing an actuarially determined appropriate share of its costs. The Risk Management Fund is actuarially reviewed ever two years with recommended allocations to each state entity made prior to the start of the next biennial budget process.

B. **Expenditures:** *Explain the expenditure amounts. Provide detail, when appropriate, for each agency, line item, and fund affected and the number of FTE positions affected.*

All expenditures would involve special funds and would be pursuant to the continuing appropriation contained in NDCC 32-12.2-07.

C. **Appropriations:** *Explain the appropriation amounts. Provide detail, when appropriate, for each agency and fund affected. Explain the relationship between the amounts shown for expenditures and appropriations. Indicate whether the appropriation or a part of the appropriation is included in the executive budget or relates to a continuing appropriation.*

Name:	Tag Anderson
Agency:	OMB
Telephone:	701-328-7580
Date Prepared:	12/28/2016

17.8014.01000

FISCAL NOTE

Requested by Legislative Council
12/23/2016

Bill/Resolution No.: HB 1088

1 A. **State fiscal effect:** *Identify the state fiscal effect and the fiscal effect on agency appropriations compared to funding levels and appropriations anticipated under current law.*

	2015-2017 Biennium		2017-2019 Biennium		2019-2021 Biennium	
	General Fund	Other Funds	General Fund	Other Funds	General Fund	Other Funds
Revenues						
Expenditures						
Appropriations						

1 B. **County, city, school district and township fiscal effect:** *Identify the fiscal effect on the appropriate political subdivision.*

	2015-2017 Biennium	2017-2019 Biennium	2019-2021 Biennium
Counties			
Cities			
School Districts			
Townships			

2 A. **Bill and fiscal impact summary:** *Provide a brief summary of the measure, including description of the provisions having fiscal impact (limited to 300 characters).*

B. **Fiscal impact sections:** *Identify and provide a brief description of the sections of the measure which have fiscal impact. Include any assumptions and comments relevant to the analysis.*

3. **State fiscal effect detail:** *For information shown under state fiscal effect in 1A, please:*

A. **Revenues:** *Explain the revenue amounts. Provide detail, when appropriate, for each revenue type and fund affected and any amounts included in the executive budget.*

B. **Expenditures:** *Explain the expenditure amounts. Provide detail, when appropriate, for each agency, line item, and fund affected and the number of FTE positions affected.*

C. **Appropriations:** *Explain the appropriation amounts. Provide detail, when appropriate, for each agency and fund affected. Explain the relationship between the amounts shown for expenditures and appropriations. Indicate whether the appropriation or a part of the appropriation is included in the executive budget or relates to a continuing appropriation.*

Name: Tag Anderson
Agency: OMB
Telephone: 701-328-7580
Date Prepared: 12/28/2016

2017 HOUSE GOVERNMENT AND VETERANS AFFAIRS

HB 1088

2017 HOUSE STANDING COMMITTEE MINUTES

Government and Veterans Affairs Committee
Fort Union, State Capitol

HB 1088
1/5/2017
26626

□ Subcommittee
□ Conference Committee

Committee Clerk Signature	Carmen Hart

Explanation or reason for introduction of bill/resolution:

Relating to data breach response and remediation costs

Minutes:

Attachment 1

Chairman Kasper opened the hearing on HB 1088.

Tag Anderson, Director of the Risk Management Division of OMB, appeared in support. Attachment 1. (1:07-2:35)

Rep. Laning: Where did the Risk Management funds originate?

Tag Anderson: The Risk Management fund has contributions from all state entities. Every two years we do an actuarial review where the projected losses from the Risk Management fund are projected into the future. Then they allocate out what each agency's appropriate share of that cost would be.

Rep. Laning: Is there a dollar amount on the fund, and is there a limit on it?

Tag Anderson: There is no cap per say on the funds. The fund level is determined by the actuarial professionals that we engage and their projections as to how much we need to maintain to meet current and future obligations. The fund is currently at about $6.7 million.

Chairman Kasper: You indicated you wanted the authority to purchase insurance. Is there a nationwide insurance fund that states purchase from or individual carriers?

Tag Anderson: Currently, Risk Management Division of OMB would have authority to purchase liability insurance where we determine that the exposure presents too significant risk to self-fund for it. This legislation would allow us to purchase insurance to cover those first party costs that an agency would otherwise be responsible for. We would be looking at all options to come up with the right mix as to what should be self-funded, what layers, the limits, and looking at all available carriers.

Chairman Kasper: Do you currently have a stop loss policy in place?

Tag Anderson: We do for third party liability claims. We have a policy with Swiss Re up to $10 million. That sits on top of the statutory caps that are established in 32-12.2 of the Century Code.

Chairman Kasper: How many claims have we had against the fund in the last five years?

Tag Anderson: As of December 1, we had about 156 outstanding claims. I would venture to guess it is about that number times five. The total indemnification from the _fund since its inception is about $5.9 million.

Chairman Kasper: When was the inception?

Tag Anderson: 1997

Chairman Kasper: You have a reserve of $6 million. Over the last 20 years, you have had a total of $6 million in claims. Is there really a problem, or are you concerned that there are potential bigger problems on the horizon because of what is going on with a tax and things like that?

Tag Anderson: The fund level is largely guided by the actuaries that we engage. They determine the contributions to the fund, but the fund also grows based upon investment returns and the nature of the losses that we have. ND has been very good at having a very low loss rate. This legislation is providing the flexibility to cover those first-party costs that otherwise would be the responsibility of the impacted agency. Keep in mind, many agencies are not large enough and don't have enough in operating to simply do what they need to do to notify people and take appropriate remediation measures that we hope would forestall or prevent third-party liability claims being brought.

Chairman Kasper: Since 1997, does that include all claims, or does it not include these remediation claims that agencies might have been responsible for?

