# Download materials featured in this session: LMC.ORG/ACMATERIALS





LEAGUE OF MINNESOTA CITIES 2025 ANNUAL CONFERENCE



### CONNECTING LEADERS CELEBRATING COMMUNITY



# JUNE 25-27 DULUTH

DULUTH ENTERTAINMENT CONVENTION CENTER

LMC.ORG/AC25

# MINNESOTA IT SERVICES

### Stronger Together: Embracing a Whole-of-State Cybersecurity Approach

Jen VanDemmeltraadt | Deputy Chief Information Security Officer

# Cybersecurity attacks in Minnesota

#### Local governments face increased cybersecurity threats and attacks

- A few of the cyber-attacks across Minnesota:
  - **2025:** A ransomware attack impacted a Minnesota municipality resulting in the shutdown of municipality services and police department.
  - 2024: A massive nationwide data breach at PowerSchool, an educational software provider, affected thousands of Minnesota students, from the metro area to Greater Minnesota.
  - 2023: A ransomware attack impacted 15 counties in west and northwest Minnesota, which all shared a system called CaseWorks.
- Communities that experienced incidents were not using Minnesota's cybersecurity tools

## MNIT's cybersecurity tools protect local entities

- How you prepare and defend your data and networks makes a difference
  - MNIT can help protect your technology, data, and systems to keep them running securely.
  - We work to make sure local entities, tribal government, education, public health, critical infrastructure, and peacekeepers have the cybersecurity tools and resources they need.







### Minnesota's Managed Detection and Response program

#### MDR protects Minnesota communities and private data



financial data, credit card processing information, public health information, student and school data

### Number of MNIT's MDR partners increases



Launch of

Navigators'

outreach

# Minnesota IT Services (MNIT)

#### MNIT is the central IT organization for the State and partners with:



• Executive branch: agencies, boards, councils, and commissions in the state. (Provides all IT services.)



 Non-executive branch: cities, counties, school districts, higher education, public libraries, legislative branch, judicial branch, constitutional offices, and other government organizations in the state. (Provides network services, security services, statewide leadership.)

### **MNIT**

#### Mission

We partner to deliver secure, reliable technology solutions to improve the lives of all Minnesotans.

#### Vision

An innovative digital government that works for all.

#### **Customers/Partners**

- Cities
- Counties
- Townships
- School districts
- Public libraries
- Higher education
- Judicial branch
- Legislative branch
- Constitutional offices
- Cabinet-level state agencies
- Non-cabinet boards, councils and commissions



### MNIT has more than 2,800 staff members who:



Support over 41,000
end users for over
70 agencies/boards



Secure and manage over 2,700 agency applications and a statewide network connecting 3,000+ locations



**Oversee** and deliver over **490** projects with major IT components



Manage over \$470M IT budget for project/program delivery **Resolve 38,000+** service desk tickets a month with a **4.7** (1-5 scale) satisfaction rating

**P** Detect and resolve

over **5,200** security incidents a year

### Minnesota's Network for Enterprise Telecommunications (MNET)

Twin Cities

#### MNIT's wide area network (WAN) service that connects sites to the state network

- Connects all 87 counties, 300 cities, and 200 public higher education campuses.
- Backbone speeds are up to 100Gbps, with up to 1Gbps wire speed to the desktop in most locations.
- MNIT and its predecessor agencies have been serving local governments with network services since the early 2000s.

## What it means to be on MNET

Enables secure, reliable connectivity and support for data communications between agency sites, MNIT Enterprise data centers, external party sites, and to the internet.

- Baseline cybersecurity capabilities, including:
  - Incident response
  - DDoS & Radware
  - Cyber threat intelligence
- 24/7 service desk
- 24/7 network monitoring
- Network hardware lifecycle management



### Minnesota cybersecurity investments

#### Security infrastructure

- Modernize Security Operation Center
- Expand implementation of web application firewalls
- Implement autonomous threat prevention

#### • Balancing security, fraud protection, and user experience

- LoginMN enterprise-wide identity service
- Mature governance, risk, and compliance program
- Advance vendor risk management program

#### • Whole-of-state approach

- New grant-subsidized services for local governments
- Mandatory cybersecurity incident <u>reporting</u>
- Partner with local and federal entities to deliver services







# Minnesota's Whole-of-State Cybersecurity Approach

Peter Alsis | MNIT Cyber Navigator Supervisor Foua Xiong | MNIT Cyber Navigator

### Minnesota Cybersecurity Task Force

Advisory body that contributes to the development and implementation of a statewide cybersecurity plan to advance cybersecurity protections for Minnesota.

