2021 HOUSE INDUSTRY, BUSINESS AND LABOR

HB 1314

2021 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Room JW327C, State Capitol

HB 1314
2/1/2021

Cybersecurity incident reporting requirements

(3:56) Chairman Lefor calls the hearing on HB 1314.

Representatives	Attendance
Chairman Lefor	P
Vice Chairman Keiser	P
Rep Hagert	P
Rep Jim Kasper	P
Rep Scott Louser	A
Rep Nehring	P
Rep O'Brien	P
Rep Ostlie	P
Rep Ruby	P
Rep Schauer	P
Rep Stemen	P
Rep Thomas	P
Rep Adams	P
Rep P Anderson	P

Discussion Topics:

- Coordination of technology services to state agencies and political subdivisions
- Cybersecurity breaches
- Out-of-state agencies

Rep Mock~District 18 introduced the bill. Attachment #4647.

Kevin Ford-Chief Information Security Officer NDIT. Attachment #4269.

Deb Birgen~MRES VP of Legislative & Government Relations. Attachment #4464.

Darin King~Vice Chancellor of IT-ND University System. Attachment #4627.

Brian Newby~Election Director, Secretary of State's office testified neutral.

Lefor closes the hearing. The bill will be held.

Rep Adams moved to add amendment on line 22, page 1 “political subdivisions with in the state”.

Rep O'Brien second.

Voice vote. Motion carried.

Additional written testimony: Attachment #4293, 4302, 4316 & 5216.

(4:50) End time.

Ellen LeTang, Committee Clerk

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

February 1, 2021

Good afternoon, Chairman Mike Lefor 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.

As you'll hear from Mr. Kevin Ford from ITD, North Dakota remains a frequent target for cyberattacks from amateur hackers to foreign-state sponsored espionage.

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. I would request this committee amend the bill to ensure we narrow that definition to mean a political subdivision within the state for reasons that will be explained later.

Beginning on Page 3 Line 24, 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 8, 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 4 Line 25 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.

Finally, you have testimony from Ms. Deb Birgen of Missouri River Energy Services (MRES) supporting HB 1314 but requesting a technical amendment. MRES is *technically* a North Dakota political subdivision based in South Dakota, creating jurisdictional and enforcement challenges. Per their request, I encourage you to work with Mr. Levi Kinnischtzke of Legislative Council to adopt necessary amendments consistent with our intent. These corrections ensure this new section of law remains technically and functionally enforceable.

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 Lefor and members of the committee.

#4269

Testimony to the House Industry, Business and Labor Committee on HB 1314

Kevin Ford – Chief Information Security Officer NDIT
2/01/2021

NORTH Dakota
Be Legendary.™

The Threat is Huge

North Dakota receives over 2.1 Billion detected attacks per year[1] from external threats including:

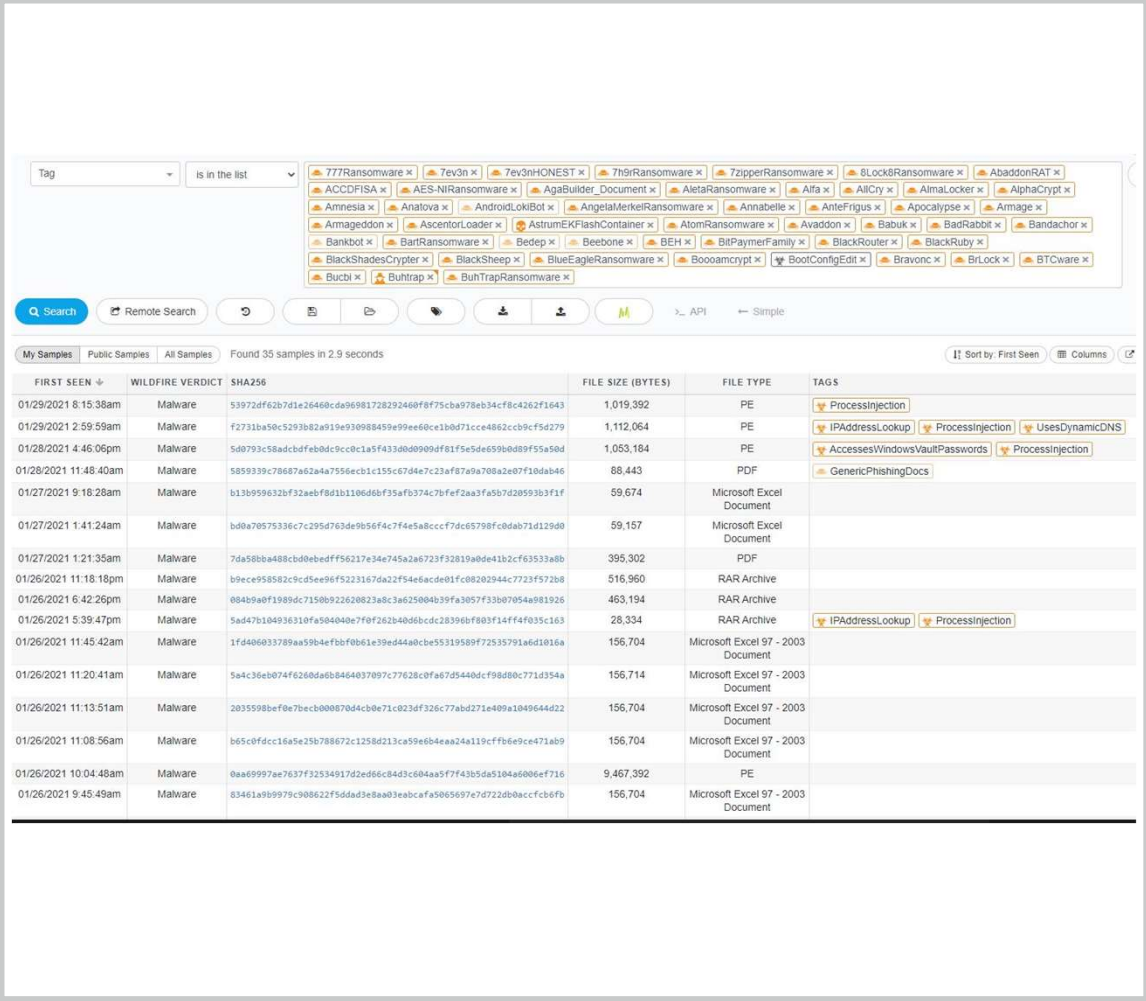
- Nation States,
  - China,
  - Russia,
  - Iran, &
  - North Korea;
- Corporate Espionage, and;
- Organized Crime Syndicates.