Tag Anderson: The $5.9 million would strictly have been indemnity payments made on third-party liability claims. We have had two fairly large data breach incidents over the last four years.

Chairman Kasper: Any idea what those two data breaches cost?

Tag Anderson: Roughly $4.5 million between the two breaches.

Chairman Kasper: In the last couple years?

Tag Anderson: Last four years.

Lisa Feldner, ND University System, appeared in support of the bill. We did experience a breach several years ago, and it is nice to have the pool with dollars to be able to litigate. Our breach was about $220,000 to litigate and to provide the credit monitoring.

Rep. C. Johnson: What kind of information is at risk with data breaches?

Lisa Feldner: In our case it was employee names, addresses, and social security numbers. All of our evidence pointed that none of the data was actually breached. None of it was ex filtrated, but we provided litigation services anyway.

No opposition.

Chairman Kasper closed the hearing.

Rep. Schneider made a motion for a DO PASS.

Rep. Karls seconded the motion.

A roll call vote was taken. 14 Yeas, 0 Nays, 0 Absent.

Rep. Vetter will carry the bill.

Date: 1-5-17
Roll Call Vote #: 1

2017 HOUSE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 1088

House Government and Veterans Affairs Committee

□ Subcommittee

Amendment LC# or Description:

Recommendation:
□ Adopt Amendment
☒ Do Pass □ Do Not Pass □ Without Committee Recommendation
□ As Amended □ Rerefer to Appropriations
□ Place on Consent Calendar

Other Actions:
□ Reconsider □

Motion Made By M. Schneider Seconded By Karls

Representatives	Yes	No	Representatives	Yes	No
Jim Kasper-Chairman	X		Pamela Anderson	X	
Scott Louser-Vice Chairman	X		Mary Schneider	X	
Jason Dockter	X				
Craig A. Johnson	X				
Daniel Johnston	X				
Karen Karls	X				
Ben Koppelman	X				
Vernon Laning	X				
Christopher D. Olson	X				
Karen M. Rohr	X				
Vicky Steiner	X				
Steve Vetter	X				

Total (Yes) 14 No 0

Absent 0

Floor Assignment Rep. Vetter

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

HB 1088: Government and Veterans Affairs Committee (Rep. Kasper, Chairman) recommends **DO PASS** (14 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). HB 1088 was placed on the Eleventh order on the calendar.

2017 SENATE GOVERNMENT AND VETERANS AFFAIRS

HB 1088

2017 SENATE STANDING COMMITTEE MINUTES

Government and Veterans Affairs Committee
Sheyenne River Room, State Capitol

HB 1088
2/16/2017
Job Number 28431

□ Subcommittee
□ Conference Committee

Committee Clerk Signature	Carie Winings

Explanation or reason for introduction of bill/resolution:

A BILL for an Act to create and enact a new section to chapter 32-12.2 of the North Dakota Century Code, relating to data breach response and remediation costs.

Minutes:

Attachments: 1 - 2

Chairman Poolman: Opened the hearing on HB 1088.

Tag Anderson, Director, Risk Management Division, OMB: See Attachment #1 for testimony to explain and in support of the bill.

(2:00) Senator Bekkedahl: Is this dealing strictly with state level agencies or does it extend to political subdivisions as well?

Tag Anderson: It is strictly state agencies.

(2:40) Dan Sipes, Interim CIO, State of North Dakota: Testified in support of the bill. About a year ago we had a cyber-security task force that was the governor cyber security task force and in looking at several of the things that we wanted to do to both improve our posture, to prevent cyber-attacks, and also to respond to cyber-attacks, this issue of cyber insurance and having options on the table to state agencies to do that was one of the recommendations that came out of the cyber security task force. This bill paves the way for some of the options that we need to effectively respond in the event of a cyber-attack. Our office certainly supports that and if you were to talk to all of the members of that task force, they would concur with that as well.

(3:33) Senator Bekkedahl: Who is on the cyber security task force? Is that a large committee or is that mostly agency people?

Dan Sipes: It was the governor cyber security task force and so that was agency heads. I think it included about 16 agencies. It included, Lisa Feldner from the university system, General Dohrmann, Greg Wilz, the tax department, PERS, DHS, OMB, Health Department, Job Service, Workforce Safety and Insurance etc. It was a lot of those agencies that would have had citizen data that we are trying to protect. I can get the committee a copy of the task force report if you would like. See Attachment #2 for a copy of the task force report.

(4:52) Lisa Feldner, Chief of Staff, North Dakota University System: Testified in favor of the bill. It is a good thing to have, that pool of money available in the event of a breach or to mitigate the costs.

Chairman Poolman: No further testimony was present. Closed the hearing on HB 1088.

Senator Bekkedahl: Moved a Do Pass.

Senator Vedaa: Seconded.

A Roll Call Vote Was Taken: 5 yeas, 0 nays, 1 absent.

Motion Carried.

Senator Meyer will carry the bill.

Date: 2/16
Roll Call Vote #: 1

2017 SENATE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 1088

Senate Government and Veterans Affairs Committee

□ Subcommittee

Amendment LC# or Description:

Recommendation: □ Adopt Amendment
☒ Do Pass □ Do Not Pass □ Without Committee Recommendation
□ As Amended □ Rerefer to Appropriations
□ Place on Consent Calendar

Other Actions: □ Reconsider □

Motion Made By Bekkedahl Seconded By Vedaa

Senators	Yes	No	Senators	Yes	No
Chairman Poolman	✓		Senator Marcellais	✓	
Vice Chairman Davison	Ab				
Senator Bekkedahl	✓				
Senator Meyer	✓				
Senator Vedaa	✓				

Total (Yes) 5 No 0

Absent 1

Floor Assignment Meyer

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

HB 1088: Government and Veterans Affairs Committee (Sen. Poolman, Chairman) recommends **DO PASS** (5 YEAS, 0 NAYS, 1 ABSENT AND NOT VOTING). HB 1088 was placed on the Fourteenth order on the calendar.

