CYBERSECURITY

Jessica Newby

Information Security Officer

NORTH Dakota

Be Legendary.™

Cyber Operations Center

Analysis and Response

- Incident Response
- Forensics
- Malware Analysis

Active Defense

- Penetration testing
- Threat Intelligence
- Exploitation Analysis

Security Infrastructure

- Endpoint Protect
- Network Detection
- Vulnerability Management

Governance, Risk and Compliance

- Cyber Risk Management
- Policy/Procedure/Standards
- Compliance with Federal and Industry Regulation
- Information Security Officer Liaisons

Education and Public Awareness

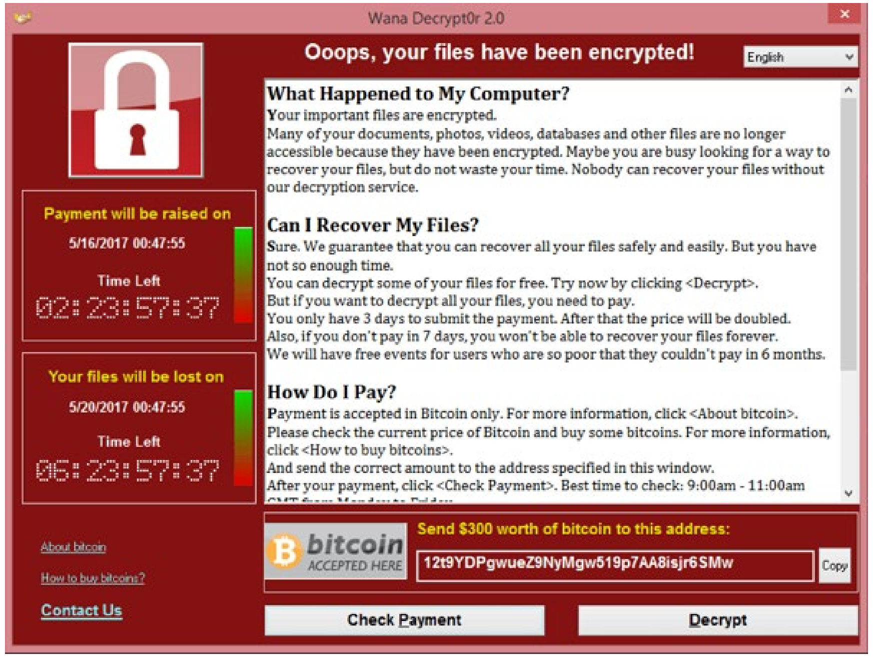
- Develops Defend.ND.gov
- Outreach to classrooms and business communities
- Works with EduTech to support K-20W initiative
- Builds a community and culture around cybersecurity in North Dakota

North Dakota Threat Environment

THREATS AND CONCERNS: RANSOMWARE IN SUPPLY CHAIN

Ransomware has been an ongoing threat in supply chain

- Energy
- Agriculture



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

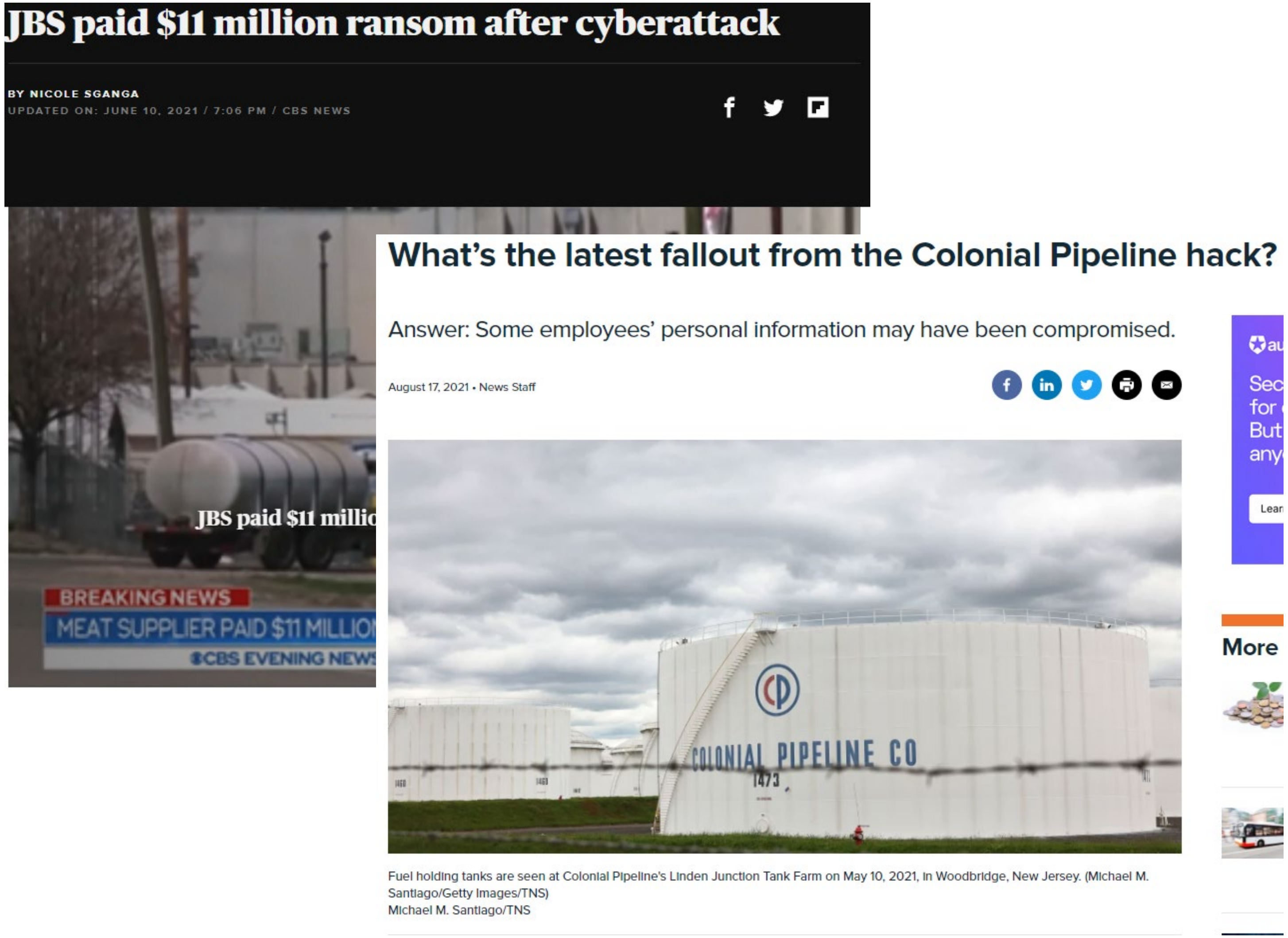
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