1. Based on ¼ Sampling of 2020 Firewall logs from June 2020, August 2020, October 2020, and Last 30 days (as of December 20, 2020)

We Have Low Visibility Around Security Events

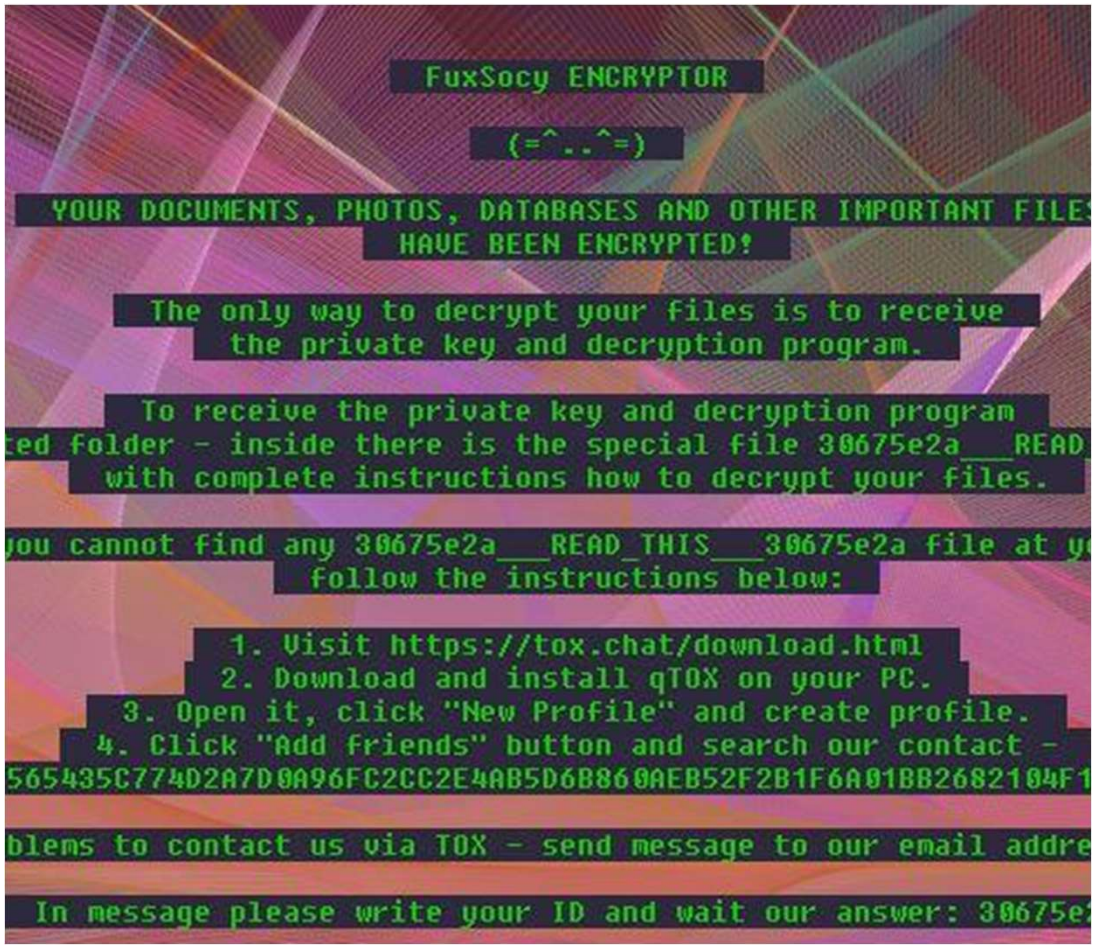
We see traffic associated with security events on STAGENet but can't attribute them

- No coordination
- No requests to centrally block
- No protection for network "neighbors"



We Have Little Information to Provide

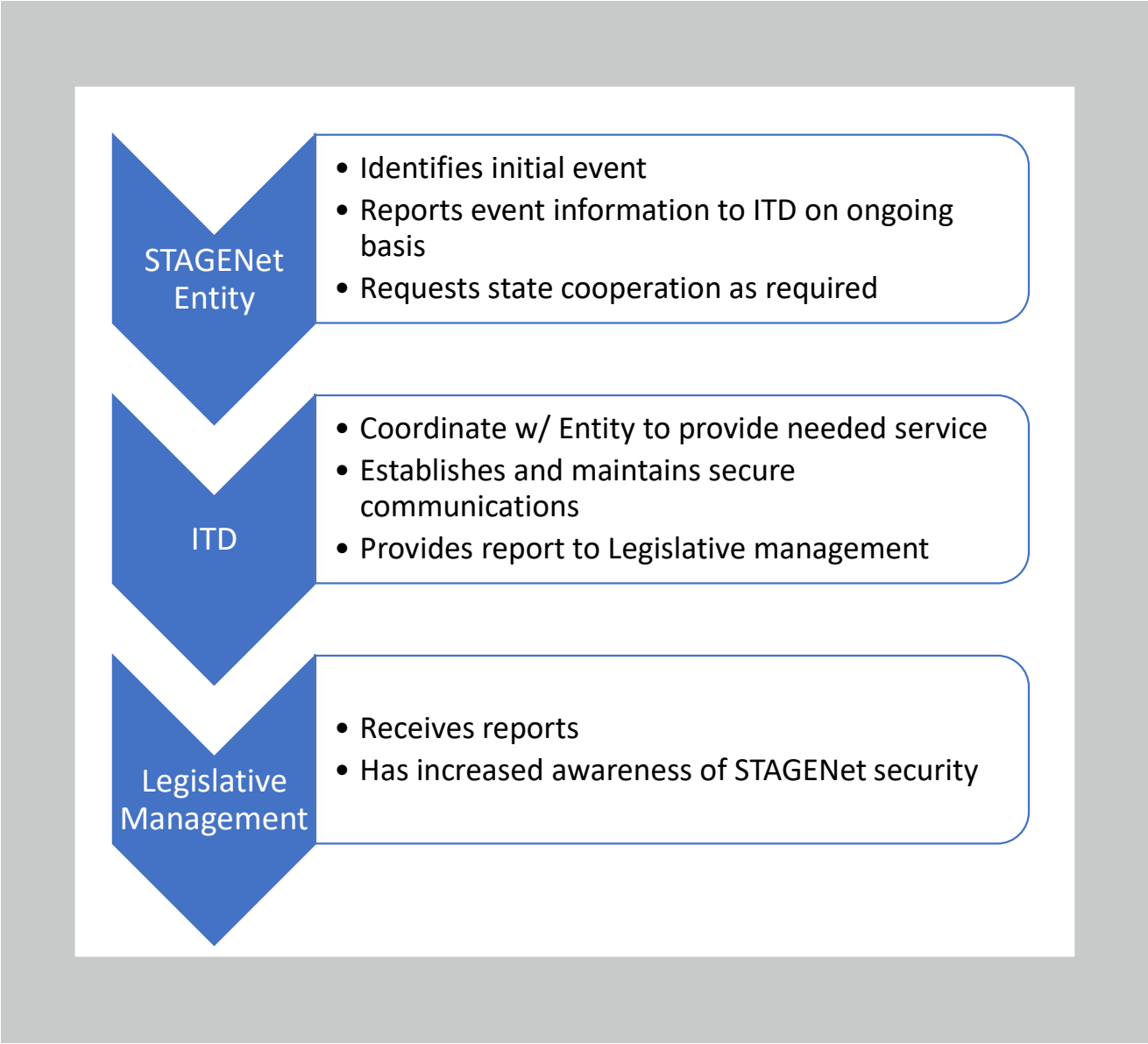
“Presentation by representatives of the Information Technology Department (ITD) regarding North Dakota's cybersecurity status, including[…] a list of North Dakota state and local government ransomware attacks known to the public.” - LITC Agenda 3/13/2020



HB 1314 - How it Works

HB 1314 will improve oversight and coordination of the state network by:

- Increases central visibility of cybersecurity events on the state network;
- Provides central network coordination to remediate impacted entity; and
- Stops the spread of cybersecurity events to other entities.