2017 TESTIMONY

HB 1088

Attach 1
1088
1-5-17

Testimony on HB 1088
Tag Anderson, Director
OMB Risk Management Division
January 5, 2017

Chairman Kasper, and members of the House Government and Veterans Affairs Committee, my name is Tag Anderson. I am the Director of the Risk Management Division of OMB. I appear today in support of HB 1088.

Following the loss of sovereign immunity, the legislative assembly established the Risk Management Fund as the State's self-retention fund to address most third-party liability exposures. The Fund is administered by the Risk Management Division of OMB pursuant to N.D.C.C. Chapter 32-12.2. HB 1088 would provide OMB with authority to spend monies from the Risk Management Fund for notification and remediation costs following a data breach that otherwise would be the responsibility of the impacted state entity. The ability to pay for these first-party costs and ensure prompt notification and remediation is an important loss control measure to reduce third-party exposures resulting from a data breach. HB 1088 would also allow OMB to purchase insurance and approve the purchase of insurance by individual state entities to cover exposures from a data breach.

This concludes my prepared remarks and I would be happy to answer any questions you may have.

Thank you.

HB 1088 2-16-17 #1

Testimony on HB 1088
Tag Anderson, Director
OMB Risk Management Division
February 16, 2017

Chairman Poolman, and members of the Senate Government and Veterans Affairs Committee, my name is Tag Anderson. I am the Director of the Risk Management Division of OMB. I appear today in support of HB 1088.

Following the loss of sovereign immunity, the legislative assembly established the Risk Management Fund as the State's self-retention fund to address most third-party liability exposures. The Fund is administered by the Risk Management Division of OMB pursuant to N.D.C.C. Chapter 32-12.2. HB 1088 would provide OMB with authority to spend monies from the Risk Management Fund for notification and remediation costs following a data breach that otherwise would be the responsibility of the impacted state entity. The ability to pay for these first-party costs and ensure prompt notification and remediation is an important loss control measure to reduce third-party exposures resulting from a data breach. HB 1088 would also allow OMB to purchase insurance and approve the purchase of insurance by individual state entities to cover exposures from a data breach.

This concludes my prepared remarks and I would be happy to answer any questions you may have.

Thank you.

#B 1088 2-16-17 #2 pg 1

State of North Dakota

Cybersecurity Task Force

Final Report

October 2016

"Cybersecurity is a significant and growing challenge facing our nation today, and North Dakota's executive branch of government is not immune from the threat of cyber-attacks."

GOVERNOR JACK DALRYMPLE

HB 1088 2-16-17 #2 pg 2

TABLE OF CONTENTS

Executive Summary

On September 28, 2015 Governor Jack Dalrymple established a Cybersecurity Task Force to help address the rapidly evolving and expanding cyber threats facing the nation and the potential impact on North Dakota's state government. The task force is comprised of information technology experts and directors from a number of state agencies. The task force was asked to focus on five primary goals and objectives:

- Raise executive level awareness
- Discuss state government cybersecurity governance model
- Discuss cyber incident response strategies
- Share best practices / review network defense strategies and tools
- Recommend new policies for mitigating future cyber-attacks

Attacks on critical infrastructure have become a growing cause of concern for organizations around the globe. Governmental agencies have become a primary target of cyber-attacks because of the vast amount of citizen data that is collected and stored. The frequency and sophistication of these attacks are increasing and the industry as a whole has made combating this activity a high priority. A variety of factors are increasing the exposure of cybersecurity threats. The interplay between advances in technology, increased interaction between computer systems, and changes in how agencies and citizens use technology increase the level of complexity of the systems we use and give rise to emerging vulnerabilities. The current digital landscape includes cyber criminals whose objective may be to steal money or information for commercial gain; nation states that may seek to acquire information to advance national objectives; and hacktivists whose objectives may be to disrupt and embarrass an organization. The insider threat must also be considered as employees inside organizations have been responsible for a number of security breaches in almost every industry.

While the State of North Dakota continues to make substantial improvements to our cybersecurity policies and practices, it is clear that cybersecurity threats are evolving and increasing – in sophistication, intensity, diversity and volume. Additional work is required to mitigate the mounting threats and disruption to state agencies if attacks succeed.

The first meeting of the task force took place on October 19, 2015 with additional meetings held periodically over the next 12 months. The members discussed the current state of cybersecurity in state government and around the world, cybersecurity governance for North Dakota state government, current North Dakota laws related to cybersecurity, cyber insurance, cyber disruption planning for critical infrastructure, cyber incident response plans, and the importance of business continuity planning in the event of a major cyber incident.

The task force worked diligently over the last year to prepare the following recommendations that will continue to reduce risk to government systems and data, build on the substantial cybersecurity investments already made by the state, and strengthen the overall cybersecurity posture of state government.

- Expand the Scope and Pace of Scanning Web Applications and Remediate High Risk Vulnerabilities
- Provide Contingency Funding to Remediate High Risk Applications
- Develop a Common Risk Ranking Methodology for the Application Inventory
- Develop and Administer a Common Security and Risk Assessment Program
- Finalize and Communicate Cybersecurity Roles and Responsibilities
- Implement a Phishing Awareness Program
- Expand the Scope of Proactive Cybersecurity Monitoring
- Expand the Use of Multi-Factor Authentication
- Finalize and Communicate a Cyber-Incident Response Guide
- Create Legislation for Self-Insurance and Proactively Negotiate Cyber-Incident Response Contracts

HB 1088 2-16-17 #2 pg 5

All organizations have limited resources and the State of North Dakota is facing a challenging budget climate in the upcoming biennium. As a result, it is important that state agencies continue to work as a single enterprise and allocate the proper resources for cybersecurity. This coordinated approach to combat the growing threat from cyber-attacks will be imperative as state agencies work together on the recommendations to improve the state's posture related to cybersecurity both now and in the future. The State of North Dakota is committed to continuing to protect the availability, integrity, and confidentiality of all systems and the data they contain.