JBS paid $11 million ransom after cyberattack

BY NICOLE SGANGA
UPDATED ON: JUNE 10, 2021 / 7:06 PM / CBS NEWS

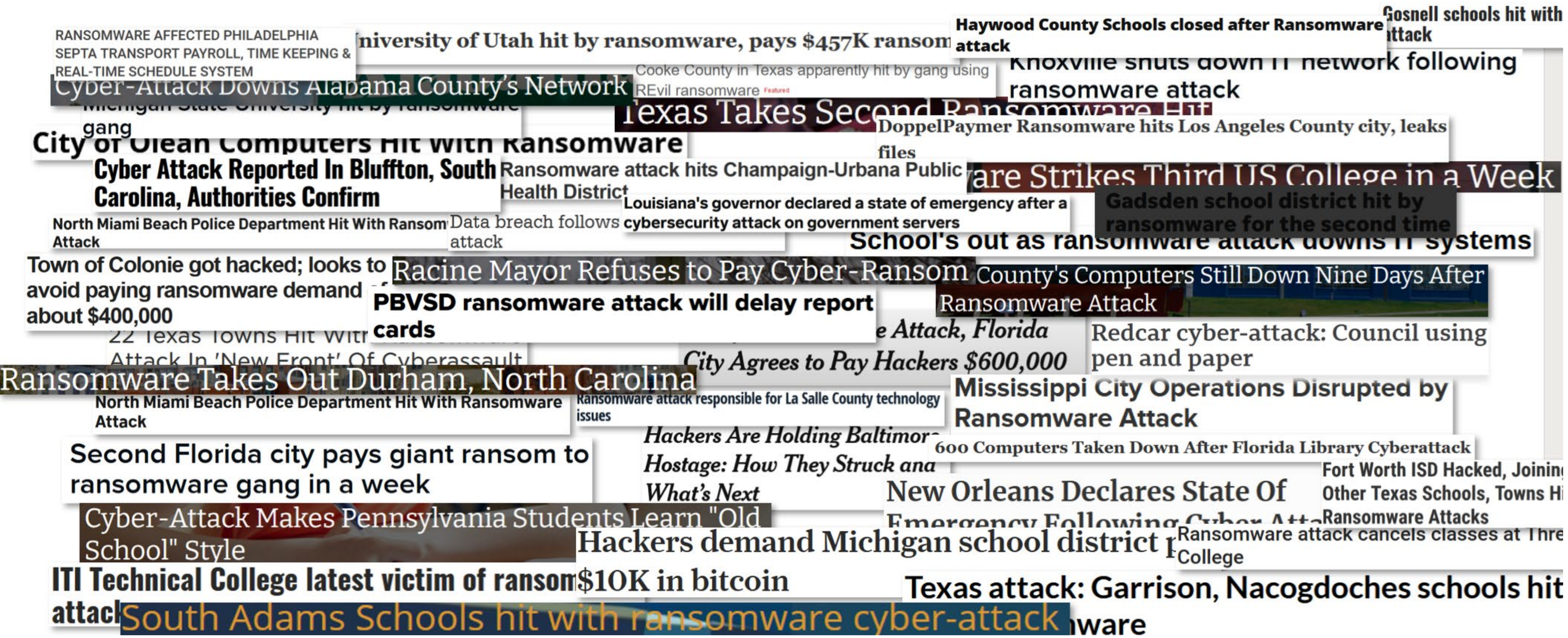
What's the latest fallout from the Colonial Pipeline hack?

Answer: Some employees' personal information may have been compromised.