Testimony in Support of
House Bill No 1314
House Industry Business and Labor Committee
February 1, 2021

Good morning, Chairman Lefor, Members of the House Industry Business & Labor Committee, my name is Deb Birgen. Unfortunately, I am unable to attend today's hearing in person but I have asked Todd D. Kranda, an attorney at Kelsch Ruff Kranda Nagle & Ludwig law firm in Mandan, a lobbyist for Missouri River Energy Services (MRES), to appear on my behalf and provide this testimony and the amendment that is attached regarding HB 1314, the cyber security report bill.

I serve as the Vice President of Legislative & Governmental Relations for MRES. I am speaking to you on behalf of MRES which is a municipal power agency that provides wholesale electricity to sixty-one (61) municipal electric utilities in four (4) states: North Dakota, Iowa, Minnesota and South Dakota. Six (6) of the communities we serve wholesale power to are in North Dakota (Riverdale, Cavalier, Northwood, Hillsboro, Lakota & Valley City with a 7th associate member community of Maddock).

What many of you probably don't know is that MRES is a unique power supplier organized under Iowa 28E law and exists under the inter-governmental cooperation laws of Iowa, Minnesota, North Dakota, and South Dakota, headquartered in Sioux Falls, South Dakota. One of the quirks of being organized under Iowa law is that the Iowa law is often interpreted to make MRES a "political subdivision" of any state in which MRES provides power—which would include North Dakota. This is despite being headquartered in South Dakota. This has caused MRES to navigate differing state laws on a variety of subject matters. That navigation has sometimes proved burdensome with layers of

legislation that require a lot of work on MRES's behalf to obtain the same objective that would have been achieved if MRES could have only followed one state's law. Therefore, to maximize efficiency and minimize unnecessary redundancy, MRES has occasionally requested a state law to be drafted in such a way to clarify that MRES will follow South Dakota's law on a matter, rather than trying to navigate the conflicts and differences among four different state laws.

Therefore, I come before you today to ask for a very simple clarifying amendment. That is to amend the definition of "entity" at page 1, line 22, to apply only to political subdivisions "within the state". With the headquarters of MRES in South Dakota, we are already subject to a cyber-security reporting law in South Dakota and are compliant with that law. MRES is also subject to a variety of federal cyber-security laws that pertain specifically to the electric industry, which MRES is also in compliance with. So, to be clear, MRES is not asking to be excused from taking prudent security measures on behalf of MRES or our customers. Rather, MRES is simply asking that we avoid unnecessary and additional work so that we may focus on the current cyber mandates of South Dakota and the federal government.

This clarification would also avoid any delays and distractions at a critical time. If MRES did have a breach that triggered the reporting requirements of the North Dakota and the South Dakota laws, MRES would have to spend time checking back and forth with both states' regulatory bodies. Not to mention the two states have different reporting and timing aspects. This could cause confusion and even interfere in effectively and quickly mitigating the breach. To be clear, MRES does support HB 1314 and the important breach procedures it puts forth. MRES is only asking that in the event of an

emergency like a breach, that it would work side-by-side with the regulatory forces that it has local contacts with in South Dakota.

Finally, by clarifying that MRES is, for lack of a better phrase, “South Dakota’s problem”, you alleviate any additional burdens for North Dakota’s own Information Technology Department.

Thank you for taking the time to consider these comments and the proposed amendment for HB 1314.

PROPOSED AMENDMENT

Page 1, line 22, after “subdivision” insert “within the state”

Renumber accordingly

NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

HB1314

House Industry, Business and Labor Committee
February 1, 2021

Darin King, Vice Chancellor of IT, NDUS
701.777.4237| darin.r.king@ndus.edu

Chairman Lefor and members of the committee:

For the record, my name is Darin King and I am the Vice Chancellor of IT and CIO for the North Dakota University System. Thank you for allowing me a few minutes to speak in support of HB 1314.

The North Dakota State Board of Higher Education implemented Policy 1202.2 – Incident Response in April of 2018 with the purpose of directing NDUS institutions to develop incident response plans that ensure "prompt and consistent reporting of and response to IT security incidents".

Overall, my support for HB 1314 is quite strong. However, I would encourage the review of the reporting thresholds within the bill. A ten thousand dollar reporting threshold for a large organization could require the reporting of a very minor incident. The same threshold for a small organization would be a major incident that should be reported.

In many ways, HB 1314 will do for the state what Policy 1202.2 has done for the North Dakota University System. The identification, reporting, and collaborative response to cyber security incidents across state government will dramatically strengthen our collective ability to protect the people, data, and assets of North Dakota.

I respectfully ask for a "Do Pass" of HB 1314 with consideration of possible amendments to reporting thresholds.

Thank You.

NORTH DAKOTA LEAGUE of CITIES

February 1, 2021
House Industry, Business and Labor
Rep. Lefor, Chairman
HB 1314

Good morning Chairman Lefor and members of House IBL. For the record Blake Crosby, Executive Director, North Dakota League of Cities.

We support HB 1314 as we recognize the importance of protecting cities and all the State and Federal agencies they communicate with. Only by identifying and reporting of cybersecurity incidents can we take measures to protect our personal and city business data.

Cybersecurity breaches are expensive and debilitating. We need to take whatever measures are necessary to minimize the threats and mitigate future threats.

I respectfully ask for a DO-PASS on HB 1314.

NRG
TECHNOLOGY SERVICES

Testimony Prepared for the
House Industry Business and Labor Committee
Monday, February 1, 2021
By: Lonny Bosch, NRG President

RE: House Bill 1314 – Cybersecurity Reporting

Mr. Chairman and committee members, thank you for the opportunity to briefly address you regarding this important statutory provision.

North Dakota Association of Counties Resources Group, (NRG) has been providing technical support to counties for 29 years and understands the challenges counties are facing.

NRG along with County and State officials are seeing growing numbers of cyber incidents occurring. Even though all County and State offices are behind separate firewalls they still have a common backbone, StageNet, with some shared applications tied back to State servers.