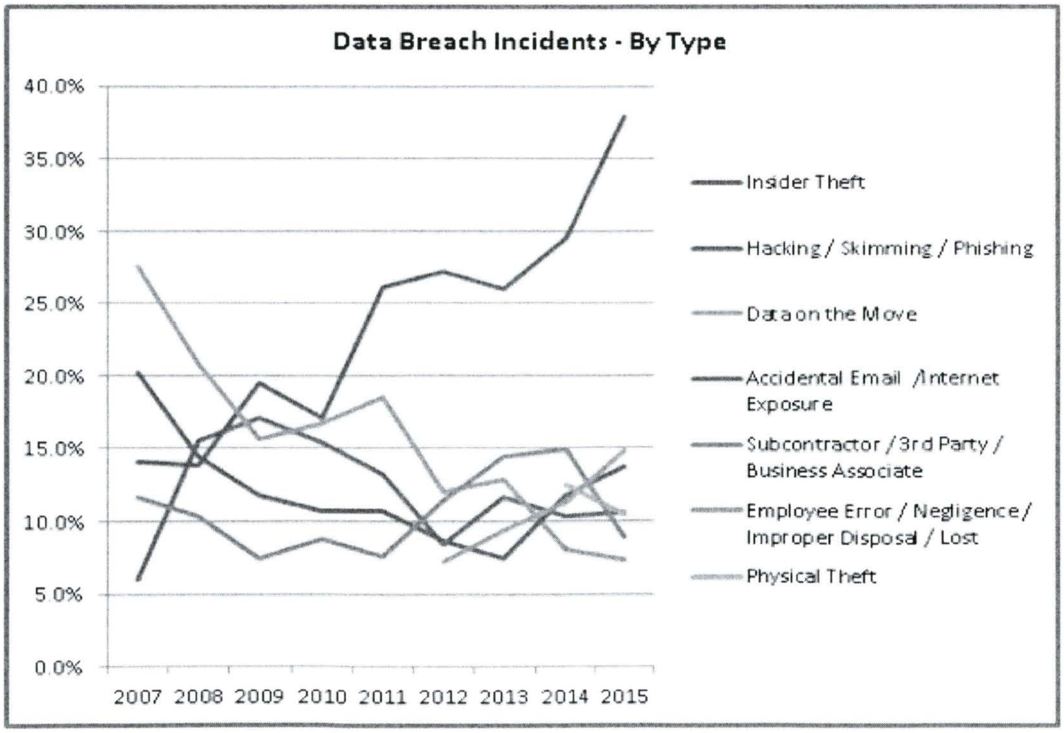
HB 1088 2-16-17 #2 pg 6

Current Cybersecurity Environment

"Cybersecurity" can be defined in a number of ways. The task force took a broad view and defined cybersecurity as protecting networks, computers, programs, and associated citizen data and information from compromise. "Compromise" refers to a loss of data confidentiality, integrity or availability.

Cyber landscape

The Identity Theft Resource Center reported that there were 780 data breaches nationally in 2015 exposing over 177 million records. Due to the volume and value of the data they manage, healthcare and government are primary targets, accounting for 44% of the breaches and 88% of the records exposed. Other targeted sectors include business, financial services and education. From the chart below we see that phishing attacks are the preferred method of cyber-attacks due to the high success ratio they return in obtaining information. This is why every individual in the organization needs to be aware of threats and be properly trained on safe computing practices.



Identity Theft Resource Center (2015)

Despite ever-improving network defenses, cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication and severity of impact. While cyber threats cannot be eliminated, cyber risk can be managed.

In September of 2013 the National Governors Association Released a paper entitled Act and Adjust: A Call to Action for Governors for Cybersecurity (www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf). The paper called out five main actions for governors to improve their cybersecurity posture and help detect and defend against cyber-attacks. The following is a brief overview of the state's activity related to each action.

- **Establish a Governance and Authority Structure for Cybersecurity**
  - ✓ Unlike most states, North Dakota operates a single statewide network and has centralized most of its information technology hosting with the Information Technology Department (ITD). As a result, North Dakota is in a strong position to treat state government agencies as a single enterprise related to information security strategies and policies.
  - ✓ North Dakota Century Code 54-59 assigns the Information Technology Department the responsibility to provide many technology services for state and local government and to ensure proper measures for security. ITD has a dedicated security division that is responsible for coordinating security of the statewide network as well as the data and computing resources hosted in the state data center. This division is headed by a Chief Information Security Officer (CISO) and reports to the state Deputy Chief Information Officer.
  - ✓ ITD's CISO chairs the Security Domain Team which is part of the state's Enterprise Architecture (EA) initiative related to technology standards and policies. This team develops state security policies and standards for state agencies. The EA program is a highly collaborative process focusing on the architecture for applications, data, security, and technology. It includes active participation from both the legislative and judicial branches of government.
  - ✓ The University System does not directly participate in the EA process but the System does have a Security Officer and an Information Security Council that represents the 11 institutions. ITD also coordinates with the NDUS CIO and their security staff on global security issues.

- ✓ The University System Information Security Council uses an Information and Security Strategic Plan to set security policies and standards for the University System. The original plan outlined six priority objectives and most have been implemented, including multifactor authentication integration, improved protection for users with elevated privileges, centralized logging, and enhanced endpoint protections.
- ✓ In the 64th Legislative Session, the North Dakota University System was given additional funding to upgrade its security posture and add security staff.
- ✓ This past legislative session, ITD was given an additional security position dedicated to partnering with the Adjutant General's office to provide better cybersecurity coordination and information sharing with the quasi-government / critical infrastructure sectors.
- ✓ An additional position was provided to work with K-12 schools across the state to enhance security education and best practices at an enterprise level.
- ✓ The state works closely with the North Dakota Association of Counties to coordinate security measures at this level of government.