- 15 members represent counties, cities, K-12 schools, tribal government, and private sector.
- Task force meets every other month; meetings are public. Next meeting is July
- <u>Cybersecurity Task Force</u> has three subcommittees:
  - Baseline Cybersecurity Capabilities
  - Advanced Cybersecurity Tools and Capabilities
  - Critical Infrastructure



# Whole-of-State Cybersecurity Plan

- MNIT partnered with the Cybersecurity Task Force to develop the <u>Whole-of-State Cybersecurity Plan</u>
- Uses an all-of-state approach to address critical cybersecurity needs for Minnesota local governments, K-12 schools, critical infrastructure, and Tribal Nations.
- Leaders at every level of government work together, and share resources and information to create a united front against cyber threats



# Federal, state funding subsidize cybersecurity services

#### Minnesota's Whole-of-State funding for cybersecurity services

- MNIT provides subsidized cybersecurity services to local governments – meeting them at their level.
- Goal: Place little to no burden on entities that might not have staff or resources to invest in advanced security tools.



### Minnesota Whole-of-State cybersecurity goals

# Minnesota Cybersecurity Task Force approved four goals to build a solid foundation for a long-term, sustainable cybersecurity system.



1. Mature cyber capabilities throughout the state



2. Increase participation in programs and services known to work



3. Collaborate and share information throughout the state



4. Strengthen the cyber-resiliency of critical infrastructure

# Cyber Navigator program

- Three cyber navigators and a supervisor supporting cities, townships, critical infrastructure cybersecurity.
- Assists local governments in risk assessments, policy development, and response planning.
- Helps districts implement security best practices and access resources.
- Connects local government with CISA's cyber hygiene services.
- Contact Cyber Navigator Team at <u>CN.MNIT@state.mn.us</u>



# **Cyber Threat Intelligence**

#### Cyber Navigators

- Connect local governments with resources and tools to bolster their cyber defenses
- Collaborate with federal, state, and local government partners to identify the threat landscape in Minnesota
- Centralize feeds
- Dedicated resource
- Proactive intelligence gathering
- Processing event data (IOCs, TTPs, reporting)
- Collaboration & representation



# **Risk Assessments**







#### **Metro State University**

- Center for Internet Security's Critical Security Controls
- Implementation Group 1 Essential Cyber Hygiene
- Risk Assessment Methodology Continued collaboration
- https://www.metrostate.edu/mncyber/clinic

#### **Cybersecurity and Infrastructure Security Agency**

- Cybersecurity Advisors
- Cybersecurity Performance Goals
- Ransomware Readiness Assessment
- Onsite

# Managed Detection and Response (MDR) Program

#### Grant-subsidized cybersecurity service available to local governments

- Fully managed, anti-virus tool to detect security risks and malicious activity
- 24/7/365 monitoring
- Rapid detection and containment
- Average response time ~ 7 minutes
- MNIT's Security Operations Center support and visibility
- MNIT and law enforcement collaboration
- Full remediation support, incident warranty



### MDR works 24/7 to protect sensitive data

#### MNIT's MDR program safeguards the integrity of Minnesota's data

- Local government records
- Public health records K-12 schools' systems, student data • Critical infrastructure Credit card Tax and real (water and wastewater information estate records facilities) resources County Student and ୍ଥିତ ..... school data financial data

# Value of MNIT's MDR Program

#### MDR looks for and blocks the types of attacks that could lead to data breaches, ransomware

- Reduces operational disruption
- Low-cost, high-value solution
- Cost-sharing model