In the past NRG has seen one Counties cyber issues affect other Counties. I am sure these types of cyber issues have been reported but having NDIT provide "*consultation services and other resources*", NRG believes is a good idea. NRG has been working with NDIT for several years, the skill and expertise NDIT has in cyber security is much appreciated by the Counties.

NRG does not see this as a burdensome mandate and urge a Do Pass recommendation on House Bill 1314.

1661 Capitol Way, Suite 102 | Bismarck, ND 58501
701.250.9400 | 888.303.0094 | Fax: 701.390.1107
www.nrgtechservices.com

Testimony Prepared for the
House Industry Business and Labor Committee
Monday, February 1, 2021
By: Terry Traynor, NDACo Executive Director

RE: House Bill 1314 – Cybersecurity Reporting

Mr. Chairman and committee members, thank you for the opportunity to briefly address you regarding this important statutory provision.

County officials, like state officials, recognize the growing concerns of cybersecurity within government. While we are all linked together somehow, state and county governments are inextricably bound through the numerous shared software systems that all ride on the state backbone.

One node on this backbone can, and has, affected other nodes. While I cannot imagine that any breach or attempted breach would not be reported without this statute, it is reasonable to make the communication crystal clear. More significantly, stating the obligation of NDIT to provide "*consultation services and other resources*" to the extent possible, is welcomed by county officials. The expertise, and depth of the staff resources, is so significant when compared to most counties – this provision is very encouraging.

County commissioners do not see this as a burdensome mandate and urge a Do Pass recommendation on House Bill 1314.

NDLA, Intern 08 - Borgen, Justin

From: King, Darin [mailto:darin.r.king@ndus.edu]
Sent: Tuesday, February 2, 2021 8:13 AM
To: NDLA, Intern 08 - Borgen, Justin <intern8@nd.gov>
Cc: Ford, Kevin B. <kbford@nd.gov>
Subject: HB 1314 amendment v.2

Good Morning

After further discussion with Kevin Ford, CISO at NDIT, please consider the language below for the amendment to HB 1314.

Page 3, line 30 : "Malware affecting more than ten thousand dollars worth of devices or services *and cause a significant disruption to confidentiality, integrity, or availability to data or services.*

Thank you!

Darin

Darin R. King
Vice Chancellor of IT/CIO
North Dakota University System
4349 James Ray Drive
Grand Forks, ND 58203
(701)777-4237

2021 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Room JW327C, State Capitol

HB 1314
2/3/2021

Cybersecurity incident reporting requirements

(11:47) Chairman Lefor called the work session to order.

Representatives	Attendance
Chairman Lefor	P
Vice Chairman Keiser	P
Rep Hagert	P
Rep Jim Kasper	P
Rep Scott Louser	P
Rep Nehring	P
Rep O'Brien	P
Rep Ostlie	P
Rep Ruby	P
Rep Schauer	A
Rep Stemen	P
Rep Thomas	P
Rep Adams	P
Rep P Anderson	P

Discussion Topics:

- Committee work.

Committee discussion.

(11:37-11:43) Recessed.

Rep Mock~District 18. Answered questions from the committee.

Chairman Lefor closes the hearing.

(11:54) End time.

Ellen LeTang, Committee Clerk

2021 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Room JW327C, State Capitol

HB 1314
2/9/2021

Cybersecurity incident reporting requirements

(3:19) Chairman Lefor called the work session to order.

Representatives	Attendance
Chairman Lefor	P
Vice Chairman Keiser	P
Rep Hagert	P
Rep Jim Kasper	P
Rep Scott Louser	P
Rep Nehring	P
Rep O'Brien	P
Rep Ostlie	P
Rep Ruby	P
Rep Schauer	P
Rep Stemen	P
Rep Thomas	P
Rep Adams	P
Rep P Anderson	P

Discussion Topics:

- Committee work.

Rep Stemen presented amendment 21.0198.03002. Attachments #6126 & 6127.

Rep Thomas moved amendment 21.0198.03002.

Rep Hagert second.

Voice vote Motion carried.

Rep P Anderson moved a Do Pass as Amended.

Vice Chairman Keiser second.

Kevin Ford~Chief Information Security Officer-NDIT answered questions.

Representatives	Vote
Chairman Lefor	Y
Vice Chairman Keiser	Y
Rep Hagert	Y
Rep Jim Kasper	Y
Rep Scott Louser	Y
Rep Nehring	Y
Rep O'Brien	Y
Rep Ostlie	Y
Rep Ruby	Y
Rep Schauer	Y
Rep Stemen	Y
Rep Thomas	Y
Rep Adams	Y
Rep P Anderson	Y

Vote roll call taken Motion carried 14-0-0 & Rep Stemen is the carrier.

(3:38) End time.

Ellen LeTang, Committee Clerk

DP 2/9/21
1 of 1

21.0198.03002
Title.04000

Prepared by the Legislative Council staff for
Representative Mock
February 8, 2021

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1314

Page 1, line 22, after "subdivision" insert "within the state"

Page 3, after line 23, insert:

"15. "Significant damage" means:

a. A degradation in or loss of mission capability to an extent and duration that the entity is not able to perform one or more of its primary functions;

b. Damages of ten thousand dollars or more to entity assets as estimated by the entity;

c. A financial loss of ten thousand dollars or more as estimated by the entity; or

d. Harm to individuals involving loss of life or serious life-threatening injuries."

Page 3, line 30, replace "affecting more than ten thousand dollars worth of devices or services" with "incidents that cause significant damage"

Renumber accordingly

REPORT OF STANDING COMMITTEE

HB 1314: Industry, Business and Labor Committee (Rep. Lefor, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (14 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). HB 1314 was placed on the Sixth order on the calendar.

Page 1, line 22, after "subdivision" insert "within the state"

Page 3, after line 23, insert:

"15. "Significant damage" means:

a. A degradation in or loss of mission capability to an extent and duration that the entity is not able to perform one or more of its primary functions;

b. Damages of ten thousand dollars or more to entity assets as estimated by the entity;

c. A financial loss of ten thousand dollars or more as estimated by the entity; or

d. Harm to individuals involving loss of life or serious life-threatening injuries."

Page 3, line 30, replace "affecting more than ten thousand dollars worth of devices or services" with "incidents that cause significant damage"

Renumber accordingly

21.0198.03002
Title.

Prepared by the Legislative Council staff for
Representative Mock
February 8, 2021

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1314

Page 1, line 22, after "subdivision" insert "within the state"

Page 3, after line 23, insert:

"15. "Significant damage" means:

a. A degradation in or loss of mission capability to an extent and duration that the entity is not able to perform one or more of its primary functions;

b. Damages of ten thousand dollars or more to entity assets as estimated by the entity;

c. A financial loss of ten thousand dollars or more as estimated by the entity; or

d. Harm to individuals involving loss of life or serious life-threatening injuries."