August 17, 2021 • News Staff

Fuel holding tanks are seen at Colonial Pipeline's Linden Junction Tank Farm on May 10, 2021, in Woodbridge, New Jersey. (Michael M. Santiago/Getty Images/TNS)
Michael M. Santiago/TNS

THREATS AND CONCERNS: RANSOMWARE



RANSOMWARE AFFECTED PHILADELPHIA SEPTA TRANSPORT PAYROLL, TIME KEEPING & REAL-TIME SCHEDULE SYSTEM

niversity of Utah hit by ransomware, pays $457K ransom

Haywood County Schools closed after Ransomware attack

Gosnell schools hit with ttack

Cooke County in Texas apparently hit by gang using REvil ransomware Featured

Knoxville shuts down IT network following ransomware attack

Cyber-Attack Downs Alabama County's Network

Michigan State University hit by ransomware gang

Texas Takes Second Ransomware Hit

DoppelPaymer Ransomware hits Los Angeles County city, leaks files

City of Olean Computers Hit With Ransomware

Cyber Attack Reported In Bluffton, South Carolina, Authorities Confirm

Ransomware attack hits Champaign-Urbana Public Health District

are Strikes Third US College in a Week

Louisiana's governor declared a state of emergency after a cybersecurity attack on government servers

Gadsden school district hit by ransomware for the second time

North Miami Beach Police Department Hit With Ransom Attack

Data breach follows attack

School's out as ransomware attack downs IT systems

Town of Colonie got hacked; looks to avoid paying ransomware demand of about $400,000

Racine Mayor Refuses to Pay Cyber-Ransom

County's Computers Still Down Nine Days After Ransomware Attack

PBVSD ransomware attack will delay report cards

22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault

e Attack, Florida City Agrees to Pay Hackers $600,000

Redcar cyber-attack: Council using pen and paper

Ransomware Takes Out Durham, North Carolina

North Miami Beach Police Department Hit With Ransomware Attack

Ransomware attack responsible for La Salle County technology issues

Mississippi City Operations Disrupted by Ransomware Attack

Hackers Are Holding Baltimore Hostage: How They Struck and What's Next

600 Computers Taken Down After Florida Library Cyberattack

Second Florida city pays giant ransom to ransomware gang in a week

Fort Worth ISD Hacked, Joining Other Texas Schools, Towns Hi Ransomware Attacks

New Orleans Declares State Of Emergency Following Cyber Atta

Cyber-Attack Makes Pennsylvania Students Learn "Old School" Style

Hackers demand Michigan school district p $10K in bitcoin

Ransomware attack cancels classes at Thre College

ITI Technical College latest victim of ransom attack

Texas attack: Garrison, Nacogdoches schools hit ware

South Adams Schools hit with ransomware cyber-attack

Ransomware / Extortion Attacks

- The global threat of ransomware
  - Since 2016, over 4,000 ransomware attacks have happened daily in the U.S. (Justice Dept)
  - 37% of respondents' organizations were affected by ransomware attacks in the last year (Sophos, 2021)
  - In 2021, the largest ransomware payout was made by an insurance company at $40M, setting a world record (Business Insider, 2021)

Ransomware / Extortion Attacks

- SLTT/Government
  - In 2020, 33% of attacks on governmental bodies were ransomware (Security Intelligence, 2020)
  - A ransomware attack against a Southern city in 2020 cost over $7M (MSSPAlert, 2020)
  - A ransomware attack struck an East coast city in 2019 and caused a loss of over $18M (Baltimore Sun, 2019)
  - In 2019, attacks against municipalities increased 60% from the year before (Kaspersky Labs, 2019)

Ransomware / Extortion Attacks

- Things will likely get worse.
  - Driven by organized crime
  - Well-developed monetary ecosystem around these attacks
  - Every successful attack gives ransomware groups bigger budgets
  - Bigger budgets means more of an ability to develop or buy better exploits and tools

https://doublepulsar.com/the-hard-truth-about-ransomware-we-arent-prepared-it-s-a-battle-with-new-rules-and-it-hasn-t-a93ad3030a54

Local Governments are Targeted. Why?

- Sheer number of American local governments – Over 90k units
  - 39k “General Purpose” Governments
  - 3K County Governments
  - 19K Municipal Governments
  - 16k Town or Township Governments
- Local governments store considerable amounts of sensitive information
  - Personally identifiable information (PII)
  - Contractual, billing and financial information
  - Data can be sold or held for ransom

Local Governments are Targeted. Why?

- Cybercriminals are very good at what they do
  - “Hacking” tools are becoming more effective and lower in cost
  - Poorly defended systems are even easier to breach
- Local governments operate under financial constraints that limit ability to implement:
  - Technology
  - Policies
  - Practices

https://icma.org/articles/pm-magazine/look-local-government-cybersecurity-2020

State and Local Government Employees Trained on Ransomware Prevention

38%

IBM Survey: https://newsroom.ibm.com/2020-02-27-IBM-Survey-Only-38-of-State-and-Local-Government-Employees-Trained-on-Ransomware-Prevention

