Contents

Letter from the Minnesota Cybersecurity Task Force ......................1
Executive summary ..............................................................................3
Plan overview ......................................................................................5
  Our partners ......................................................................................6
  Why it’s important ..............................................................................6
  What it means for you as a participant ............................................7
  What it means for the Minnesotans we serve .................................7
Understanding how cybersecurity works ...........................................8
Our Whole-of-State approach ..............................................................10
  Minnesota’s goals .............................................................................10
  Building on our existing foundations .............................................13
  What we want to accomplish .........................................................15
Funding ..............................................................................................16
Timeline .............................................................................................17
How we will measure success ...........................................................18
How we will sustain these efforts ......................................................18
Participation .......................................................................................19
  Eligibility ..........................................................................................19
How to get started .............................................................................20
Appendix ............................................................................................20
Greetings,

The Minnesota Cybersecurity Task Force is pleased to present the 2023 Whole-of-State Minnesota Cybersecurity Plan and Participant Guide.

The Whole-of-State Cybersecurity Plan seeks to present a united front against cybersecurity threats and to protect our increasingly connected digital services. The plan will support how Minnesota embraces new and emerging technologies while navigating the ever-changing cybersecurity landscape.

The plan is the first step to ensure that all government organizations in Minnesota can better protect the systems, data, and information with which we are entrusted by the people we serve. We recognize how seriously organizations take cybersecurity and the reality of limited resources. This plan represents our continued commitment to improving cybersecurity and supporting practitioners across jurisdictions – streamlining what everyone needs.

Representatives from state, county, municipal and Tribal governments, public education, public health, critical infrastructure, the Minnesota National Guard, and private and nonprofit sectors collaborated to develop the Whole-of-State Plan through the task force.
Our approach includes state and federal funding, State and Local Cybersecurity Grant Program (SLCGP) focus areas and objectives, continued efforts through the Statewide Security Monitoring Initiative (SSMI), and strategic objectives from MNIT’s 2023-2027 Strategic Plan. The plan has specific goals and objectives with identified leaders to ensure successful implementation. The goals and objectives focus on Minnesota’s strategy to:

- Mature cyber capabilities.
- Reduce risk by leveraging statewide programs.
- Collaborate and share information.
- Plan and prepare for cyber incidents.

The plan also incorporates the required elements for U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program – helping Minnesota focus on best practices and measurable cybersecurity outcomes. As we continue to enhance cybersecurity, we must remain dedicated to improving our resilience among disciplines and across jurisdictional boundaries. With help from cybersecurity practitioners, we will work to achieve the goals outlined in the Whole-of-State Cybersecurity Plan and become a national model for cyber resilience.

Sincerely,

Tarek Tomes
Commissioner and Minnesota Chief Information Officer, Minnesota Information Technology Services (MNIT)
Chair of the Minnesota Cybersecurity Task Force

John Israel
Assistant Commissioner and Minnesota Chief Information Security Officer, Minnesota Information Technology Services (MNIT)
Co-Chair of the Minnesota Cybersecurity Task Force
Executive summary

In the fall of 2022, the U.S. Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) announced the Notice of Funding Opportunity for the State and Local Cybersecurity Grant Program (SLCGP). This grant program is funded by the Bipartisan Infrastructure Law (BIL) through the Infrastructure Investment and Job Act (IIJA).

One of the SLCGP requirements was to establish a cybersecurity planning committee comprised of diverse membership and representation from across the state. In October 2022, the state established the Minnesota Cybersecurity Task Force with membership from public sector partners, the National Guard, Tribal Nations, and private, nonprofit, and critical infrastructure industries. Through the Task Force, the state committed to a sustainable, whole-of-state approach to addressing critical cybersecurity needs throughout Minnesota.

This Whole-of-State Cybersecurity Plan is based on current best practices for states to provide and sustain a strong cybersecurity posture.

The SLCGP and matching funding from the Minnesota legislature provide Minnesota with $23 million to distribute over the next four years. Through this grant, Minnesota seeks to improve the cybersecurity posture of state, local, and Tribal (SLT) governmental organizations through partnership and collaboration to reduce the overall cyber risk and bolster the overall cyber posture of the state.