➢ **Conduct Risk Assessments and Allocate Resources Accordingly**

- ✓ The state network and the state data center undergo regular audits which include targeted penetration tests. This includes a biennial audit performed by the State Auditor's office in tandem with a cybersecurity consultant as well as various federal audits of specific programs that have applications and data hosted at ITD.
- ✓ The North Dakota University campuses undergo annual security audits conducted through the State Auditor's office. Results of the audits have helped determine the allocation of additional security resources.
- ✓ ITD conducts an internal risk assessment to help prioritize its security initiatives and make any necessary changes to the controls and processes in the Cybersecurity Framework.
- ✓ The state recently completed an initiative to create an enterprise inventory of all the information systems in use by state government. This initiative helps to identify which systems contain personally identifiable information (PII) and other critical data and allows ITD and agencies to apply proactive security measures for these systems if necessary.

- ✓ ITD has implemented an application brokering service for state agencies. With the maturity of cloud computing some agencies have selected Software as a Service (SaaS) solutions where the systems and data are managed and hosted by cloud vendors. However moving applications to the cloud does not remove the need to evaluate and document the security posture of these applications. The application brokering process helps to ensure we are taking an enterprise approach to the data and systems we move to the cloud and helps to ensure that the security of the data and system are adequate before these solutions are implemented.
- ✓ Select staff within ITD and other state agencies have security clearances to receive security briefings from the Department of Homeland Security (DHS).

➢ **Implement Continuous Vulnerability Management and Threat Mitigation Practices**

- ✓ ITD performs regular internal scans on its networks, servers and applications to proactively identify and remediate security vulnerabilities.
- ✓ ITD has implemented and administers identity management systems, firewalls, intrusion prevention / detection systems, security information and event correlation systems to prevent and detect cyber-attacks against the state network and state computing infrastructure.
- ✓ ITD partners with the Multi-State Information Sharing & Analysis Center (MS-ISAC). The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial governments. The MS-ISAC has a 24x7 cybersecurity operations center and provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.
- ✓ ITD participates in the Department of Homeland Security Continuous Diagnostics and Mitigation program. This partnership augments the state's cybersecurity monitoring capabilities and helps to proactively identify cybersecurity risks.

- **Ensure the State Complies with Current Cybersecurity Methodologies**
  - ✓ ITD documents its security objectives and controls in the Cybersecurity Framework. This document maps to the federal Cybersecurity Framework issued by the National Institute of Standards and Technology (NIST). The framework focuses on the following five security functions:
    - **Identify**
      This function focuses on identifying the state's most critical digital assets and potential risks to those assets.
    - **Protect**
      This function focuses on developing and implementing appropriate safeguards and controls to protect networks, systems and data.
    - **Detect**
      This function focuses on implementing technology and processes to enable timely identification of cybersecurity events.
    - **Respond**
      This function focuses on developing and implementing processes and protocols to take appropriate action in response to a detected cybersecurity event.
    - **Recover**.
      This function focuses on restoring critical services and reducing the impact from a cyber event.
  - ✓ The NIST framework includes a cross-mapping of high level security controls and processes which allows ITD to map their processes and controls to other information standards including COBIT (Control Objectives for Information Technology) and ISO (International Organization for Standardization).
  - ✓ Various state and federal audits evaluate ITD's compliance with cybersecurity standards and best practices including NIST and COBIT.
  - ✓ ITD is an active member in the National Association of State Chief Information Officers (NASCIO), the National Association of State Technology Directors (NASTD), the Multi-State Information Sharing Analysis Center (MS-ISAC), InfraGard, and partners with other vendors in the private sector. These organizations provide information on cybersecurity trends and best practices regarding combatting cybersecurity threats.

HB 1088 2-16-17 #2 pg 11

- **Create a Culture of Risk Awareness**
  - ✓ ITD, in conjunction with the MS-ISAC, promotes an annual Cybersecurity Awareness program in state government. This includes a proclamation signed by the governor along with training on current cyber threats and safe computing practices for all state employees.
  - ✓ Each state agency appoints a Security Officer who is responsible for communicating with ITD on all agency cyber security issues and raising security awareness within the agency.
  - ✓ Agencies are encouraged to participate in the biennial briefing conducted by the security consultant who audits ITD as part of the audit conducted by the State Auditor.
  - ✓ The Consumer Protection division of the North Dakota Attorney General's office promotes cybersecurity awareness issues to state citizens.

HB 1088 2-16-17 #2 pg 12

Cybersecurity Task Force Activities

During the past year, the task force discussed the evolving threats in cybersecurity and how they were impacting state government and individual agencies. The task force also reviewed the processes and practices the state has in place today. Here is an overview of task force activities grouped by the task force's main objectives.