Best Practices

Employee Security Awareness Training

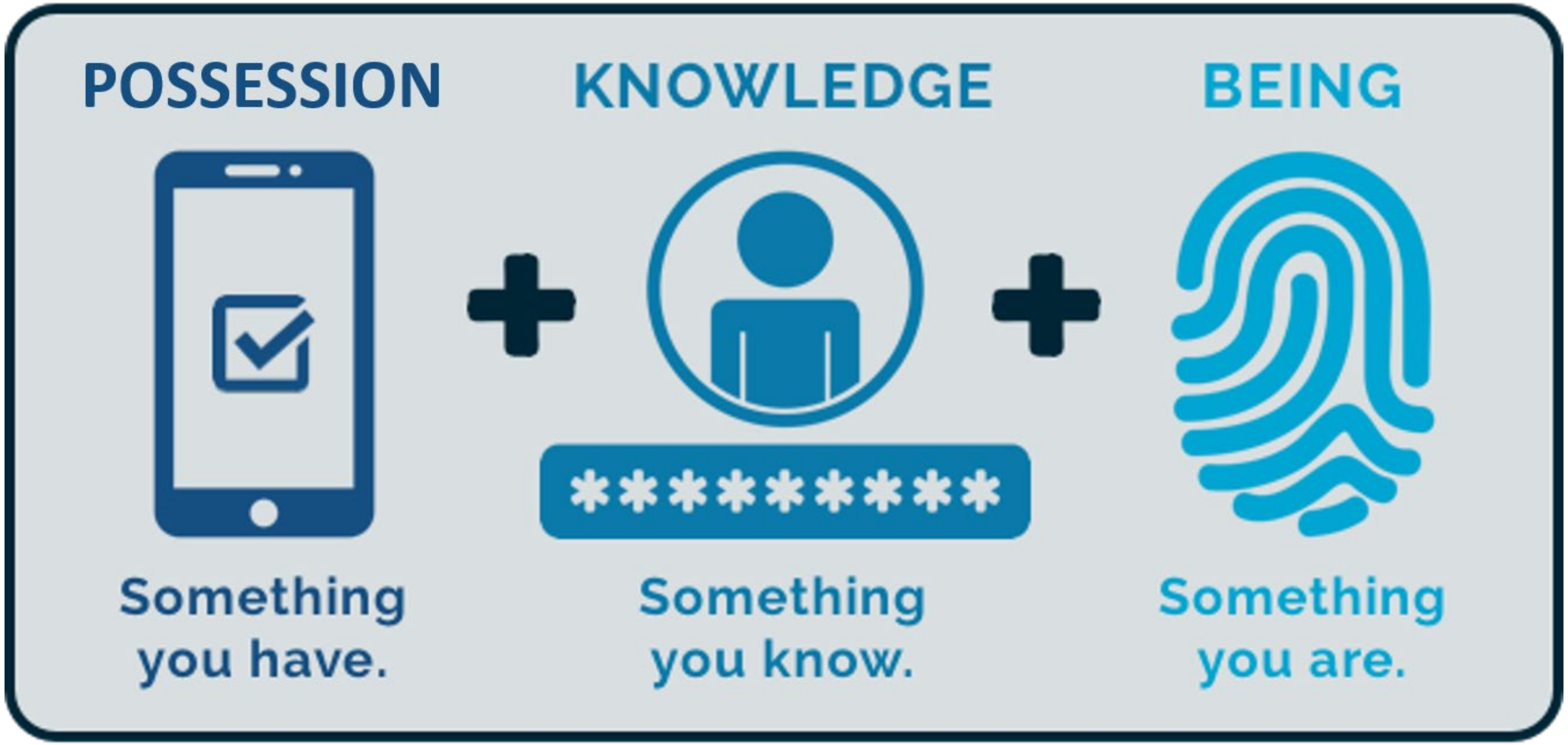
State of North Dakota Standard:

- Provide Information Security Awareness overview on the first day of employment
- Complete Security Awareness Training within three days of receiving computer access
- Complete annual refresher training
- Complete ongoing, brief training quarterly
- Disable system access if annual and quarterly training is not completed within 60 days

Passwords – Long and Strong

- 12 to 15 Characters long
- Upper, lowercase, numbers and special characters
- 15 characters and all 4 complexity requirements = 12-month life
- A weak 12-character password can be cracked in 25 seconds
- A strong 15-character Password? More than a Billion Years!

Multi-Factor Authentication (MFA)



POSSESSION

Something you have.

KNOWLEDGE

Something you know.

BEING

Something you are.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
IT Security
Supply Chain
OT Security
Insider Threat
Physical Security
Interoperable Communications
Sign Up for a .gov Domain
DEFEND TODAY, SECURE TOMORROW
.COM ✗
.ORG ✗
.GOV ✓