Page 3, line 30, replace "affecting more than ten thousand dollars worth of devices or services" with "incidents that cause significant damage"

Renumber accordingly

21.0198.03002

Sixty-seventh
Legislative Assembly
of North Dakota

HOUSE BILL NO. 1314

Introduced by

Representatives Mock, Bosch, Dockter, Louser, Roers Jones, Toman, Vigesaa, Weisz

Senators Davison, Piepkorn, Vedaa

A BILL for an Act to create and enact a new chapter to title 54 of the North Dakota Century Code, relating to cybersecurity incident reporting requirements.

BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:

SECTION 1. A new chapter to title 54 of the North Dakota Century Code is created and enacted as follows:

Definitions.

As used in this chapter, unless the context otherwise requires:

1. "Breach" means unauthorized access or acquisition of computerized data that has not been secured by encryption or other methods or technology that renders electronic files, media, or databases unreadable or unusable. Good faith acquisitions of personal information by an employee or agent of the employee is not a breach of security of the system if the personal information is not used or subject to further unauthorized disclosure.
2. "Criminal justice information" means private or sensitive information collected by federal, state, or local law enforcement including the following:
   a. Fingerprints or other biometric information;
   b. Criminal background and investigation information; and
   c. Personal information.
3. "Denial of service attack" means an attack against a computer system designed to make the system inaccessible to users.
4. "Department" means the information technology department.
5. "Entity" means an executive branch state agency or a political subdivision within the state.

6. "Financial information" means banking, credit, or other account information that, if accessed without being authorized, may result in potential harm to an individual and includes:
   a. Account numbers or codes;
   b. Credit card expiration dates;
   c. Credit card security codes;
   d. Bank account statements; and
   e. Records of financial transactions.
7. "Health insurance information" means an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify an individual.
8. "Identity theft or identity fraud" means all types of crime in which an individual wrongfully obtains and uses another individual's personal data in a way that involves fraud or deception, most commonly for economic gain.
9. "Malware" means software or firmware intended to perform an unauthorized process that will have adverse effect on the confidentiality, integrity, or availability of an information system and includes a virus, worm, trojan horse, spyware, adware, or other code-based system that infects hosts.
10. "Medical information" means an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
11. "Personal information" means an individual's first name or first initial and last name in combination with the following when names and data are not encrypted, but does not include information available to the public from federal, state, or local government records:
    a. The individual's social security number;
    b. The operator's license number assigned to an individual under section 39-06-14;
    c. A nondriver photo identification card number assigned to the individual under section 39-06-03.1;
    d. The individual's financial institution account number, credit card number, or debit card number in combination with required security codes, access codes, or passwords that permit access to an individual's financial accounts;

e. The individual's date of birth;

f. The maiden name of the individual's mother;

g. Medical information;

h. Health insurance information;

i. An identification number assigned to the individual by the individual's employer in combination with security codes, access codes, or passwords; or

j. The individual's digitized or other electronic signature.

12. "Ransom" means a payment for services or goods to a malicious agent to:

a. Decrypt data on a computer system;

b. Retrieve lost or stolen data; or

c. Prevent the disclosure and dissemination of information.

13. "Regulated information" means information and information technology resource protection requirements established by the federal government and regulating organizations.

14. "Regulating organizations" means organizations that issue laws, regulations, policies, guidelines, and standards, including the:

a. Federal bureau of investigation;

b. Internal revenue service;

c. Social security administration;

d. Federal deposit insurance corporation;

e. United States department of health and human services;

f. Centers for Medicare and Medicaid services; and

g. Payment card industry security standards council.

15. "Significant damage" means:

a. A degradation in or loss of mission capability to an extent and duration that the entity is not able to perform one or more of its primary functions;

b. Damages of ten thousand dollars or more to entity assets as estimated by the entity;

c. A financial loss of ten thousand dollars or more as estimated by the entity; or

d. Harm to individuals involving loss of life or serious life-threatening injuries.

Immediate disclosure to the department.

An entity shall disclose to the department an identified or suspected cybersecurity incident that affects the confidentiality, integrity, or availability of information systems, data, or services. Disclosure must be made in the most expedient time possible and without unreasonable delay. Cybersecurity incidents required to be reported to the department include:

1. Suspected breaches;
2. Malware ~~affecting more than ten thousand dollars worth of devices or services~~incidents that cause significant damage;
3. Denial of service attacks that affect the availability of services;
4. Demands for ransom related to a cybersecurity incident or unauthorized disclosure of digital records;
5. Identify theft or identity fraud services hosted by entity information technology systems;
6. Incidents that require response and remediation efforts that will cost more than ten thousand dollars in equipment, software, and labor; and
7. Other incidents the entity deems worthy of communication to the department.

Ongoing disclosure to the department during a cybersecurity incident.

Until a cybersecurity incident is resolved, an entity shall disclose clarifying details regarding a cybersecurity incident to the department, including:

1. The number of potentially exposed records;
2. The type of records potentially exposed, including health insurance information, medical information, criminal justice information, regulated information, financial information, and personal information;
3. Efforts the entity is undertaking to mitigate and remediate the damage of the incident to the entity and other affected entities; and
4. The expected impact of the incident, including:
   a. The disruption of the entity services;
   b. The effect on customers and employees that experienced data or service losses;
   c. The effect on entities receiving wide area network services from the department; and

d. Other concerns that could potentially disrupt or degrade the confidentiality, integrity, or availability of information systems, data, or services that may affect the state.

Disclosure to the department - Legislative and judicial branches.

The legislative and judicial branches may disclose to the department cybersecurity incidents that affect the confidentiality, integrity, or availability of information systems, data, or services.

Method of disclosure of cybersecurity incidents.

The department shall establish and make known methods an entity must use to securely disclose cybersecurity incidents to the department.

Statewide cybersecurity incident response.

The department, to the extent possible, shall provide consultation services and other resources to assist entities and the legislative and judicial branches in responding to and remediating cybersecurity incidents.

Disclosure to the legislative management.

The department shall report to the legislative management all disclosed cybersecurity incidents as required by this chapter, including the status of the cybersecurity incident and any response or remediation to mitigate the cybersecurity incident. The department shall 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.

2021 SENATE INDUSTRY, BUSINESS AND LABOR

HB 1314

2021 SENATE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Fort Union Room, State Capitol

HB 1314
3/8/2021 9 AM

relating to cybersecurity incident reporting requirements

Chair Klein opened the hearing at 9:00 a.m. All members were present. Senators Klein, Larsen, Burckhard, Vedaa, Kreun, and Marcellais.

Discussion Topics:

- Background on bill
- Understanding of cybersecurity attacks
- Firewalls

Representative Corey Mock introduced the bill and submitted testimony #7801 and 7802 [9:01].

Kevin Ford, Security Officer for ND IT testified in favor and submitted testimony #7711 [9:14].

Additional written testimony: 7580.

Chair Klein ended the hearing at 9:32 a.m.

Isabella Grotberg, Committee Clerk

#7801

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.