➢ Raise executive level awareness

- ✓ Reviewed the NGA Call to Action document
- ✓ Reviewed the Cybersecurity National Action Plan
  (https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan)
- ✓ Discussed a cybersecurity overview from the National Association of Insurance Commissioners
- ✓ Discussed current cyber-attack tactics occurring internationally, including the growing threat of ransomware attacks
- ✓ Reviewed the current roles and responsibilities of ITD and agencies relating to the security of state government systems
- ✓ Discussed the 2015 state cybersecurity incident
- ✓ Discussed cyber insurance needs / current risk management coverages
- ✓ Discussed the importance of agency disaster recovery / business continuity programs
- ✓ Reviewed current cybersecurity laws that exist in ND Century Code
- ✓ Discussed the multiple entities that audit the state data center and state network and potential strategies to better coordinate the audit processes
- ✓ Discussed the annual cybersecurity awareness month program each October and the importance of communicating this to all employees

➢ Discuss state government cybersecurity governance model

- ✓ Discussed cybersecurity governance for state government, higher education, K-12 education, and critical infrastructure and key resources
- ✓ Discussed ND Century Code 54-59 which defines ITD cybersecurity responsibilities for state government
- ✓ Discussed the advisory role of the state information technology advisory committee (SITAC) which includes all three branches of government and includes private sector members
- ✓ Discussed the role of the Enterprise Architecture program in setting cybersecurity policies and standards

- ✓ Reviewed high level responsibilities for cybersecurity for the following roles in state government
  - o ITD
  - o State Agency Directors
  - o State Agency IT Coordinators
  - o State Agency Security Officers
  - o End Users

➢ Discuss cyber incident response strategies

- ✓ Discussed the importance of notifying affected stakeholders of cyber events
- ✓ Reviewed and discussed current North Dakota Century Code regarding notification requirement for cyber events involving personally identifiable information (PII) or protected health information (PHI) *(see Appendix B)*
- ✓ Reviewed and enhanced the ND template for responding to unauthorized data disclosures which provides guidance on the protocols and process for coordinating the proper response to potential cyber events involving the disclosure of personally identifiable information *(see Appendix A)*

➢ Share best practices / review network defense strategies and tools

- ✓ The task force reviewed high level practices around the following items
  - o Centralized identity management systems and multi-factor authentication availability
  - o State network protection and monitoring technologies such as firewalls, intrusion prevention and detection systems and security event information management systems
  - o Tools and current practices related to proactively scanning web applications and computer systems to identify potential security vulnerabilities
  - o The impact of the timing patch cycles in relation to the state's cybersecurity posture and associated impact on the performance and availability of production systems
  - o Investments made to enhance the redundancy and resilience of the state network (STAGEnet) and data center
- ✓ The task force reviewed potential challenges to remediate web applications with vulnerabilities

HB 1088 2-16-17 #2 pg 14

➢ Recommend new policies for mitigating future cyber attacks

- ✓ Discussed the importance of agencies coordinating with the ND Risk Management office if an agency procures cyber insurance
- ✓ Discussed developing a cybersecurity education initiative across the University System in order to meet the unmet demands for a cybersecurity workforce. Initial discussions are focusing on a graduate certificate in cybersecurity; an undergraduate minor in cybersecurity; and a non-credit professional certificate in cybersecurity. The non-credit professional certificate could consist of short course offerings to business and industry
- ✓ Discussed the development of a Cyber Disruption Plan to address cybersecurity related to critical infrastructure and key resources within the state
- ✓ Discussed the ND National Guard's participation in the Army National Guard Protection Team initiative
- ✓ Created a list of ten recommendations to improve the cybersecurity posture for state government

HB 1088 2-16-17 #2 pg 15

Recommendations

The task force developed a list of ten security initiatives which are grouped below according to the objectives of the task force.

Initiatives	Task Force Objective
Finalize and Communicate Cybersecurity Roles and Responsibilities	Governance and Awareness
Develop and Administer a Common Security and Risk Assessment Program	Governance and Awareness
Implement a Phishing Awareness Program	Governance and Awareness
Expand the Scope and Pace of Scanning Web Applications and Remediate High Risk Vulnerabilities	Best Practices and Policies for Mitigation
Develop a Common Risk Ranking Methodology for the Application Inventory	Best Practices and Policies for Mitigation
Expand the Scope of Proactive Cybersecurity Monitoring	Best Practices and Policies for Mitigation
Expand the use of Multi-Factor Authentication	Best Practices and Policies for Mitigation
Provide Contingency Funding to Remediate High Risk Applications	Policies for Mitigation
Finalize and Communicate a Cyber-Incident Response Guide	Incident Response Strategy
Create Legislation for Self-Insurance and Proactively Negotiate Cyber-Incident Response Contracts	Incident Response Strategy

The task force was asked to rank the importance of each initiative. The following is a list of the recommendations based on the initial rankings along with a description of the recommendation.

1) Expand the Scope and Pace of Scanning Web Applications and Remediate High Risk Vulnerabilities

   - Today, ITD is running security scans on agency web applications that were developed by ITD development staff. Due to the in-depth nature of the current scanning process combined with the large number of applications, the current process is projected to take 12-18 months to complete. The task force recommended that ITD add resources to the scanning team to cover all applications hosted in the ITD data center and attempt to shorten the timeframe to complete the scanning.

     If high risk vulnerabilities are discovered while scanning the web applications, the agency should remediate them as soon as possible. The scope of the remediation effort will vary depending on the potential impact of the vulnerability and the complexity of the application.

2) Finalize and Communicate Cybersecurity Roles and Responsibilities

   - The task force recommended that ITD work with the agencies to further refine and document the security roles and responsibilities for agencies.

3) Implement a Phishing Awareness Program

   - The task force recommended that ITD procure a training and education service to help state employees identify and avoid phishing attempts. The proposed service typically includes random testing, reporting metrics, and education for employees to help them recognize phishing attacks.

4) Expand the Scope of Proactive Monitoring

   - ITD has existing investments in software and hardware tools designed to protect the state's network infrastructure, computer systems and the volumes of sensitive data being stored. To improve the state's posture and decrease time to detect security anomalies, the task force recommended that additional staff be utilized to proactively monitor and respond to potential cyber threats. The task force recommended that ITD be able to monitor both general attacks against the state infrastructure and targeted attacks against specific applications. Specialized software tools, skills, and licensing are required to perform this monitoring. Accordingly the task force recommended keeping this service centralized within ITD.