Like most states, Minnesota has experienced cyber-attacks against schools, governmental entities, private industry, and nonprofits. Threats from bad actors from across the world with all levels of sophistication and intentions, attempt to compromise Minnesota systems. These actors are motivated by individual causes, geopolitical events, access to sensitive information, notoriety, and monetary gain. While our state’s experience is important to address, it is not unique. Across the country, healthcare, emergency services, education, critical infrastructure, and government entities are common targets.
A collaborative approach to cybersecurity is essential to build resiliency and stay ahead of these threats. The plan intends to bring together the knowledge, resources, and experiences of everyone in positions of responsibility for cybersecurity across our state. It will enable collaboration and eliminate information silos to make data, resources, and responses readily available.

The state’s IT agency, Minnesota IT Services (MNIT), assists and supports local government cybersecurity efforts with the Statewide Security Monitoring Initiative (SSMI). The SSMI program offers grant subsidies to small SLT organizations that may not otherwise have the personnel or funds for advanced cybersecurity tools. As this plan will describe, Minnesota will partly use SLCGP funds to evolve and expand SSMI programs.

Since 1993, MNIT has also provided network access with embedded cybersecurity to state partners through the Minnesota Network for Enterprise Telecommunications (MNET). MNET is designed to deliver a secure, reliable integrated statewide network for all branches and levels of Minnesota government, public safety, and education. MNET is a public-private partnership that provides a high-speed statewide backbone network and secure network access to all interested public entities. MNIT has grown to cover all 87 Minnesota counties and provides direct service lines to nearly 400 cities. All executive branch state agencies connect to MNET. MNIT provides all network monitoring, detection, and response for incidents occurring on MNET. Additional MNET services include enhanced threat intelligence, distributed denial of service (DDoS) mitigation, intrusion detection and prevention, and web application firewall services.

The Whole-of-State Cybersecurity Plan supports Governor Tim Walz’s One Minnesota Plan. All levels of state, local, and Tribal government, as well as public and private organizations across all sectors, have a role in keeping Minnesota government digital services secure. This plan seeks to:

- Consider every organization and the resources it maintains, whether it is a public health agency, a small city, or a rural law enforcement unit.
- Recognize the cybersecurity infrastructure and capabilities that exist and build upon them. The plan will not have mandates but will use collaboration to identify and develop critical capabilities.
- Provide the equipment, training, personnel, and ongoing support needed to achieve and sustain a high level of cybersecurity.
- Keep Minnesota’s and Minnesotans’ data secure.

Cybersecurity is constantly evolving. New defense capabilities are often matched by new malicious attempts to circumvent security and expose systems. We must remain vigilant and committed to working together to protect the state.
Plan overview

The Whole-of-State Cybersecurity Plan is one critical piece of a much larger puzzle aimed at securing Minnesota.

This plan provides a strategic overview of work conducted under the Minnesota Cybersecurity Task Force, together with recommendations and cybersecurity efforts under MNIT and related advisory councils, cybersecurity grant programs, and other agencies, programs, and initiatives dedicated to securing Minnesota.

The plan seeks to harden and improve cyber defenses at every level of state and local government, with input from partners across public and private sectors. It allows leaders at every level of government to work together and share resources, exchange information, and leverage federal and state funding to solve their collective cybersecurity issues. We aim to create a united front against threat actors.

The Whole-of-State Cybersecurity Plan:

- Allows leaders at every level of government to work together, share resources, swap information, and leverage federal and state funding to solve their collective cybersecurity issues to create a united front against threat actors.
- Focuses on fundamentals.
- Keeps governance top-of-mind.
- Coordinates early and often.
- Stresses communication and relationship-building.
- Removes barriers to compliance.
Our partners

The Whole-of-State Cybersecurity Plan relies on everyone who works in the public realm. That means, for example, front desk workers at police stations, as well as Tribal leaders, mayors, state legislators, and all branches of government. While information technology workers, and particularly cybersecurity professionals, will be the most deeply engaged, everyone at every level of public service should be aware of the need to take cybersecurity seriously and personally. Our partners include:

- County, city, and township governments
- K-12 public education
- Minnesota National Guard
- Local government consortiums and cooperatives
- Nonprofit organizations
- Public health and safety agencies
- State government and agencies
- Tribal Nations
- Vendor partners

Why it’s important

Cyber-attacks are an increasing problem across our state and the world. Most people are aware of social media hacks – you or someone you know may have been affected by these hacks yourself and had to scramble to make sure no malware got into your electronic device. Many people have fallen victim to online phishing or experienced identity theft.

The State of Minnesota is no stranger to cyber-attacks, with recent attacks on organizations that ultimately harmed Minnesotans. In a cyber-connected world, bad actors can be anywhere, working day and night to attempt to breach public as well as private data systems. It is MNIT’s job to protect the 5.7 million Minnesotans who entrust their data to the state and the state’s 35,000+ employees. This is one of MNIT’s most critical functions.
What it means for you as a participant

The Whole-of-State Cybersecurity Plan will provide you with the tools, resources, and information you need to secure the data that Minnesotans have entrusted to your organization.

The plan is a collaborative initiative designed to ensure cybersecurity best practices and ultimately protect the confidentiality, integrity, and accessibility of Minnesota information systems. It is inspired by Governor Tim Walz’s One Minnesota vision, which promotes servant leadership and seeks to form collaborative partnerships between state agencies and communities.

This whole-of-state approach relies on cooperation and engagement from government workers at every level – including front-line workers at the Department of Vehicle Services, sheriffs’ offices, city halls, and Tribal Nations, as well as city managers, mayors, state legislators, the governor and everyone in between.

What it means for the Minnesotans we serve

This plan and our whole-of-state approach reassure Minnesotans of our state’s continuing commitment to collaboration and cooperation that secures and protects the personal data they entrust to us.
Understanding how cybersecurity works

It’s important to understand how all the products, services, and resources work together to form a strong cybersecurity ecosystem, both for individual organizations and by extension, the entire state. The illustration and steps on the next page describe the cybersecurity elements the program will address for all Minnesota governments and schools.
Steps of cybersecurity:

The steps on this page provide details about the cybersecurity elements on page 8 that the whole-of-state program will address.

1. Don’t let them in (perimeter security): Implement practices and technologies designed to defend the perimeter of organizations’ environments (computers, people, and software).

2. Limit exposure (network, application, mission-critical asset hardening): Reduce risks of loss, corruption, and theft by keeping environments separated by the type of use, and allowing access only to the people who need to use them.

3. Make data incomprehensible: Encrypt data in databases, files, and on networks and individual computers to make it unusable if it is discovered.

4. Protect from within: Implement policies, procedures, training, role-based privileges, technologies, and best practices to recognize that threats can originate from errors or lack of knowledge.

5. Protect in transit: Make it safe to share information. With more digital government services, information and data often need to be shared. When that happens, it should be kept safe through industry standard protocols and encryption.

6. Recover from a catastrophic event (business continuity): Keep running with a redundant computing facility that uses backup systems in the event of a total or significant loss of a facility or environment.

7. Keep them out (continuous hardening): Learn, innovate, and quickly respond to limit the impact of attacks, and learn to continue to protect as the environment changes in the future.
Our Whole-of-State approach

The Minnesota Whole-of-State Cybersecurity Plan brings together the knowledge, resources, and experiences of everyone in positions of responsibility for cybersecurity across our state. It will help collaborate, share, and eliminate information silos. It aims to make data, resources, and responses readily available to all.

Minnesota’s goals

We will reach the four goals of our Whole-of-State program through collaboration and a One Minnesota approach. We strongly encourage participation from every organization. A whole-of-state approach is voluntary, but is more successful when everyone participates.

There is no final destination with cybersecurity. It morphs, takes new directions, and requires constant vigilance. It also requires inclusion. The program relies on building trusted partnerships with organizations across Minnesota. This is not a top-down mandate from the state. While there are specific efforts associated with our goals, the plan is flexible enough to meet every organization where it is in its cyber maturity and help increase its cyber capabilities.