#### MDR cost structure per device

2025	\$22
2026	\$32
2027	\$38
Post-SLCGP	TBD

\*per device annually; current rates



COMPLETENESS OF VISION  $\longrightarrow$ 

Magic Quadrant for Endnoint Protection Platforms

## **MDR Cybersecurity Detections**

### MNIT's MDR prevented threats (past 90 days)

- Critical: 31
- High: 512
- Medium: 265
- Low: 12,415



#### **Detections (Past 90 Days)**

### **MDR** Partners



\*MDR totals include entities who are onboarding but not yet active; currently eight (8) total

\*\* Interested entities have expressed interested but have not yet started the onboarding process  $_{6/18/2025}$ 

# **Cybersecurity Incident Reporting**

#### Reporting tool: <u>mn.gov/mnit/cir</u>

- Law took effect Dec. 1, 2024.
- Standardizes reporting protocols.
- State may collect information about cybersecurity incidents, anonymize it, and share it with appropriate organizations to strengthen cyber defenses statewide.

About MNN       Cybersecurity Incident Reporting Online Form         Who We Are       Incident point of contact         Strategic Plan       Incident point of contact         Geographial       Incident point of contact         Budget       Incident point of contact         Accessibility       Incident point of contact         Geographial       First Name         Security       Incident Reporting         Whole of State Plan       Vork email*         Work end Questions       Vork email*         Constration & Strategy Delivery       Job title*         Careers       Reports and Plans         Cornate Us       Work phone*         Ornate Us       Impacted organization         Accessibility bis incident on behalf of another organization?	Who We Are         Strategic Plan         Leadetship         Governance         Burget         Accessbility         Geospatial         Security         Security in cident Reporting         Frequently Kaked Questions         Goossary         Transformation & Strategy Delivery         Carers         Reports and Plans         Contact Us	Wine We Are         Stretegic Plan         Leadership         Governance         Budget         Accessibility         Geospasial         Security         Security         Whole of State Plan         Whole of State Plan         Whole of State Plan         Work email*         Description         Gossary         Frequently Asked Questions         Gossary         Careers         Reports and Plans         Cormative s and Councils         Contact Us         Impacted organization	About MNIT For Government For Med			
Leadership       Incident point of contact         Governance       Budget         Budget	Leadership       Incident point of contact         Governance       Name*         Accessibility       Image:	Leadership       Incident point of contact         Governance       Name*         Accessbility       Image: I	Who We Are	Cybersecurity Incident	Reporting Online For	m
Governance         Budget         Accessibility         Geospatial         Security         Whole-of-State Plan         Work emails*         Vincensity Distorse Program         Frequently Asked Questions         Gossary         Transformation & Strategy Delivery         Careers         Reports and Plans         Contract Us         Impacted organization	Governance       Burget         Burget       Name*         Accessbility       End         Geospatal       First Name         Security       Eirst Name         Whole-of-State Plan       Work email*         Work email*       United Questions         Goossay       Goossay         Transformation & Strategy Delivery       Job title*         Careers       Work phone*         Constact Us       Work phone*         Impacted organization       Impacted organization	Governance         Budget         Accessbility         Geospaial         Security         Whole-of-State Plan         Work email*         Verk email*         Gossary         Transformation & Strategy Delivery         Garders         Reports and Plans         Committees and Councils         Contact Us         Impacted organization		Incident point of contact		
Accessbility         Geospatial         Security         Whole of State Plan         Vulnerability Disclosure Program         • Cybersecurity Incident Reporting         Frequently Asked Questions         Glossary         Greers         Reports and Plans         Cornnittees and Councils         Contact Us         Impacted organization	Accessbility         Geospatial         Security         Whole-of State Plan         Work email*         Verk email*         Verk email*         Job title*         Transformation & Strategy Delivery         Careers         Reports and Plans         Corntact Us         User blance         Umpacted organization	Accessibility         Geospatial         Security         Whole-of-State Plan         Work end State Plan         Security Indient Reporting         Frequently Asked Questions         Globasty         Job title*         Security Indient Reports and Plans         Contact Us         Umpacted organization				
Security     First Name     Last Name       Whole-of-State Plan     Work email*       Vulnerability Disdosure Program     Impacted organization	Security     First Name     Last Name       Whole-of-State Plan     Work email*       Vulnerability Disclose Program        S Optimizeuruhy Insident Reporting        Frequently Asked Questions        Glossary     Job title*       Transformation & Strategy Delivery        Careers        Reports and Plans     Work phone*       Contact Us	Security     First Name     Last Name       Whole-of-State Plan     Work email*       Vulnerability Disclosure Program				