#7802

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

---

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

FOREWORD

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347). These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the federal government. The NIST, through its Information Technology Laboratory, provides leadership, technical guidance, and coordination of government efforts in the development of standards and guidelines in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

-- SUSAN ZEVIN, ACTING DIRECTOR
INFORMATION TECHNOLOGY LABORATORY

AUTHORITY

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).

TABLE OF CONTENTS

1 PURPOSE

The E-Government Act of 2002 (Public Law 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), tasked NIST with responsibilities for standards and guidelines, including the development of:

- Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each category; and
- Minimum information security requirements (i.e., management, operational, and technical controls), for information and information systems in each such category.

FIPS Publication 199 addresses the first task cited—to develop standards for categorizing information and information systems. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices. Subsequent NIST standards and guidelines will address the second and third tasks cited.

2 APPLICABILITY

These standards shall apply to: (i) all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and (ii) all federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2). Agency officials shall use the security categorizations described in FIPS Publication 199 whenever there is a federal requirement to provide such a categorization of information or information systems. Additional security designators may be developed and used at agency discretion. State, local, and tribal governments as well as private sector organizations comprising the critical infrastructure of the United States may consider the use of these standards as appropriate. These standards are effective upon approval by the Secretary of Commerce.

3 CATEGORIZATION OF INFORMATION AND INFORMATION SYSTEMS

This publication establishes security categories for both information[1] and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

[1] Information is categorized according to its *information type*. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Security Objectives

The FISMA defines three security objectives for information and information systems:

CONFIDENTIALITY

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

A loss of *confidentiality* is the unauthorized disclosure of information.

INTEGRITY

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of *integrity* is the unauthorized modification or destruction of information.

AVAILABILITY

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of *availability* is the disruption of access to or use of information or an information system.

Potential Impact on Organizations and Individuals

FIPS Publication 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

The *potential impact* is **LOW** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.[2]

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The *potential impact* is **MODERATE** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

[2] Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

The *potential impact* is **HIGH** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Security Categorization Applied to Information Types

The security category of an information type can be associated with both user information and system information[3] and can be applicable to information in either electronic or non-electronic form. It can also be used as input in considering the appropriate security category of an information system (see description of security categories for information systems below). Establishing an appropriate security category of an information type essentially requires determining the *potential impact* for each security objective associated with the particular information type.

The generalized format for expressing the security category, SC, of an information type is:

SC information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.[4]

EXAMPLE 1: An organization managing *public information* on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. The resulting security category, SC, of this information type is expressed as:

SC public information = {(**confidentiality**, NA), (**integrity**, MODERATE), (**availability**, MODERATE)}.

EXAMPLE 2: A law enforcement organization managing extremely sensitive *investigative information* determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting security category, SC, of this information type is expressed as:

SC investigative information = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, MODERATE)}.

EXAMPLE 3: A financial organization managing routine *administrative information* (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security category, SC, of this information type is expressed as:

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

[3] System information (e.g., network routing tables, password files, and cryptographic key management information) must be protected at a level commensurate with the most critical or sensitive user information being processed, stored, or transmitted by the information system to ensure confidentiality, integrity, and availability.

[4] The potential impact value of *not applicable* only applies to the security objective of confidentiality.

Security Categorization Applied to Information Systems

Determining the security category of an information system requires slightly more analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system.[5]

The generalized format for expressing the security category, SC, of an information system is:

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Note that the value of *not applicable* cannot be assigned to any security objective in the context of establishing a security category for an information system. This is in recognition that there is a low minimum potential impact (i.e., low water mark) on the loss of confidentiality, integrity, and availability for an information system due to the fundamental requirement to protect the system-level processing functions and information critical to the operation of the information system.

EXAMPLE 4: An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. The management within the contracting organization determines that: (i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and (ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security categories, SC, of these information types are expressed as:

SC contract information = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is expressed as:

SC acquisition system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the acquisition system.

[5] It is recognized that information systems are composed of both programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential mission-related functions and operations. These system processing functions also require protection and could be subject to security categorization as well. However, in the interest of simplification, it is assumed that the security categorization of all information types associated with the information system provide an appropriate *worst case* potential impact for the overall information system—thereby obviating the need to consider the system processes in the security categorization of the information system.

EXAMPLE 5: A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting security categories, SC, of these information types are expressed as:

SC sensor data = {(**confidentiality**, NA), (**integrity**, HIGH), (**availability**, HIGH)},

and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is initially expressed as:

SC SCADA system = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system. The management at the power plant chooses to increase the potential impact from a loss of confidentiality from low to moderate reflecting a more realistic view of the potential impact on the information system should there be a security breach due to the unauthorized disclosure of system-level information or processing functions. The final security category of the information system is expressed as:

SC SCADA system = {(**confidentiality**, MODERATE), (**integrity**, HIGH), (**availability**, HIGH)}.

Table 1 summarizes the potential impact definitions for each security objective—confidentiality, integrity, and availability.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

APPENDIX A TERMS AND DEFINITIONS

AVAILABILITY: Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]

CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]

EXECUTIVE AGENCY: An executive department specified in 5 U.S.C., SEC. 101; a military department specified in 5 U.S.C., SEC. 102; an independent establishment as defined in 5 U.S.C., SEC. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., CHAPTER 91. [41 U.S.C., SEC. 403]

FEDERAL INFORMATION SYSTEM: An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. [40 U.S.C., SEC. 11331]

INFORMATION: An instance of an information type.

INFORMATION RESOURCES: Information and related resources, such as personnel, equipment, funds, and information technology. [44 U.S.C., SEC. 3502]

INFORMATION SECURITY: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., SEC. 3542]

INFORMATION SYSTEM: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., SEC. 3502]

INFORMATION TECHNOLOGY: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. [40 U.S.C., SEC. 1401]

INFORMATION TYPE: A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

INTEGRITY: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]

NATIONAL SECURITY SYSTEM: Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. [44 U.S.C., SEC. 3542]

SECURITY CATEGORY: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

SECURITY CONTROLS: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

SECURITY OBJECTIVE: Confidentiality, integrity, or availability.

APPENDIX B REFERENCES

[1] Privacy Act of 1974 (Public Law 93-579), September 1975.

[2] Paperwork Reduction Act of 1995 (Public Law 104-13), May 1995.

[3] OMB Circular A-130, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

[4] Information Technology Management Reform Act of 1996 (Public Law 104-106), August 1996.

[5] Federal Information Security Management Act of 2002 (Public Law 107-347), December 2002.