.gov Domain

.gov is Secure

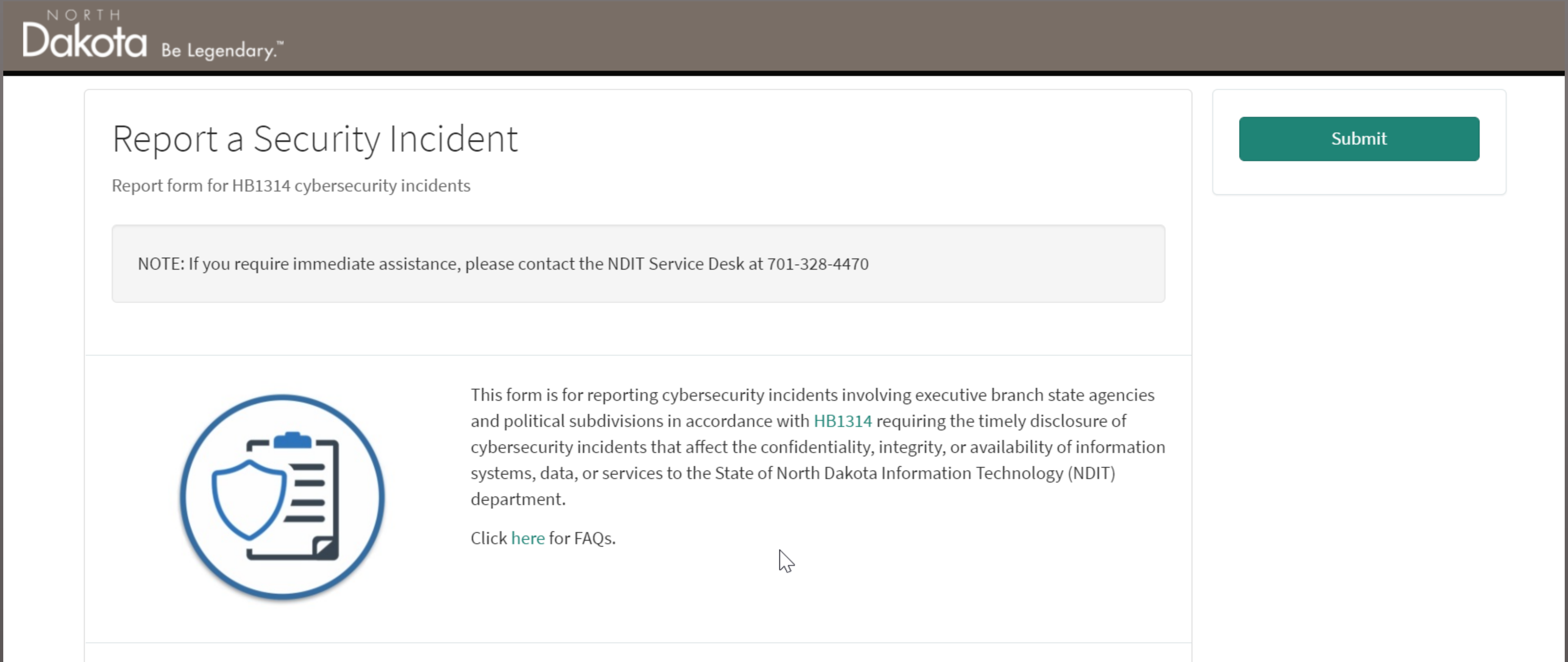
.gov is Trusted

.gov is Authoritative

Cybersecurity Incident Reporting/Plan

- Who you going to call?
- Create a cybersecurity awareness culture
  - Cybersecurity is everyone’s business
  - Encourage reporting – no shame or consequences
- Include Cybersecurity in COOP plan
- Exercise your Plan

Cybersecurity Incident Reporting



Report a Security Incident

Report form for HB1314 cybersecurity incidents

NOTE: If you require immediate assistance, please contact the NDIT Service Desk at 701-328-4470

This form is for reporting cybersecurity incidents involving executive branch state agencies and political subdivisions in accordance with HB1314 requiring the timely disclosure of cybersecurity incidents that affect the confidentiality, integrity, or availability of information systems, data, or services to the State of North Dakota Information Technology (NDIT) department.

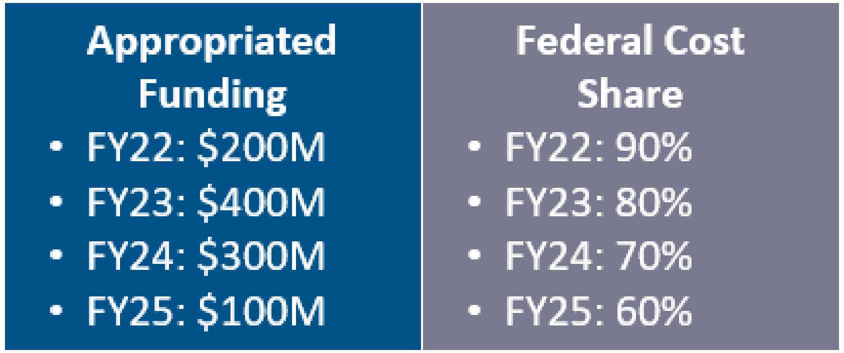
Click here for FAQs.

https://www.ndit.nd.gov/support/report-security-incident

IIJA Grant Funding

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

- Infrastructure Investment and Jobs Act (IIJA) amended Homeland Security Act of 2022 and appropriated $1B over 4 years
  - Funds appropriated to FEMA; CISA identified as subject matter expert
  - Baseline allocation plus population-based allocation formula
  - 80% passthrough to local entities
  - 25% of total state allocation must go to rural communities
  - Increasing SLTT cost share over time
- Eligible entities–States, territories, and tribes, with subawards made to local entities
- Multi-entity grants can be made to groups of eligible entities
- Defined uses of funds
  - Develop and revise Cybersecurity Plan
  - Implement Cybersecurity Plan (including individual projects)
  - Grant administration (5%)
  - Address imminent cybersecurity threats, as confirmed by the Secretary, acting through the Director of CISA
  - Fund any other appropriate activity determined by the Secretary, acting through the Director of CISA



Appropriated Funding	Federal Cost Share
• FY22: $200M	• FY22: 90%
• FY23: $400M	• FY23: 80%
• FY24: $300M	• FY24: 70%
• FY25: $100M	• FY25: 60%

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM REQUIREMENTS

PLANNING COMMITTEE

All eligible entities must establish a planning committee

Roles

- Develop, implement, and revise Cybersecurity Plans
- Approve Cybersecurity Plans
- Assist with determination of effective funding priorities (i.e., individual projects)

Required membership

- Eligible entity
- Local/counties (if eligible entity is a state)
- Representatives from varying densities
- Public education
- Public health
- 50% of members must have professional experience relating to cybersecurity or information technology