Whole-of-State Plan       Work email*         Vulnerability Disdoure Program          Cyberseurity Indext Reporting          Frequently Keed Questions          Glossary       Job title*         Transformation & Strategy Delivery          Careers          Reports and Plans          Committees and Councils          Centact Us          Impacted organization	Whole-of State Plan     Work email*       Vulnerability Disclosure Program        > Cybersecurity incident Reporting	Whole-of State Plan       Work email*         Vulnerability Disclosure Program          Cyberseurity Indicet Reporting		First Name	Last Name	
Vulnerability Disdoure Program         Cybersecurity Insident Reporting         Frequently Asked Questions         Glossary         Transformation & Strategy Delivery         Careers         Reports and Plans         Committees and Councils         Contact Us         Impacted organization	Vulnerability Disclosure Program         S Opherscurity Incident Reporting         Frequently Acident Reporting         Glossary         Transformation & Strategy Delivery         Carers         Reports and Plans         Committees and Councils         Contact Us         Impacted organization	Vulnerability Disclosure Program         Cybersecurity Insident Proporting         Frequently Asked Questions         Grossary         Transformation & Strategy Delivery         Carcers         Reports and Plans         Committees and Councils         Contact Us         Impacted organization		Mark om silt		
Frequently Asked Questions       Glossary       Transformation & Strategy Delivery       Careers       Reports and Plans       Committees and Councils       Contact Us   Impacted organization	Frequently Asked Questions       Glossary       Transformation & Strategy Delivery       Careers       Reports and Plans       Constact Us   Work phone* Impacted organization	Frequently Asked Questions       Glossary       Transformation & Strategy Delivery       Careris       Reports and Plans       Committees and Councils       Contract Us    Impacted organization	Vulnerability Disclosure Program	work email*		
Giossary     Job title*       Transformation & Strategy Delivery	Clossary       Transformation & Strategy Delivery       Carers       Reports and Plans       Committees and Councils       Contact Us    Impacted organization	Giossary       Transformation & Strategy Delivery       Careers       Reports and Plans       Committees and Councils       Contact Us    Impacted organization				
Transformation & Strategy Delivery Careers Reports and Pians Committees and Councils Contact Us Impacted organization	Transformation & Strategy Delivery Careers Reports and Plans Committees and Councils Contact Us Impacted organization	Transformation & Strategy Delivery Careers Reports and Plans Committees and Councils Contract Us Impacted organization		Job title*		
Reports and Plans Committees and Councils Contact Us Impacted organization	Reports and Plans Committees and Councils Contact Us Unpacted organization	Reports and Plans Committees and Councils Contact Us Impacted organization	Transformation & Strategy Delivery	Job dile		
Committees and Councils Contact Us Impacted organization	Contact Us Work phone* Impacted organization	Contract Us Work phone* Impacted organization				
Impacted organization	Impacted organization	Impacted organization		Work phone*		
Impacted organization Are you submitting this incident on behalf of another organization?	Impacted organization Are you submitting this incident on behalf of another organization?	Impacted organization Are you submitting this incident on behalf of another organization?	Contact Us			
Impacted organization Are you submitting this incident on behalf of another organization?	Impacted organization Are you submitting this incident on behalf of another organization?	Impacted organization Are you submitting this incident on behalf of another organization?				
Are you submitting this incident on behalf of another organization?	Are you submitting this incident on behalf of another organization?	Impacted organization		in and ergapization		
Are you submitting this incident on behalf of another organization	Are you submitting this incident on behalf of another organization.	Are you submitting this incident on behalf of another organization.		Impacted organization	station?	
				Are you submitting this incident on beh	alf of another organization.	
					COLUMN ADDRESS OF THE OWNER OF	
		AND A REAL PROPERTY AND A REAL		Are you submitting una		
		and the second sec	2 10 20			200
			1. 200	and the second	2 2 2 2	
			lever m		2. 2. 2. 2	
			the second		2 - 2 - 2	and the second
	THE OWN OWN OWN OWN OWN OWN OWN OWN	and the second	12	and the state of the	the rest was not	
		the stand and the stand of the stand of the stand of the	le se	the the state		
E state to be be be and	En al the state of the set	the state of the second state of the second	the form		Contraction of the second	
Propher and a start of the star	E the state of the state	lie the for the for the star to the start the				
Contra a a a a a a a a a a a a	Contractor of the second	le state to to to to to to to				
a a proto to to to to to to to	E the trade of the	le the the for the source of the the				
C 22 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	C. S.	le the the for the source of a last				