5) Expand the use of Multi-Factor Authentication

- Multi-factor authentication (MFA) is a security process that requires the end-user to utilize multiple components to successfully authenticate and access computer systems. Most solutions in use today combine two separate forms of credential components: what the user knows (a password) and what the user has (a security token). MFA is becoming a requirement for many federal programs when accessing sensitive data. The task force recommended that agencies consider expanding the use of MFA to increase the security posture for critical data and systems.

  When an agency chooses to use MFA to control access to their application, the application may require coding changes to integrate with the MFA solution. When implementing the changes, continued use of the state's centralized identity management solution for all applications will help to optimize the administration of identities and mitigate the costs for implementing MFA solutions.

6) Finalize and Communicate a Cyber-Incident Response Guide

- When an incident occurs, it is important to have a plan in place designed to ensure a standardized approach within state government. As discussed during task force meetings, ITD will work with the Risk Management division to maintain the guide and provide communication to all agencies on its use.

7) Develop and Administer a Common Security and Risk Assessment Program

- ITD has an existing cybersecurity framework it uses to manage security for the state network and state data center. As systems continue to become more complex and integrate more with third parties, the need for a common cybersecurity program is essential. Taking an enterprise approach to cybersecurity helps to ensure that all aspects of the organization are addressed and cybersecurity processes are consistent from agency to agency. Using a standard approach to security risk assessments will allow agencies to measure their risk profile and take appropriate steps to modify their overall security posture.

8) Develop a Common Risk Ranking Methodology for the Application Inventory

- ITD has developed an inventory of agency applications that documents the type of data being collected, processed and stored for each application. It also identifies if the data is maintained in a publicly accessible system and the access controls in place for each system. Using the data collected to date along with some additional information, a risk score can be assessed for each application to determine future actions (for example the need for MFA, the level of scanning, the urgency of remediating vulnerabilities, etc.). A common scoring methodology to rank the risk of each of the applications will help the state to focus its security efforts on critical systems and data.

9) Create Legislation for Self-Insurance and Proactively Negotiate Cyber-Incident Response Contracts

- The ND Legislature created a risk management program for all state agencies. The Risk Management division of the Office of Management and Budget is responsible for managing this program and the State's self-insurance fund. The fund covers damages for third party injuries caused by the negligence or wrongful act or omission of a state employee acting within the scope of employment. The current coverage would include third party liability for damages resulting from a cybersecurity event. However, the fund does not cover first party losses. In the event of a data breach, potential first party losses for services commonly offered include: notification to those potentially affected; a central help desk that citizens can call into and get answers; credit repair and/or monitoring services. Other costs incurred by the state may include technical forensics of the equipment breached and the costs to repair the technology impacted. Cyber insurance is now being offered by insurance companies to cover these costs. The coverage can be expensive and includes complex policy language governing coverage. The cybersecurity task force discussed this and recommended the state investigate self-funding this potential liability through the Risk Management program.

The task force also recommended that the state identify the services to offer in the event of a data breach and work to proactively negotiate any necessary contracts. This will allow agencies to respond quickly if a breach occurs and will allow the state to obtain better rates because contract negotiation will occur prior to an event.

10) Provide Contingency Funding to Remediate High Risk Applications

- When vulnerabilities are discovered while scanning applications, the agency may not have the appropriation authority and/or available funding to remediate the vulnerabilities depending on the effort required. The task force recommended that contingent appropriation authority be available for agencies that have available funds. For agencies who do not have adequate resources, the task force recommended utilizing ITD's existing borrowing authority under NDCC 54-59-05 to borrow money to cover the remediation costs. The agency would then request funding in the next biennium to pay off the note.

All of these recommendations would help to improve the security posture for state government, however the task force understands that not all might be funded in the upcoming biennium. Managing security is managing risk; unless you have unlimited resources, an organization needs to focus on the policies and procedures that will have the most impact.

HB 1088 2-16-17 #2 pg 20

APPENDIX A

State of North Dakota

Responding to an Unauthorized Data Disclosure

The following checklist provides best practice recommendations to help North Dakota State agencies and institutions create a robust data breach response plan. The list also makes recommendations regarding critical decision-making activities organizations commonly face during the breach response. Note that the checklist is not linear; some response activities may happen concurrently. The checklist is general in nature and should be adapted to meet security needs and legal requirements specific to your organization. Agencies and institutions should always seek legal counsel when planning for and responding to a data breach, to ensure compliance with all applicable federal, state, and local regulations.

Validate that an unauthorized data disclosure occurred

- ☐ Examine the initial information and available logs to confirm that an unauthorized data disclosure occurred.
- ☐ Agency staff need to identify the type of information disclosed, does the identified incident include a breach of Personally Identifiable Information (PII) or Protected Health Information (PHI).
- ☐ Try to determine the method of disclosure (internal or external disclosure, malicious attack or accidental).

Once it is determined that unauthorized data was disclosed, immediately assign an incident manager (agency employee) to be responsible for the investigation

- ☐ If the Information Technology Department (ITD) discovers the disclosure, ITD will notify the Director of the agency who is responsible for the data along with their IT coordinator.
- ☐ Assign a senior level manager, such as the agency business officer or an individual at an equivalent director level position, to serve as an incident manager to coordinate multiple organizational units and the overall incident response.
- ☐ Begin breach response documentation, determine the reporting process and coordinate the flow of information (create a time line of events) about the breach so further communication will be accurate.

Assemble incident response team

- □ Create an incident response team consisting of representatives from agency management, agency public affairs, information technology, legal, risk management, finance, and possibly HR, for internal incidents.
- □ Contact ITD, if they are not already aware of the incident. The ITD security team will notify the Department of Emergency Services State and Local Intelligence Center (SLIC) if the data disclosure was a malicious act.
- □ Contact the Attorney General's Office.
- □ Contact Risk Management.
- □ Contact the Governor's Office.
- □ If criminal activity is suspected, notify the State Highway Patrol. This is the proper state agency to contact for compliance with law enforcement notification.
- □ In concert with executive leadership and legal counsel, designate a single organizational representative (typically the incident manager) authorized to initiate and/or communicate breach details to any party, including the media and/or law enforcement.