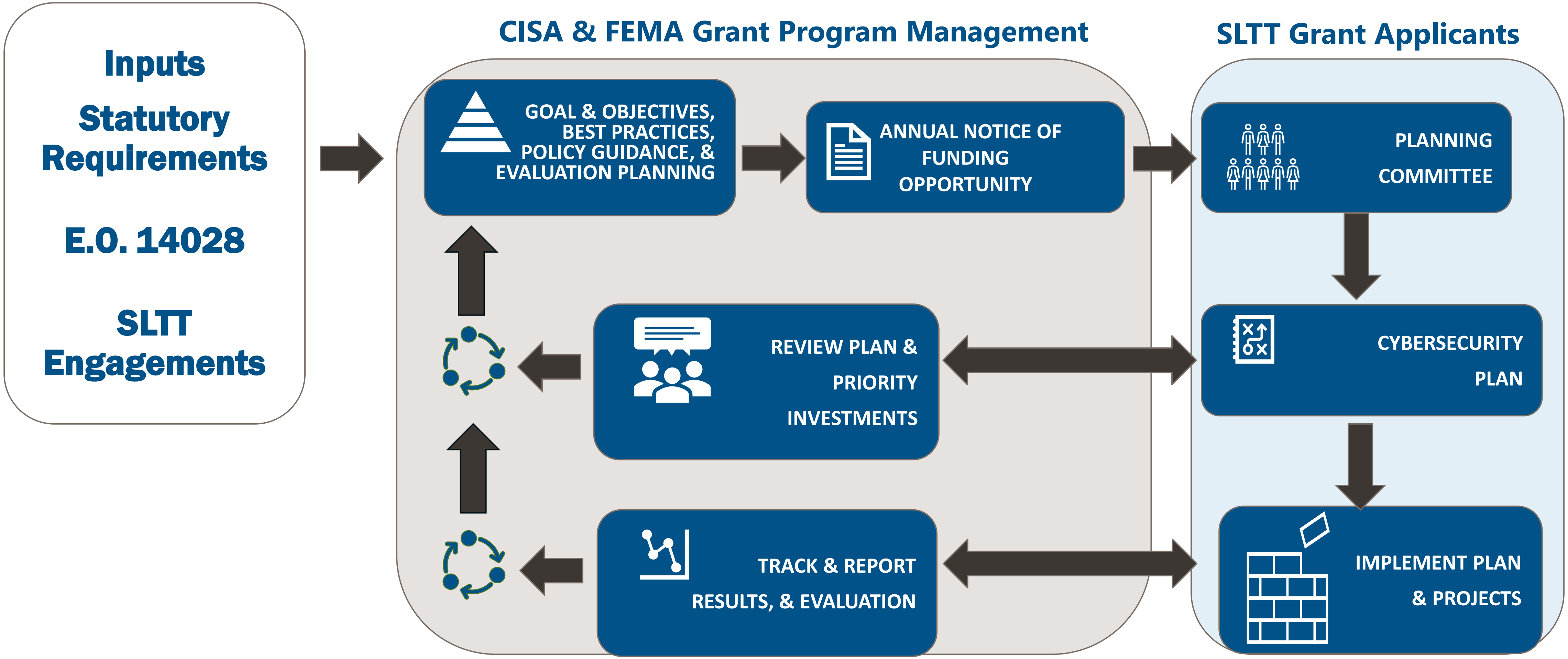
CYBERSECURITY PLAN

Mandates Cybersecurity Plan submission, approved by planning committee and state Chief Information Officer (CIO)

- 16 cyber-specific elements, including list of projects for SLCGP funding
- Description of SLTT roles in overarching plan
- Assessment of capabilities (16 elements)
- Resources and timeline for implementing plan
- Metrics

FEMA

STRATEGIC APPROACH LEVERAGES FEEDBACK LOOPS



Inputs

Statutory Requirements

E.O. 14028

SLTT Engagements

CISA & FEMA Grant Program Management

GOAL & OBJECTIVES, BEST PRACTICES, POLICY GUIDANCE, & EVALUATION PLANNING

ANNUAL NOTICE OF FUNDING OPPORTUNITY

REVIEW PLAN & PRIORITY INVESTMENTS

TRACK & REPORT RESULTS, & EVALUATION

SLTT Grant Applicants

PLANNING COMMITTEE

CYBERSECURITY PLAN

IMPLEMENT PLAN & PROJECTS

FEMA

CYBERSECURITY BEST PRACTICES

- Recipients may be required to include adoption of specific cybersecurity best practices in their Cybersecurity Plans
- Individual projects support implementation over time, as appropriate:
  - Implement multi-factor authentication.
  - Implement enhanced logging.
  - Data encryption for data at rest and in transit.
  - End use of unsupported/end of life software and hardware that are accessible from the Internet.
  - Prohibit use of known/fixed/default passwords and credentials.
  - Ensure the ability to reconstitute systems (backups).
  - Migration to the .gov internet domain.

2022 North Dakota Share

2.7M

IBM Survey: https://newsroom.ibm.com/2020-02-27-IBM-Survey-Only-38-of-State-and-Local-Government-Employees-Trained-on-Ransomware-Prevention

NDIT SERVICES

Cyber Liability and Data Breach Coverage

In response to the ever-changing cyber risk landscape due to the expanded use of technology and data, the NDIRF provides a comprehensive cyber coverage solution for NDIRF Members.

Each NDIRF member may receive up to a four percent (4%) general liability rate reduction by implementing the following cybersecurity services and practices: cyber maturity assessment, antimalware software, and vulnerability scanning service.

North Dakota Information Technology (NDIT) offers these cybersecurity services and practices at no cost to North Dakota schools, cities, and counties as part of its One State, One Cybersecurity initiative to help elevate the state's collective cybersecurity posture. Contact NDIT at (701) 328-4470 for more information or visit their online service portal Service-Now.com.

CYBER MATURITY ASSESSMENT

Cyber Maturity Assessment

- NDIT in cooperation with political subdivisions, is conducting a Cybersecurity Maturity Assessment (CMA) that will be used to gain insight into each political sub-division's capabilities to detect, prevent and respond to cyber-attacks.