The four overarching goals of this plan will include products and service offerings that will be available to eligible organizations on a rolling basis.
1. Mature cyber capabilities throughout the state

We recognize that every organization is at a different place in its cybersecurity maturity. This goal is designed to meet each participant organization where it is in its cybersecurity maturity cycle and provide the services and resources they need to improve.

What participants can expect:

- Baseline assessments to identify your organization’s capabilities and gaps.
- Resources, equipment, and training that will bring your organization to an acceptable level of security.

2. Increase participation in programs and services known to work

Minnesota already has several programs and services that have demonstrated success and provide advanced cybersecurity tools to participating organizations. We will expand those by including new participants and providing better service offerings.

What participants can expect:

- Access to best-in-class tools and a vulnerability analyst to identify critical vulnerabilities, and detect and remediate cyber-attacks.
- Training to optimize the use of these cyber defense tools.
- Help to streamline and implement industry best practices, standard testing, reporting, and response procedures to speed containment of emerging threats, and align all organizations.
- Help your organization adopt CISA Cyber Hygiene services and other related programs.
- Assistance to adopt trusted internet provider services by using the trusted .gov domain where appropriate.
3. Collaborate and share information throughout the state

We will expand threat intelligence sharing, analysis, and collaboration statewide. The U.S. Department of Homeland Security has Fusion Centers in every state that bring information on all kinds of national threats under one umbrella for that state. Minnesota uses this model to share timely and critical cybersecurity information with all of its partners.

What participants can expect:

- Increased involvement with the Minnesota Fusion Center (MNFC), CISA, and other resources to employ best practices in cyber defense strategies that may include:
  - MNFC threat liaison officer (TLO) programs.
  - Recurring threat briefings and bulletins.
  - CISA outreach programs.
- A Cyber Navigator will be assigned as your organization’s partner to help you with focus areas related to your assessment.
- Connections to national and regional threat intelligence forums, and shared cyber threat intelligence capabilities.

4. Strengthen the cyber-resiliency of critical infrastructure

This area will focus on local government critical infrastructure in an evolving program throughout the life of this plan. The initial program will focus on creating and delivering foundational cybersecurity services for water and wastewater systems operated by local and Tribal governments in Minnesota.

What participants can expect:

- Help to implement industry best practices, standard testing, reporting, and response procedures that focus on protecting critical infrastructure.
- Help developing your organization’s capability for 24/7 cybersecurity monitoring and response.
- Collaboration to assess current cybersecurity capabilities for critical infrastructure, identify gaps, and create a plan to address the gaps.
Building on our existing foundations

The Whole-of-State Cybersecurity Plan builds on the success of an existing program, the statewide Security Monitoring Initiative (SSMI), new funding from the federal government and the Minnesota Legislature, and objectives in the state IT agency’s strategic plan.

SSMI

The Statewide Security Monitoring Initiative (SSMI) has existed for over 10 years. SSMI is a grant-funded program devoted to partnering with participating qualified county governments, port cities, and Tribal Nations to fortify the cybersecurity of the entire state of Minnesota. SSMI participation has grown exponentially by taking a layered approach to security – meeting participants where they are in their cybersecurity maturity. SSMI partners benefit from monitoring and threat response from MNIT’s Security Operations Center (SOC) and coordination with the Fusion Center.

The program’s successes include:

• 100% of counties are participating in some portion of the program.
• Decreased cyber-attacks through vulnerability monitoring.
• Consistent endpoint detection and response.
• 100% software cost savings for participants in the first year of redesign, and continuing savings through reduced costs and subsidies.
• Stronger cybersecurity communication pathways throughout the state.

The images below show the growing SSMI participation in endpoint detection and vulnerability scanning across Minnesota. Adoption of these programs helps raise cybersecurity maturity levels across the state while also realizing cost savings for participants through reduced software costs and subsidies.