### Non-Executive Branch Cybersecurity Incident Reports



Total YTD: 154

(Current as of 27 May 2025)

### Cybersecurity Incident Reporting Requirements

#### Who must report

- State agencies, political subdivisions; school districts, charter schools, intermediate districts, cooperative units, and public post-secondary (higher education) institutions.
- Government contractors or vendors that provide goods or services to a public agency must report an incident to the public agency.

#### When to report

- Within 24 hours if Criminal Justice Information is impacted.
- Within 72 hours of when incident was identified or occurred.

Reporting tool: <u>mn.gov/mnit/cir</u>

# **Cybersecurity Incidents To Report**



#### What to report:

Cybersecurity incidents that impact services, systems, or people.

#### **Types of incidents to report:**

- Compromised account/password
- Defacement
- Denial of service
- Malware
- Network attack
- OT/ICS/SCADA

- Potential data exposure
- Ransomware
- Social engineering
- Unauthorized access
- Web application attack

### **Protected Information**

#### **Reported cybersecurity incidents are:**

- Security information pursuant to section 13.37.
- Not discoverable in a civil or criminal action absent a court order or a search warrant.
- Not subject to subpoena.

#### **MNIT or BCA may:**

• Anonymize and share cyber threat indicators and relevant defensive measures to help prevent attacks.



• Share cybersecurity incident notifications with potentially impacted parties through cybersecurity threat bulletins or relevant law enforcement authorities.

# **Cybersecurity Incident Reporting Benefits**



Shared information can help prevent other cyber attacks from occurring or help other organizations better remediate attacks.

#### Minnesotans

• Gain a better understanding of the nature of and impacts from cybersecurity events.

#### **MNIT and BCA**

- Gain awareness of the scope of incidents.
- Assist organizations in defending their IT resources.
- Understand how bad actors bypass security controls.
- Track and identify trends in cybersecurity incidents.

#### **Public entities**

 May receive advisories or guidance from MNIT/BCA to help defend against cybersecurity threats.

#### **Public leaders**

- Gain improved quality of data related to cybersecurity risks.
- Able to better identify potential gaps that require resources to mitigate risk.



Join Us October 21-22, 2025 at the Minneapolis Marriott Northwest

**New this year**: Step into the **Public Sector Village on Wednesday, Oct. 22**, to explore hands-on cybersecurity tools and shared services available to Minnesota's public entities.

- Learn how local governments, schools, and utilities can leverage no-cost and discounted resources for system hardening, detection and response, and incident support.
- See demonstrations, walk-throughs, and real tools in use across the state.
- All summit attendees are welcome to tour the Village.
- Hosted by Minnesota National Guard C3 and MNIT.

**Also new**: Two **SLTT Cyber101 classes** will provide State, Local, Tribal & Territorial personnel and school personnel with the fundamentals of cyber security.

• There will be time before or after class to visit the Public Sector Village.



# Questions?

#### **Minnesota IT Services**

jen.vandemmeltraadt@state.mn.us

peter.alsis@state.mn.us

foua.xiong@state.mn.us

Cyber Navigator Team: CN.MNIT@state.mn.us



# Thank you!



### CONNECTING LEADERS CELEBRATING COMMUNITY



# JUNE 25-27 DULUTH

DULUTH ENTERTAINMENT CONVENTION CENTER

LMC.ORG/AC25