Determine the status of the breach (ITD will assist)

- □ Immediately determine the status of the breach (is it active or is it post breach.) If the breach is active, take action to prevent further data loss by securing and blocking unauthorized access to systems / data and preserve evidence (computer logs/files) for investigation.
- □ Document all mitigation efforts for later analysis.

Determine the scope and composition of the unauthorized data disclosure (ITD will assist)

- □ Identify all affected data, machines, and devices.
- □ Conduct interviews with key personnel and document facts (if criminal activity is suspected, coordinate these interviews with law enforcement).
- □ When possible, preserve evidence (backups, images, hardware, etc.) for later forensic examination. Locate, obtain, and preserve (when possible) all written and electronic logs and records applicable to the breach for examination.
- □ Determine whether in-house resources or an outside service provider will conduct forensics. ITD may contact the Multi-State Information Sharing and Analysis Center (MS-ISAC), for their assistance in the forensics process.
- □ Work collaboratively with affected parties (ITD or outside hosting vendor) to secure sensitive data, mitigate the damage that may arise from the breach, and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.
- □ Seek advice from agency legal counsel on the approved methods for protecting digital evidence, so that you are prepared and are able to properly preserve and document all evidence to ensure it can be used in a court of law, if necessary. This requires detailed

recording and following proper collection, handling, storage, custody documentation, and destruction procedures (if applicable).

Determine whether notification of affected individuals and other interested parties is appropriate and, if so, when and how to provide such notification

- □ Determine whether notification is warranted and when it should be made. Executive leadership at the senior technical and/or administrative level, in coordination with legal counsel, is the authority that should generally make this decision.
- □ Determine proper method to notify affected parties; letters, telephone calls, media, etc.
- □ If the breach represents a threat to affected individuals' identity security, consider providing credit repair, credit monitoring or identity theft protection services to mitigate the risk of negative consequences for those affected.
- □ Determine the need to notify legislators, board members, and advisory councils.

Notify the individuals / entities whose data has been disclosed

- □ Notify affected individuals whose sensitive information, including PII, has been compromised, as required by applicable federal, state, and local laws. Reach out to affected parties as soon as possible to notify them about the breach.

Collect, review, and finalize any breach response documentation and analyses reports

Assess the data breach to determine the probable cause(s) and minimize the risk of future occurrence.

- □ Address and/or mitigate the cause(s) of the data breach.
- □ Solicit feedback from the responders and any affected entities.
- □ Review breach response activities and feedback from involved parties to determine response effectiveness.
- □ Make necessary modifications to your breach response strategy to improve the response process.
- □ Enhance and modify your information security and training programs, which includes developing countermeasures to mitigate and remediate previous breaches; lessons learned must be integrated so that past breaches do not reoccur.
- □ Prepare final report.
- □ Once investigative activities have been completed, safely store, record, and/or dispose (where appropriate) all evidence. This must be done in consultation with legal counsel and Risk Management.

Consider all alternatives to replacing or clearing compromised resources and machines, including the cost of remediation or rebuilding of the assets to an acceptable security level.

HB 1088 2-16-17

#2 pg 23

APPENDIX B

North Dakota Century Code Related to Cybersecurity

NDCC	Description
NDCC 54-59-05.2	ITD will protect the network infrastructure from damage and security breaches.
NDCC 54-59-05.14	ITD will assure proper measures for security and firewalls.
NDCC 54-59-16	ITD can receive confidential information from other agencies and is subject to the same restrictions and penalties regarding the dissemination of this information as the entity involved.
NDCC 44-04-18	Specifies Exempt Records which may be withheld at the discretion of the public entity.
NDCC 44-04-24, 26	Security system plans are exempt from open record and open meeting statutes.
NDCC 44-04-27	Computer passwords and security information are considered confidential records.
NDCC 12.1-06.1-08	Computer fraud and computer crime definition and penalty.
NDCC 12.1-11-05	Tampering with public records statute. Defines government records and defines tampering with government records. Additionally, the statute covers the associated penalties for tampering with government records.
NDCC 51-30	Requires a disclosure in the event of a security breach involving personal information.

HB 1088 2-16-17 #2 pg 24

APPENDIX C

North Dakota Cybersecurity Task Force Members

The Cybersecurity Task Force was facilitated by Lt. Governor Drew Wrigley and the membership was comprised of the following:

- Mike Ressler – State Chief Information Officer
- Dan Sipes – State Deputy Chief Information Officer
- Lisa Feldner – Chief Information Officer, ND University System
- Lonnie Grabowska – Deputy Director, ND Bureau of Criminal Investigation
- Major General Alan Dohrmann – Director, Department of Emergency Services
- Greg Wilz – Director, Division of Homeland Security
- Grant Levi – Director, Department of Transportation
- Adam Hamm - State Insurance Commissioner
- Ryan Rauschenberger – State Tax Commissioner
- Maggie Anderson – Executive Director, Department of Human Services
- Sparb Collins – Executive Director, ND Public Employees Retirement System
- Pam Sharp – Director, Office of Management and Budget
- Terry Dwelle – State Health Officer
- Cheri Giesen – Executive Director, Job Service ND
- Eric Hardmeyer – President and Chief Executive Officer, Bank of North Dakota
- Bryan Klipfel – Director, Workforce Safety and Insurance
- Mark Johnson – Executive Director, Association of Counties

Members from other state agencies, including the legislative branch of government, attended the meetings and participated in the conversation.