- The NDIT Security Team has sent out electronic surveys in July. These Assessments are not an audit and are meant to establish a baseline for each agency that, evaluated collectively, will help us create a strategy to address gaps or vulnerabilities, ultimately helping elevate our cybersecurity posture statewide.

- CMA data will be used to identify key areas of need which will help determine how the IIJA grant funds will be used.

tenable®
network security

KnowBe4
Human error. Conquered.

HackNotice

CORTEX™ XDR
BY PALO ALTO NETWORKS

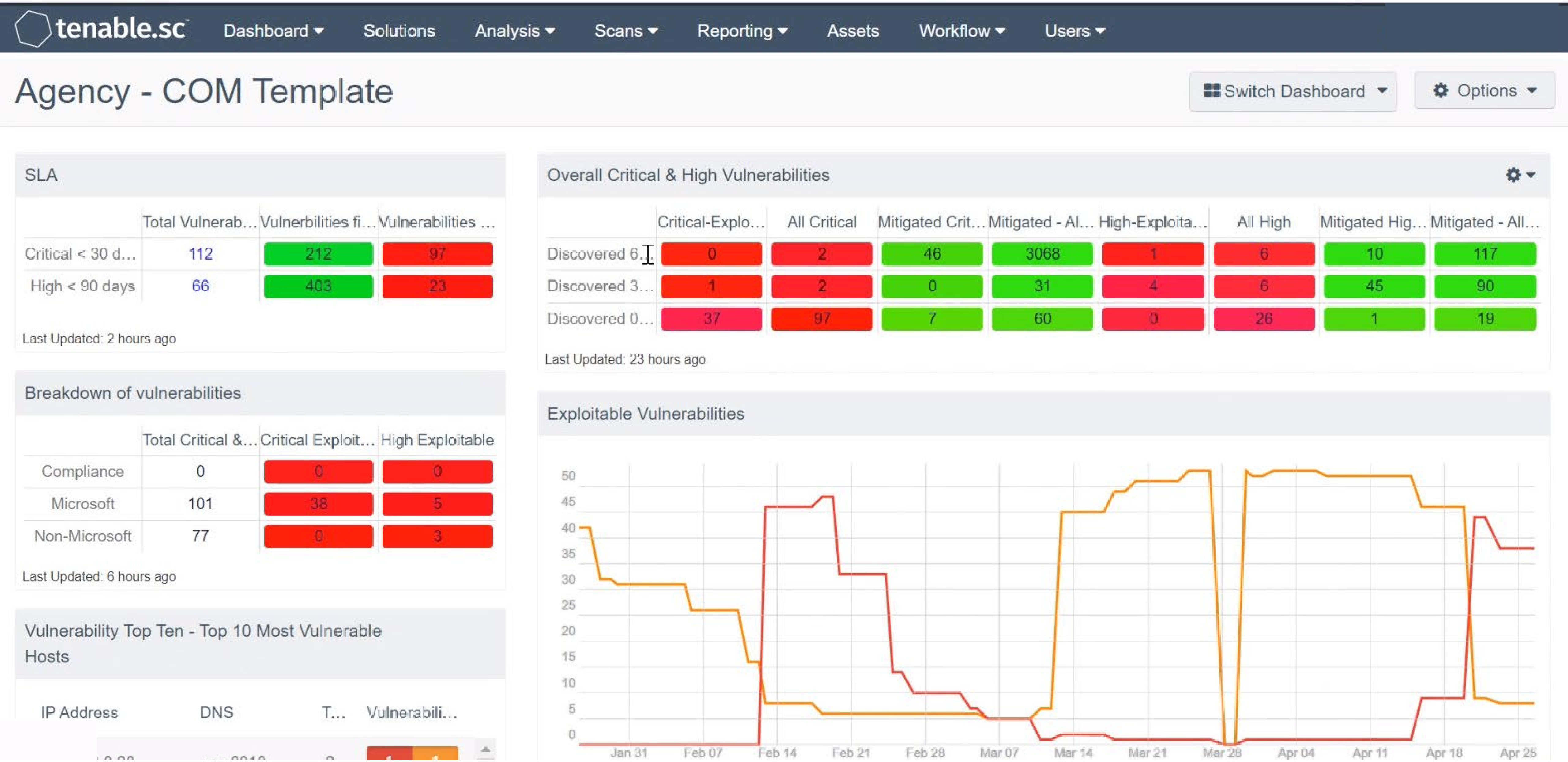
CORTEX™ XDR

BY PALO ALTO NETWORKS

- Advanced Endpoint Protection (AEP) Antimalware software
- Proactively protects devices from malware and malicious activity
- Team NDIT actively monitors systems
- System access at the local level
- Available for Windows, macOS, and Chromebooks
- Submit a ticket to the NDIT Service Desk
- **Available at no cost to gov’t entities**

tenable® network security

- Scans, identifies all software, including 3rd party, on each device
- Reports vulnerabilities and recommends actions for remediation
- Dashboards to easily see most critical vulnerabilities
- Clients available for Windows and macOS devices
- Submit a ticket to the NDIT Service Desk
- **Available at no cost to gov't entities**



Agency - COM Template

SLA

	Total Vulnerab…	Vulnerbilities fi…	Vulnerabilities …
Critical < 30 d…	112	212	97
High < 90 days	66	403	23

Last Updated: 2 hours ago

Overall Critical & High Vulnerabilities

	Critical-Explo…	All Critical	Mitigated Crit…	Mitigated - Al…	High-Exploita…	All High	Mitigated Hig…	Mitigated - All…
Discovered 6…	0	2	46	3068	1	6	10	117
Discovered 3…	1	2	0	31	4	6	45	90
Discovered 0…	37	97	7	60	0	26	1	19

