

Collaboration is Key to Unlock Minnesota's Whole-of-State Security Potential



State of Minnesota: Minnesota IT Services

Category: Cross-Boundary Collaboration & Partnerships

Initiated: October 2022

Completed: September 2023

Kendall Johnson

Director of Communications

kendall.johnson@state.mn.us

(C) 651-334-1760

Executive Summary


Before Minnesota IT Services (MNIT) launched its Whole-of-State Cybersecurity Plan in September 2023, our state had a disparate approach to protecting the private data of Minnesotans against ever-evolving cyber threats and attacks. While successful programs like the Statewide Security Monitoring Initiative (SSMI) and Minnesota’s Network for Enterprise Telecommunications (MNET) increased the number of entities protected and started communication pathways, there were large gaps in our security net that attackers could exploit.

The growing number of cyber-attacks against schools, local governments, and critical infrastructure required a different approach. When Minnesota received federal funding through the State and Local Cybersecurity Grant Program (SLCGP) to strengthen cyber resiliency, we took a bold step forward.

While other states distributed SLCGP funding in a traditional manner, we took the opportunity to build a whole-of-state approach that matured cyber capabilities throughout the state, increased participation and collaboration on programs and services, and partnered with local government entities across Minnesota.

By focusing on partnerships and collaboration, we improved threat protections and rolled out successful pilot programs for risk assessments with organizations like Metro State University. The impact of this funding and statewide collaboration on cybersecurity in Minnesota is one of the biggest in the country.

Why it matters: MNIT launched a unique whole-of-state approach to maximize a strategic use of funding, leading to pilot programs that mitigate risk and strengthen cyber-defenses across the state.

 **Statewide entities engaged in plan:** 562

 **Eligible K-12 public schools improving cybersecurity posture:** 40%

 **New endpoints protected:** 85,000

 **High alerts mitigated:** 130+

 **Initial software cost savings:** 100%



Idea

Reports of data breaches and ransomware attacks have become commonplace, including within our schools and local government. Hackers' ability to move laterally within the IT environment while evading detection can lead to disastrous results for communities and governments.

MNIT builds, maintains, and secures the state's IT infrastructure, applications, and services in partnership with all levels of government. Minnesota is one of a few states in the U.S. with a dedicated, statewide network – MNET – that connects branches of government, plus all 87 counties and 1,500+ locations that serve cities, public safety, health care, Tribal Nations, K-12, education consortiums, and 200 public education and higher education campuses, including the University of Minnesota, and Minnesota State Colleges and Universities.

MNIT helps eligible entities secure data that Minnesotans have entrusted to their organization by thoughtfully and strategically using two main funding sources: SSMI, which delivers cybersecurity resources and programs to Minnesota Tribal Nations, port cities, and all 87 counties; and SLCGP, which funds initiatives that strengthen the cyber resiliency of Minnesota entities, including cities, towns, public schools, and government-affiliated critical infrastructure. However, every organization is at a different place in its cybersecurity maturity, and our defenses are only as successful as those of each organization. Therefore, we needed to take a whole-of-state approach to strengthen Minnesota's joint cybersecurity chain.

An Executive Order

In August 2022, Governor Tim Walz signed [Executive Order 22-20](#), instructing state entities responsible for regulating critical infrastructure providers to identify and concentrate resources on safeguarding Minnesota's critical infrastructure.

Additionally, it highlights the importance of securing state government cyber defenses, preparing for cyber-attacks, and identifying opportunities to enhance state cybersecurity. This order set the stage for MNIT to take a larger role in the coordination and delivery of cybersecurity services statewide.

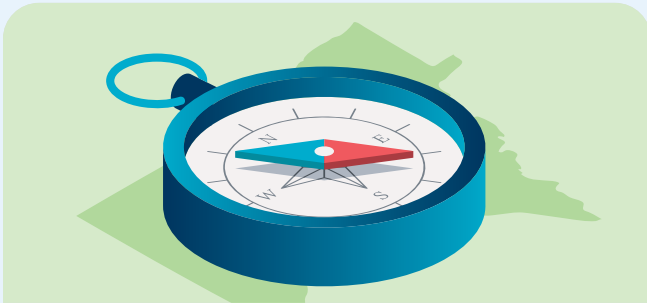
The Whole-of-State Plan

The Whole-of-State Plan was Minnesota's first statewide cybersecurity plan; and MNIT uses it as the framework for developing and delivering cost-efficient, sustainable, advanced technologies with federal and state funding.