SLTs that use SSMI’s Endpoint Detection and Response (EDR) service

SLTs that use SSMI’s Vulnerability Scan service
The Technology Advisory Council (TAC) is a permanent body that advises MNIT and executive branch agencies on technology initiatives. In their January 2023 Report, the TAC made recommendations that directly relate to the Whole-of-State Cybersecurity Plan:

- To provide safe, reliable, and secure environments for Minnesota government services, and ensure that cybersecurity is included and sustainably funded for all technology-related assets.
- Promote cybersecurity threat information sharing and collaboration between state and local governments, state agencies, and Tribal Nations.
- MNIT should engage with state agencies, constitutional offices, and other state entities to increase opportunities for collaborative procurement and implementation, and to drive adoption of advanced cybersecurity protections that meet or exceed the standard defenses currently provided by MNIT.

MNIT’s Strategic Plan includes objectives that were designed with the Whole-of-State Cybersecurity Plan in mind by being more collaborative about how we manage and safeguard data and systems. Our related goals and objectives include:

- Convene and lead state, local, and Tribal (SLT) governments in Minnesota to build and implement a whole-of-state cybersecurity framework.
- Provide specific SLT recommendations around high-value investments through active collaboration with our partners.
- Define and implement an omnichannel cybersecurity communication strategy.
- Develop and implement a cybersecurity outreach and educational program.
- Implement a zero trust cybersecurity framework that requires all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.
What we want to accomplish

Ultimately, this program will protect Minnesotans by advancing the protection of state and local government information systems from unapproved access. This process towards stronger and sustainable processes will help all to meet their cybersecurity objectives. In addition to leveraging best practices with, we will build on past successes, meet every organization where they are, and educate and freely share all available cybersecurity information.

This continued cybersecurity modernization effort will allow us to collectively:

- Learn the current status of participants statewide. Discover our collective cybersecurity strengths, weaknesses, opportunities, and threats so they can be addressed.
- Analyze what we learn to identify solutions.
- Meet participants where they are in their cybersecurity maturity, and provide security products and services that will help expand statewide security endpoint detection and response (EDR) capabilities.
- Grow the Minnesota cybersecurity community to work together under the .gov domain. Collaborate and share technology and information about industry changes and the state of Minnesota-specific security observations, including collaboration with the Minnesota National Guard. This community will be served by an expanded Cyber Navigator Program that assigns security experts to each participating organization to help with their efforts.
- Establish a shared plan that encourages participants to adopt sustainable and evolutionary systems.
- Continue to build up cybersecurity capabilities to form a foundation for automation, artificial intelligence, and machine learning to modernize and harden our infrastructure.
Funding

Funding for the whole-of-state plan will come from several sources.

1. MNIT has vast experience in delivering statewide cybersecurity resources and programs through the existing Statewide Security Monitoring Initiative program, which has been funded through federal homeland security grants since 2012. The SSMI grant program was renewed for 2024 with $1.9 million of federal funds awarded to MNIT to deliver SSMI services to counties, port cities, and Tribal Nations.

2. Over the next four years (July 1, 2023 - June 30, 2027), the Whole-of-State Cybersecurity Plan will include an additional $23.5 million for this effort through SLCGP funds. The funds are available to Minnesota through an annual application process and are designed to adjust annually based on a four-year program formula. This grant program is not expected to be renewed by the federal government at the end of the four years and requires an increasing percentage of state matching funds each year to encourage state and local governments to develop sustainable funding for efforts that will last longer than the four-year SLCGP. To drive sustainable program investments and to ensure programs are available to as many eligible organizations as possible, the task force may require participating ones to share the costs and benefits of shared solutions and approved efforts in focus areas.

The SLCGP funding is provided by:

- $18 million in federal funds allocated to Minnesota through the SLCGP.
- $5.5 million in state match funds from the Minnesota Legislature.

How the funds will be used

At least 80% of funding will go directly to programming and 25% is designated for rural areas where resources are fewer. This funding will drive toward four outcomes:

1. Help local governments, Tribal Nations, and school organizations acquire the tools and resources they need to enhance their existing baseline cybersecurity capabilities. It will also support them with real security experts available through an expanded Cyber Navigator Program. Cyber Navigators are security experts who are allocated 100% to help participants.