Testimony to the Senate Industry, Business and Labor Committee on HB 1314

Kevin Ford – Chief Information Security Officer NDIT
3/08/2021

NORTH Dakota
Be Legendary.™

The Threat is Huge

North Dakota receives over 2.1 Billion detected attacks per year[1] from external threats including:

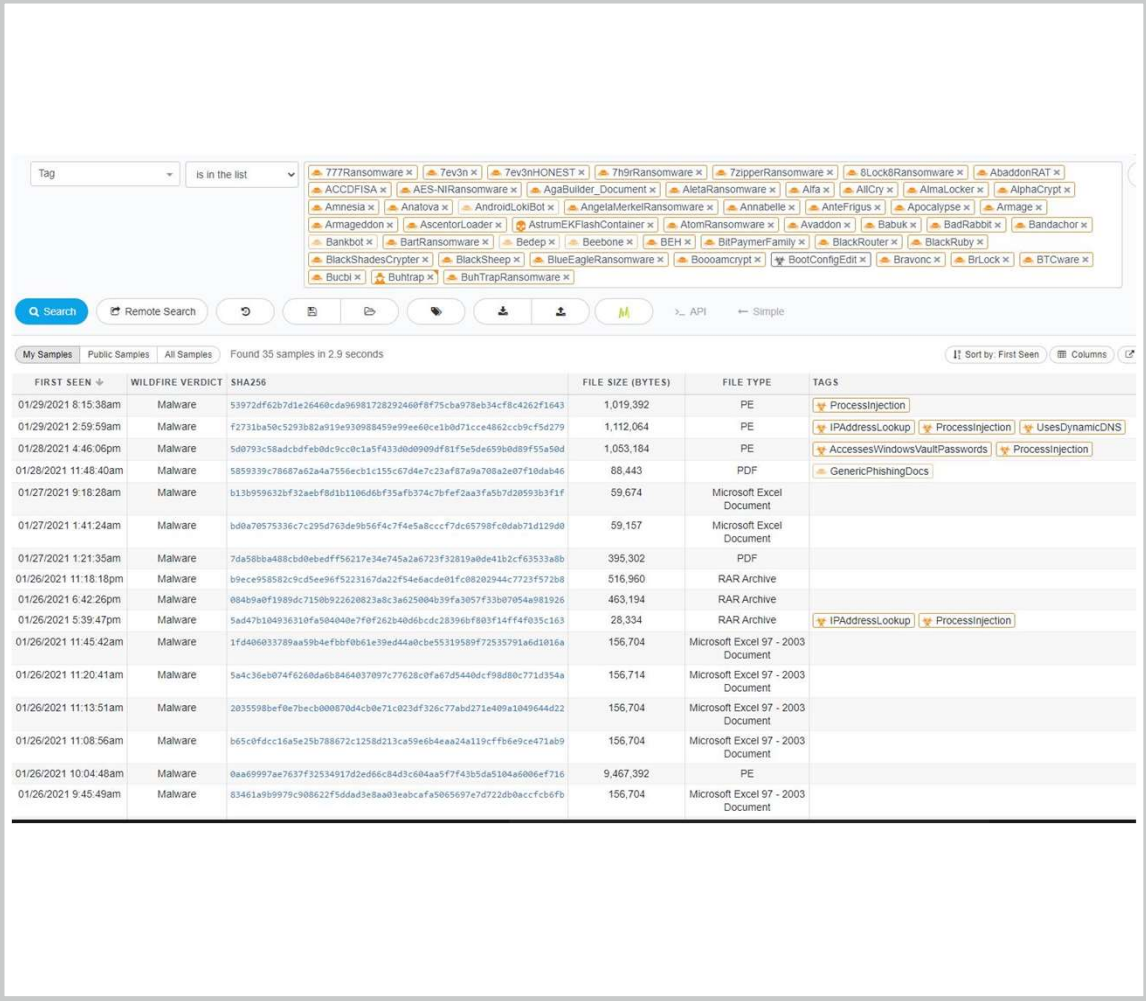
- Nation States,
  - China,
  - Russia,
  - Iran, &
  - North Korea;
- Corporate Espionage, and;
- Organized Crime Syndicates.

1. Based on ¼ Sampling of 2020 Firewall logs from June 2020, August 2020, October 2020, and Last 30 days (as of December 20, 2020)

We Have Low Visibility Around Security Events

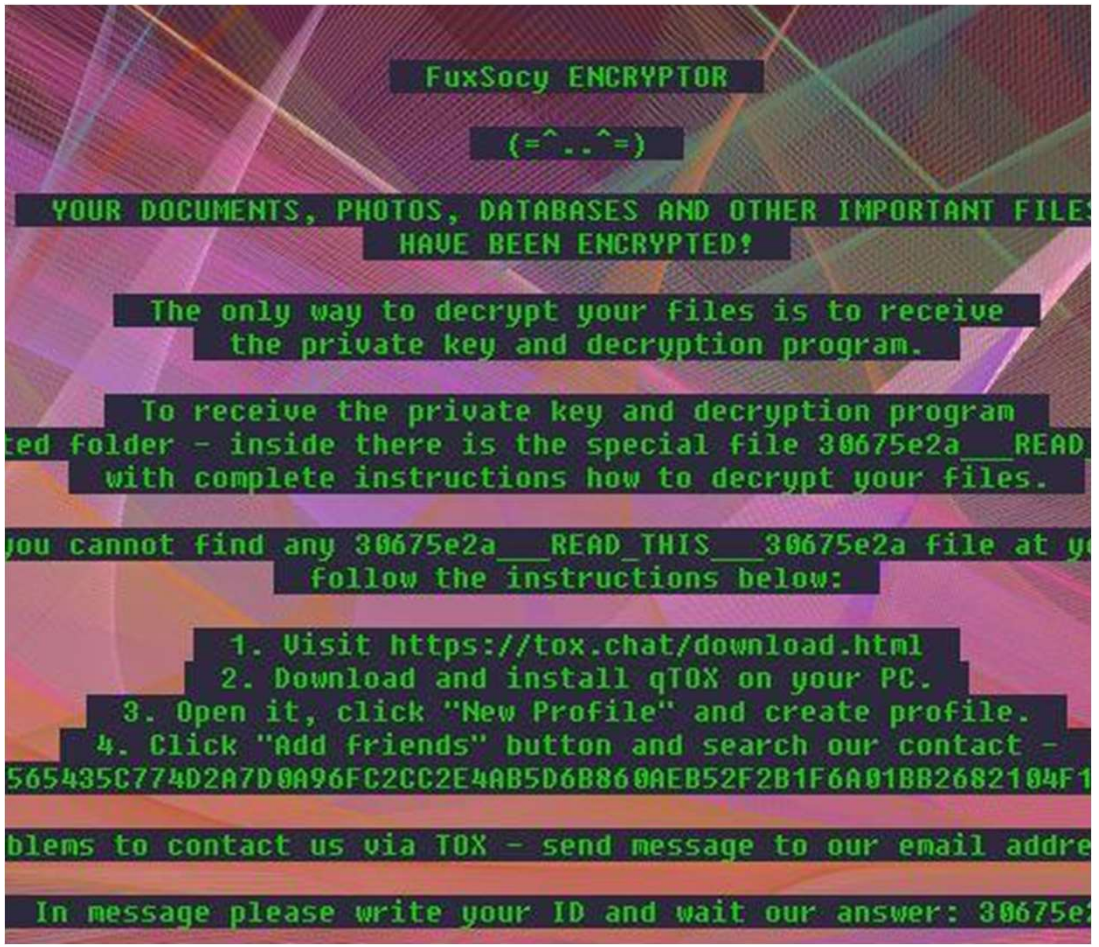
We see traffic associated with security events on STAGENet but can't attribute them