Our partners widely applauded the Whole-of-State Plan, garnering positive media coverage with over 22 articles and TV/radio interviews, including the [Star Tribune](#) and [WCCO-TV](#).



The Cybersecurity Plan includes four goals approved by the Task Force and our federal partners.



1. Mature cyber capabilities throughout the state: Roll out resources, equipment, and training.



2. Increase participation in programs and services known to work: Include new participants and provide better service offerings.



3. Collaborate and share information throughout the state: Bring together cybersecurity information under one umbrella that previously was maintained in separate silos.



4. Strengthen the cyber-resiliency of critical infrastructure: Create and deliver cybersecurity services for local water and wastewater systems.



As schools experience more cybersecurity incidents, we can't assume that schools can do more with less. The plan is the result of long discussions at the task force about how we can use the new funding to bridge the affordability gap for cybersecurity measures in underfunded schools across the state.

-Nicole Pruden

Minnesota Cybersecurity Task Force Education Sector Member,
ECMECC Network and Security Administrator

Implementing Statewide Collaboration

MNIT formed the [Minnesota Cybersecurity Task Force](#) in October 2022, which is made up of 15 members, who represent many of our partners: counties, cities, townships, Tribal Nations, and K-12 schools, as well as private sector IT experts. After a year of collaboration with the Task Force, [MNIT launched the Whole-of-State Plan](#) in September 2023.

Cyber Navigators Play Pivotal Role

The Cybersecurity Task Force saw the importance of developing strong connections with our local government partners and partnered with MNIT to quickly hire Cyber Navigators. MNIT's Cyber Navigators were key to:

- **Customer experience:** They triaged questions after the plan launched and the rollout of two pilot programs. They formed relationships with entities to ensure positive and successful interactions.
- **Solution adoption:** They conducted listening sessions with vendors, led sessions with partners to address concerns, and served as liaisons between MNIT, vendors, and our local government partners.
- **Best practices:** They are members of groups that share knowledge with other states.

Delivering Cybersecurity Resources

With the plan's release, MNIT launched an awareness campaign encouraging eligible entities to complete a survey to describe their concerns and interest in shared services. We provided more information about the plan on [MNIT's public site](#), including a [participant guide and FAQs](#). One month after launch, 300 entities had completed the survey. To date, that number is 562 entities.

Survey respondents expressed a need for enterprise-grade tools and services. With the Task Force's guidance, MNIT prioritized, developed, and delivered two pilot programs to enhance local governments cyber resiliency:

- **Managed detection and response (MDR):** Onboarded 125 entities (K-12 schools, cities, towns, and critical infrastructure) that enrolled in our early adopter program to protect up to 85,000 endpoints.
- **Security risk assessments:** Partnered with Metro State University to conduct risk assessments of entities' cybersecurity posture and provide meaningful recommendations to mitigate risk.

Managed Detection and Response

MDR is an advanced antivirus solution that can identify attacks that could lead to data breaches, ransomware, or other major events if not detected and blocked. When MNIT launched a pilot MDR program, 125 eligible organizations volunteered to become early adopters. They received a free six-month enterprise-grade MDR tool funded by the Whole-of-State Plan, with the option to continue at a subsidized cost.

The MDR vendor team managed and actively monitored the platform, investigated detections and incidents, and remotely remediated malicious activity 24 hours a day, 7 days a week, 365 days a year.

The result: Up to 85,000 new endpoints are protected through this program statewide.



Security Risk Assessments

MNIT partnered on a security risk assessment pilot program with [Metro State University](#) (MSU) in St. Paul, Minnesota, which has undergraduate and graduate cybersecurity programs. MNIT and the Cyber Navigators collaborated with a group of CompTIA Security+ certified students to launch the pilot program with **seven entities that represent K-12 schools, city, and county government.**

MNIT Cyber Navigators provided training to MSU students and faculty. Risk-assessment meetings were set up with each entity's key personnel for MSU students to assess the maturity of 56 cybersecurity safeguards within that organization using the Center for Internet Security's (CIS) Risk Assessment Methodology (RAM).