2. Expand the use of advanced cybersecurity detection and defensive tools and capabilities to join all of Minnesota in a cybersecurity chain with a set of solid links that will form a barrier for the safety of all Minnesotans. Our joint statewide team will have no weak links when we are done.

3. Expand threat intelligence analysis and collaboration throughout Minnesota by partnering with security organizations at the federal, state, local, and private industry levels to quickly share cybersecurity intelligence in a way that helps organizations respond.

4. Bring security products, services, and resources to critical infrastructure through strategic partnerships.
Timeline

The plan timeframe is for 2023-2027, but it will build on existing programs and develop new efforts to transition into a sustainable framework that goes beyond that timeframe.

2010 – present day and beyond
Minnesota Statewide Security Monitoring Initiative (SSMI)

2018
Minnesota creates Information Security Strategic Plan

January 2019
Governor establishes IT Blue Ribbon Council

May 2019
MNIT receives $5M per year investment in cybersecurity

September 2022
Department of Homeland Security announces State and Local Cybersecurity Grant Program (SLCGP) availability

October 2022
Minnesota creates Cybersecurity Task Force to design Whole-of-State Cybersecurity Plan for sustainable security for Minnesotans

2023 – 2027
Whole-of-State Cybersecurity Plan implemented with SLCGP funds

2023
Minnesota publishes Whole-of-State Cybersecurity Plan and SLCGP availability

2027 and beyond
Next-generation cybersecurity evolution

2018
Minnesota creates Information Security Strategic Plan
How we will measure success

The Cybersecurity Task Force will gather initial data about each organization’s current cybersecurity maturity. That data will establish baseline metrics to track improvements and identify the resources needed to bring all participants up to a high and sustainable level of cybersecurity.

Key measures will include:

- Percentage of eligible organizations that have conducted an assessment, resulting in identified gaps and supported by implementation plans.
- Average time to detect and remediate vulnerabilities.
- Ability to address vulnerabilities within the policy window for each level of threat severity.
- Aging vulnerability trends and their risk and resolution with automation and detection.
- Availability of policies related to the severity of vulnerabilities and their remediation windows.
- Percent of systems with critical vulnerabilities.
- Partner participation/adoptions rate compared to the goal.

How we will sustain these efforts

While we are kicking off the Whole-of-State Cybersecurity Plan in 2023, our efforts will continue to evolve. Cybersecurity is not a one-and-done issue. Any system can be exploited by bad actors looking for security weaknesses. It is a never-ending battle. We have planned ongoing strategies to keep cybersecurity a top-of-mind issue, including:

- Continuing education and training at every level.
- Continuous upgrading of software, hardware, and systems to eliminate vulnerabilities.
- Open communication channels between organizations.
- Emphasis on continuous improvement.
- A culture of learning and listening between job levels.
- A culture of respect between local, Tribal, and state entities.
We strongly encourage participation from every organization, although participation is voluntary.

While the whole-of-state approach is intended to improve cybersecurity resources and capabilities for all eligible organizations, the Minnesota Cybersecurity Task Force recognizes that it will not be able to fund all requests and may need to limit funding available to any specific proposal. The task force will evaluate all requests and provide resources and solutions in alignment with the focus areas highlighted in the statewide cybersecurity plan.

Complete the SLCGP Survey with your organization’s contact information so you can stay informed. MNIT will use the survey information to better shape and deliver cybersecurity services for our plan, and will be in contact with interested organizations as services are available.

You can also sign up to receive news and updates about the plan and the SLCGP.

Eligibility

All state and local government entities are eligible to participate in the SLCGP, including:

1. A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government.

2. Authorized Tribal governments and organizations.

3. A rural community, unincorporated town or village, or other public entity.
How to get started

Visit MNIT’s Security website. Select the link for SLCGP for more information.

Appendix

Resources

Cybersecurity resources available to all Minnesota state and local government organizations include:

- DHS CISA Resources
- DHS CISA Services
- NJCCIC Resources
- MS-ISAC Resources