- No coordination
- No requests to centrally block
- No protection for network "neighbors"



We Have Little Information to Provide

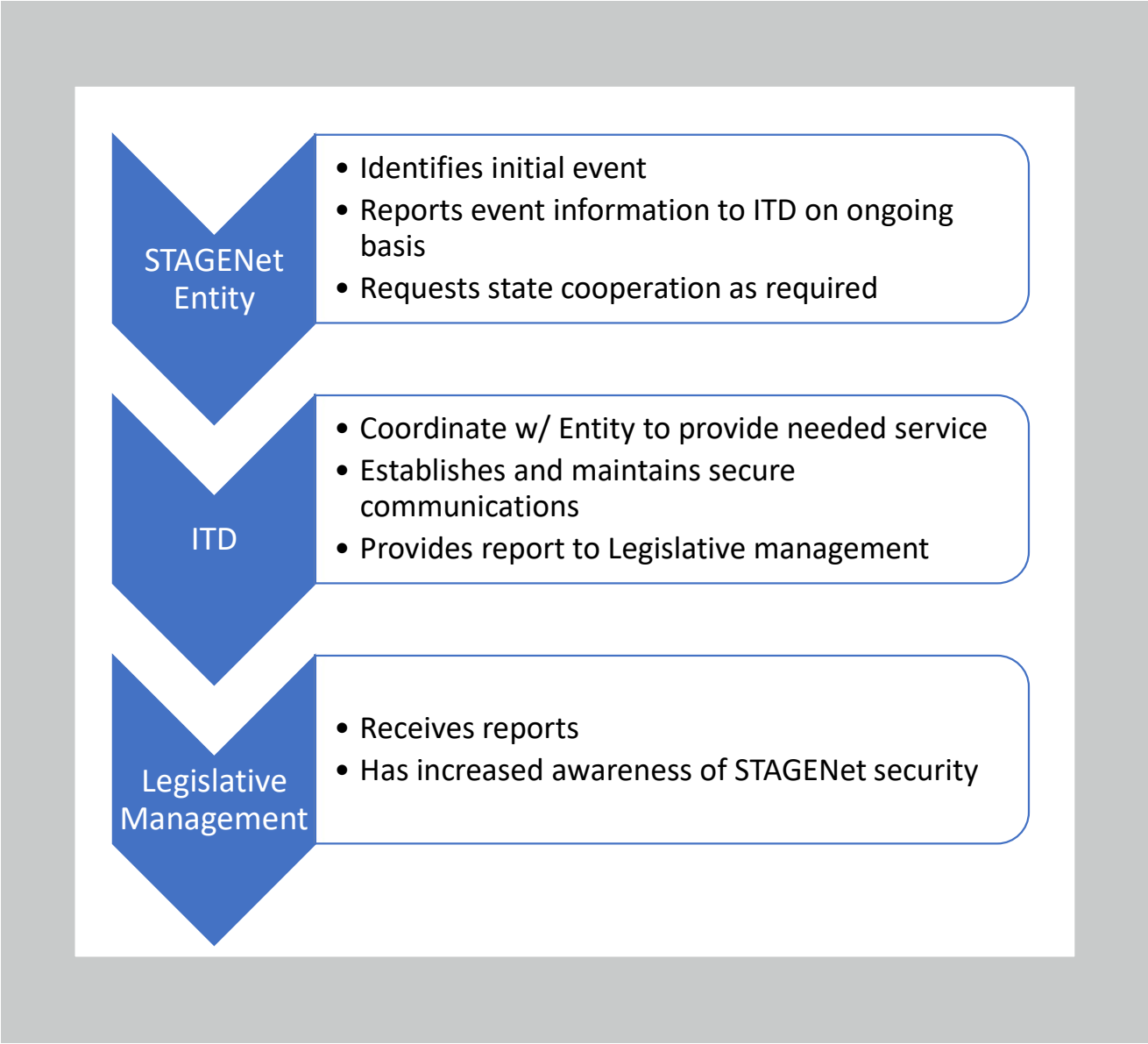
“Presentation by representatives of the Information Technology Department (ITD) regarding North Dakota's cybersecurity status, including[…] a list of North Dakota state and local government ransomware attacks known to the public.” - LITC Agenda 3/13/2020



HB 1314 - How it Works

HB 1314 will improve oversight and coordination of the state network by:

- Increases central visibility of cybersecurity events on the state network;
- Provides central network coordination to remediate impacted entity; and
- Stops the spread of cybersecurity events to other entities.



NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Engrossed HB1314
Senate Industry, Business and Labor Committee
March 8, 2021
Darin King, Vice Chancellor of IT, NDUS
701.777.4237| darin.r.king@ndus.edu

Chairman Klein and members of the committee:

For the record, my name is Darin King and I am the Vice Chancellor of IT and CIO for the North Dakota University System. Thank you for allowing me a few minutes to speak in support of engrossed HB 1314.

The North Dakota State Board of Higher Education implemented Policy 1202.2 – Incident Response in April of 2018 with the purpose of directing NDUS institutions to develop incident response plans that ensure "prompt and consistent reporting of and response to IT security incidents".

In many ways, engrossed HB 1314 will do for the state what Policy 1202.2 has done for the North Dakota University System. The identification, reporting, and collaborative response to cyber security incidents across state government will dramatically strengthen our collective ability to protect the people, data, and assets of North Dakota.

I respectfully ask for a "Do Pass" of engrossed HB 1314.

Thank You.

2021 SENATE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Fort Union Room, State Capitol

HB 1314
3/8/2021 10 AM

relating to cybersecurity incident reporting requirements

Chair Klein opened the meeting at 9:58 a.m. All members were present. Senators Klein, Larsen, Burckhard, Vedaa, Kreun, and Marcellais.

Discussion Topics:

- Necessity of bill

Senator Vedaa moved a DO PASS [9:59].
Senator Marcellais seconded the motion [9:59].

[10:00]

Senators	Vote
Senator Jerry Klein	Y
Senator Doug Larsen	Y
Senator Randy A. Burckhard	Y
Senator Curt Kreun	Y
Senator Richard Marcellais	Y
Senator Shawn Vedaa	Y

Motion passed: 6-0-0

Senator Vedaa will carry the bill [10:00].

Chair Klein ended the hearing at 10:00 a.m.

Isabella Grotberg, Committee Clerk

REPORT OF STANDING COMMITTEE

HB 1314, as engrossed: Industry, Business and Labor Committee (Sen. Klein, Chairman) recommends **DO PASS** (6 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). Engrossed HB 1314 was placed on the Fourteenth order on the calendar.