Last Updated: 23 hours ago

Breakdown of vulnerabilities

	Total Critical &…	Critical Exploit…	High Exploitable
Compliance	0	0	0
Microsoft	101	38	5
Non-Microsoft	77	0	3

Last Updated: 6 hours ago

Exploitable Vulnerabilities

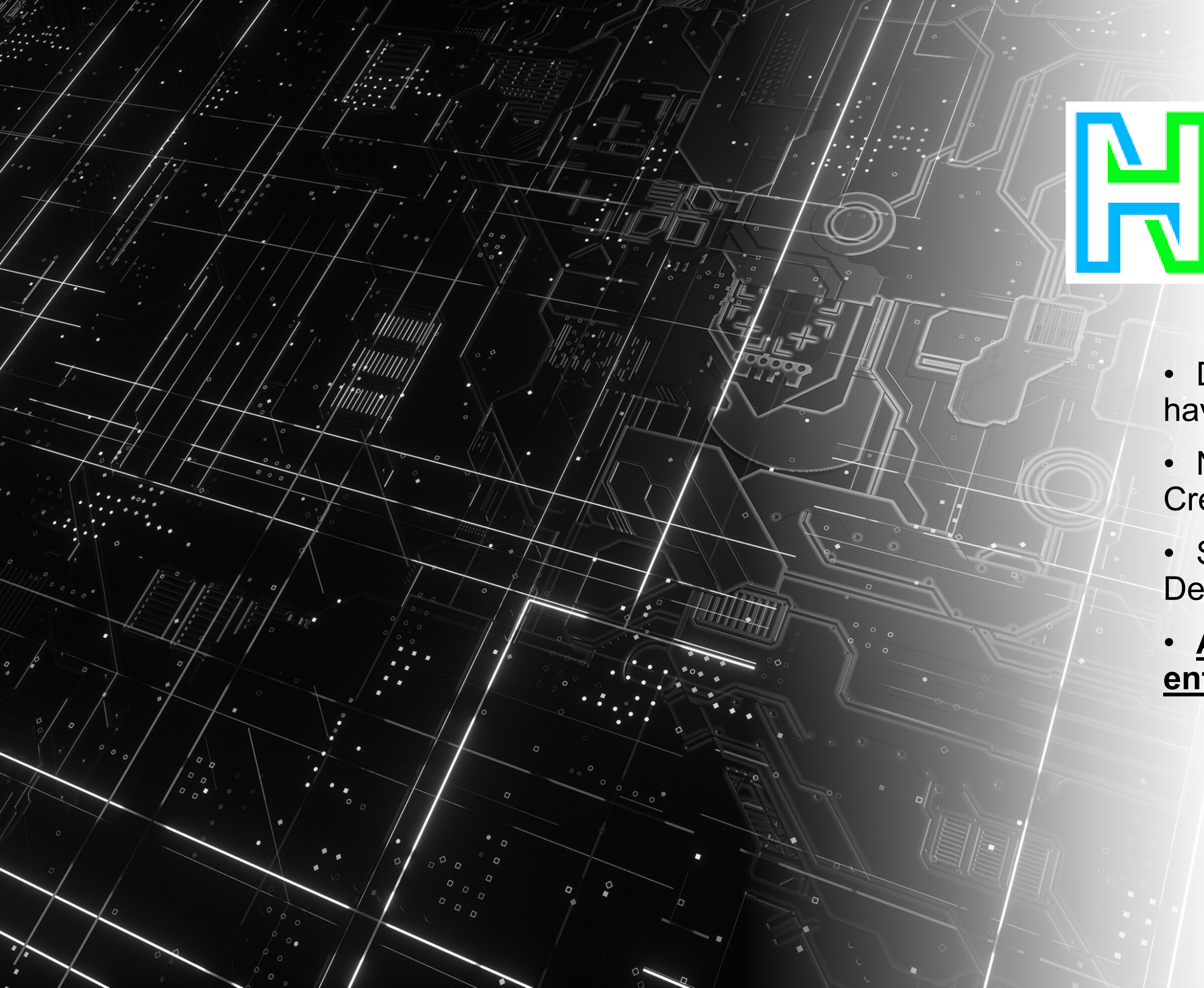
Vulnerability Top Ten - Top 10 Most Vulnerable Hosts

IP Address	DNS	T…	Vulnerabili…

Mean Time to Response

Detection and Notification During a Major Statewide Incident

Cortex XDR & Tenable	15 Minutes to 3 Hours
StageNet Only	24 to 72 Hours
No Visibility	5+ days to Never Detected



HackNotice

- Dark Web Monitoring for sites that have been breached
- Notification of Leaked Credentials for your Domain
- Submit a ticket to the NDIT Service Desk
- **Available at no cost to gov't entities**

KnowBe4

Human error. Conquered.

- End-User Cybersecurity Training
- Simulated Phishing Attacks
- Phishing Report Button for Outlook
- Submit a ticket to the NDIT Service Desk
- **Available at no cost to gov’t entities**

Security Awareness Education

- **90% plus of all data breaches begins with a phishing campaign**

- **Phishing Campaigns**
  - Crucial Education
  - Real world examples of today’s phishing threats
  - Phish Alert Button

- **Security Training Campaigns**
  - New Hire 45 Mins with Quiz
  - Annual training 15 – 30 Mins in length with Quiz
  - Microburst quarterly education courses are roughly 5 minutes
  - KnowBe4 training portal

KnowBe4
Human error. Conquered.