To ensure a smooth and efficient risk assessment process:

- All information was treated confidentially. Any non-public data was handled securely.
- MSU students compiled their findings for each entity into a Security Risk Assessment report with an analysis of potential risks they could address to enhance organizational cyber resilience.
- MNIT and MSU staff reviewed and guided the students' reporting process.

This collaboration brought significant value to local governments, students, and the broader community: MSU students applied their academic knowledge and gained practical experience; pilot participants gained innovative ideas, while they supported the development of the next generation of cybersecurity professionals.

Partnerships Result in Widespread Impact

Through the Whole-of-State Cybersecurity Plan, the number of entities that are now protected through advanced tools or plugged into information sharing has proven its value. In the past, MNIT programs primarily focused on counties and tribal governments. Today, public schools, cities, and towns, as well as government-affiliated critical infrastructure are within scope.

The dialogue that is taking place is unprecedented and transcends local, state, and federal government. New ideas and initiatives are taking form as the cybersecurity environment is coalescing behind these efforts.

Here is what a few of our early partners said about MDR and our whole-of-state approach:

- **Steele County:** *Genuinely appreciate working with (the whole-of-state project). Also appreciate having access to (training). That is helping to make sense of that environment.*
- **City of Woodbury:** *The implementation process unfolded precisely as communicated, swift, and flawless. This added layer of oversight brings us a sense of security ... recognizing the imperative nature of round-the-clock monitoring and remediation for cybersecurity incidents.*
- **Milaca K-12 School District:** *The integration (of MDR) was seamless. It has only been a few weeks since the sensors were installed, and we have already had instances where the MDR stopped a user from accessing a bad URL. The product and support have been great.*

Highlighting the Successes of Whole-of-State Plan

The key to the success of Minnesota’s Whole-of-State Cybersecurity Plan is outreach, partnership, and understanding entities’ needs, while having the experience to know what is scalable, financially sound, sustainable, and provides the most secure solutions in an evolving threat landscape.

MNIT’s outstanding partnership with the Cybersecurity Task Force, all types of local governments, as well as with university students and faculty has led to measurable results, including:



Consistent MDR mitigated an average of **133 high alerts** and an average of **14 critical alerts** tied to threat actors over a three-month period.



100% initial software cost savings for participants, and continued savings through reduced costs and subsidies.



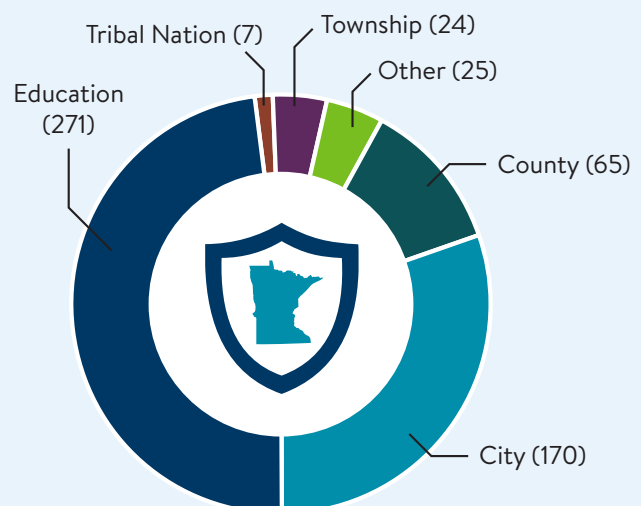
A **sustainable model** that goes beyond grant dependence.

Looking Ahead

Through the whole-of-state approach, MNIT increased its reach across Minnesota, and is now working with governmental entities of all types and sizes who completed the Whole-of-State SLCGP survey, **including seven Tribal Nations, 24 townships, 65 counties, 170 cities, and 271 education entities.**

To address additional concerns SLCGP survey respondents identified, MNIT is developing services for threat intelligence – to monitor for indicators of compromised data and provide timely alerts; and for vulnerability management – to scan public-facing devices, domains, and IPs for vulnerabilities and provide timely mitigation guidance. Both services are nearly at the rollout stage and will benefit a range of partners across the state. MNIT will continue to work with our partners and the Cybersecurity Task Force to identify gaps and needs for additional cybersecurity efforts.

The Whole-of-State Plan is a statewide strategy that includes collaboration, guidance, and opportunities to share information, expand services, and extend cyber expertise to Minnesota’s governments and critical infrastructures in an effort to keep the data of Minnesotans safe.



Entities Engaged in Minnesota’s Whole-of-State Plan