NORTH DAKOTA HOUSE OF REPRESENTATIVES

STATE CAPITOL
600 EAST BOULEVARD
BISMARCK, ND 58505-0360

Representative Corey Mock
District 18
P.O. Box 12542
Grand Forks, ND 58208-2542
C: 701-732-0085
crmock@nd.gov

COMMITTEES:
Appropriations

March 8, 2021

Chairman Jerry Klein and Members of the Industry, Business and Labor Committee,

Today I stand before your committee as chairman of the legislative Information Technology Committee and sponsor of HB 1314.

This legislation came before your IT Committee throughout the interim as a concept per our discussion regarding cybersecurity within the state IT network.

Before I walk through the bill I'd like to offer background on North Dakota's IT network to help you better understand why this bill has been introduced.

Our Information Technology Department (ITD) was established in 1999 and has expanded in scope over the years as technology has shifted functionally from a tool to vital component of government operations. In many ways, IT has become a modern utility.

One term that has become ubiquitous in state government is STAGEnet, which is the operational term for North Dakota's state wide area network. This coordination of services has been built out over the last 20+ years to connect every state agency and political subdivision – a feat just accomplished this biennium.

Unless granted a waiver (cost or functional efficiencies, for example), each county, city and school district shall be connected to STAGEnet for voice, data, or video services. We also require ITD to establish IT security standards that must be adhered to by all users of STAGEnet, primarily for the integrity of the system and all users on the network.

Keep in mind that North Dakota has several critical services on or connected to this network, including (but not limited to) financial and vital records, service applications, state and national defense, oil and gas records, and much more.

ITD will testify to the fact that North Dakota remains a frequent target for cyberattacks from amateur hackers to foreign-state sponsored espionage. In fact, North Dakota was involved in a recent attack by state-sponsored Chinese threat actors known commonly as Hafnium. This security breach was not unique to North Dakota, but agencies and political subdivisions across the state were targeted once Microsoft discovered flaws in their software and hackers moved to exploit the hole before a patch could be deployed.

As we've learned: a breach of one is potentially a breach of all, which makes legislation found in HB 1314 critically important.

Before we move into other testimony I'll quickly walk through the legislation that will create a new section in Title 54 (state government) of North Dakota Century Code:

Definitions include industry standard and clarifying terms, such as breach, criminal justice information, denial of service (DOS) attack, financial, medical, personal, and health insurance information, malware, ransom, and others.

Where you see the term "entity" in this bill, know that it's referring to an executive branch state agency or political subdivision within this state. House IBL made this important distinction upon our request once we learned that Missouri River Energy Services (MRES) is technically a political subdivision based in South Dakota but servicing municipal clients in North Dakota. It was never intended for MRES to fall under the jurisdiction of ITD – they are already highly regulated as an energy service provider – and thus the correction was made.

The House also added the Federal Information Processing Standards (FIPS) definition of significant damage to clarify when an incident warrants reporting to ITD. This issue was heavily reviewed and considered throughout the first half of the session. We made this clarification to ensure all potentially serious incidents are reported to ITD but preventing a large number of unnecessary reports from overwhelming our IT security team.

Beginning on Page 4 Line 1, this new section of law would require any executive branch agency or political subdivision to disclose to ITD an "identified or suspected cybersecurity incident that affects the confidentiality, integrity, or availability of information systems, data, or services." Disclosure must happen in the most expedient time possible and without reasonable delay, but no specific timeline is provided understanding circumstances vary wildly.

The bill proceeds to outline the types of incidents that shall be reported to ITD once they occur or are suspected to have occurred.

On Page 4 Line 16, the bill also requires executive agencies and political subdivisions to provide ongoing disclosure to ITD until the incident is fully resolved. This section essentially requires the attacked agency or political subdivision to cooperate with ITD as they investigate and mitigate damages caused by the attack.

On Page 5 Line 4 we permit legislative and judicial branches of governments to inform ITD of any known or suspected cybersecurity attacks that would affect the confidentiality, integrity, or availability of information systems, data, or services. As separate branches of government this remains options and permissive.
The bill concludes by:

- requiring ITD to establish methods in which agencies and political subdivisions are to securely disclose incidents;
- requiring ITD to provide consultation services and other resources to assist entities, including the legislative and judicial branches, in responding to and remediating cybersecurity incidents; and
- requires ITD to report to legislative management all disclosed cybersecurity incidents as defined by this new chapter, including status updates and response / remediation efforts to mitigate the incident.

North Dakota's IT Committee unanimously supported this legislative concept; after due consideration we hope your committee comes to a similar conclusion.

Thank you for your time and efforts, Chairman Klein and members of the committee.