MINNESOTA

Minnesota’s Cybersecurity Plan

A Whole-of-State Approach to Strengthening
Minnesota Government Defenses

September 2023

Contents

Letter from the State of Minnesota

from MNIT Commissioner Tarek Tomes

We are living in a time when it's easier to access information than ever before. While this creates a great opportunity for many, that access can also make information a target for cyber criminals to attempt to invade our privacy and steal our data. Reports of data breaches and ransomware attacks have become commonplace, including our schools and government that affected Minnesota's children and families.

As One Minnesota, it is our responsibility to put in place the measures and efforts that help prevent attacks from being successful. This Whole-of-State Plan outlines how we are going to do that.

Protecting the technology, data, and systems that make our government and schools run is one of our highest priorities. We aim to make sure that our state, county, municipal and tribal government, education, public health, critical infrastructure, and peacekeepers have all the cybersecurity tools and resources they need.

To do that, the Minnesota Cybersecurity Task Force created the 2023 Minnesota Whole-of-State Cybersecurity Plan.

This plan seeks to strengthen local government cyber defenses and collaboration with funding from the federal State and Local Cybersecurity Grant Program (SLCGP) and the Minnesota Legislature.

Cybersecurity is, by its nature, a constantly changing field. As soon as we create new defenses, enemies and bad actors will work to find vulnerabilities. We all must remain vigilant and committed to each other and our responsibility in the greater landscape. This plan is only one piece of a much larger puzzle aimed at making our government digital services as safe as they can be in Minnesota.

We are confident that the investments in this massive effort will protect data and systems for Minnesota and Minnesotans, and hope you'll follow our progress.

Tarek Tomes

Commissioner and Minnesota
Chief Information Officer,
Minnesota Information Technology Services (MNIT)

Chair of the Minnesota Cybersecurity Task Force

Summary

We are sharing the Whole-of-State Cybersecurity Plan with all Minnesotans to inform you about what Minnesota governments are doing together to keep your information safe.

In October 2022, the state established the Minnesota Cybersecurity Task Force. This Whole-of-State Cybersecurity Plan was created by members of the task force, including representatives from state, county, and municipal governments, Tribal Nations, public education, public health, critical infrastructure, the Minnesota National Guard, and from private and nonprofit sectors.

Our whole-of-state approach presents a strong, united front against cybersecurity threats. The State of Minnesota and its partners work hard to keep you and the private information that you share with the government safe and secure by preventing unauthorized access.

This plan provides a strategic overview of work by the Minnesota Cybersecurity Task Force. It also encompasses the goals and cybersecurity efforts dedicated to securing Minnesota, including those of Minnesota Information Technology Services (MNIT) and related advisory councils, cybersecurity grant programs, and other agencies, programs, and initiatives.

We will:

- Bring together the knowledge, resources, and experiences of everyone in a position of responsibility for government cybersecurity across our state.
- Make data, tools, resources, and responses readily available to all our government partner organizations, no matter how large or small.
- Work together and share information. That means no information silos.

When government systems and data are safe, it ultimately keeps **you** safe.

What is the threat?

Minnesota has experienced cyber-attacks against schools, governmental entities, private industry, and nonprofits. There is an increasing and evolving risk from people known in the cybersecurity world as bad actors. The internet and innovations in technology has provided opportunities for bad actors across the world to attempt to compromise Minnesota's computer systems that hold confidential and private information. 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 remain among the most targeted organizations.

Who are 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 the executive branch. While information technology and 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 entities
- Public health and safety agencies
- State government and agencies
- Tribal Nations

The Whole-of-State approach

The Whole-of-State Plan brings together the knowledge, resources, and experiences of everyone responsible for cybersecurity across our state. We will reach our goals through collaboration and a One Minnesota approach. A whole-of-state approach benefits everyone but also needs everyone's participation. There is no finish line with cybersecurity. It morphs, takes new directions, and requires eternal vigilance.

It also requires inclusion. This program is not a top-down mandate from the state. While there are specific efforts associated with our goals, these are created to meet every organization where it is in its cyber maturity. Participation is voluntary and each organization's goals will be their own. At least 80% of funding will go directly to programming, and 25% is designated for rural areas where resources are fewer. The plan relies on building trusted partnerships with entities across Minnesota.

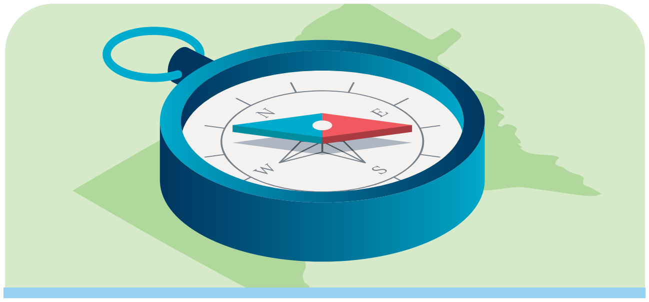
This plan continues our efforts to collaborate with governments and schools responsible for keeping Minnesotans' information secure. As One Minnesota, we aim to defend against any threat coming at any level of government.

The Minnesota Cybersecurity Task Force has approved four goals to advance the Whole-of-State Cybersecurity Plan. These are designed to provide a solid foundation for a long-term, sustainable cybersecurity system that builds on results and evolves with the times. We are reaching out to local governments, school districts, and Tribal Nations to explain the plan in depth and gather information about their cybersecurity needs.

Our state's cybersecurity chain is only as strong as the weakest link. Our defenses and protections are only as successful as those of each organization. All Minnesota government and schools are strongly encouraged to participate together in this Whole-of-State approach so that Minnesota's joint cybersecurity chain is as strong as it can be across government organizations to protect our neighbors, families, and children.

Minnesota's goals

There are four goals of this whole-of-state plan.



1. Mature cyber capabilities throughout the state

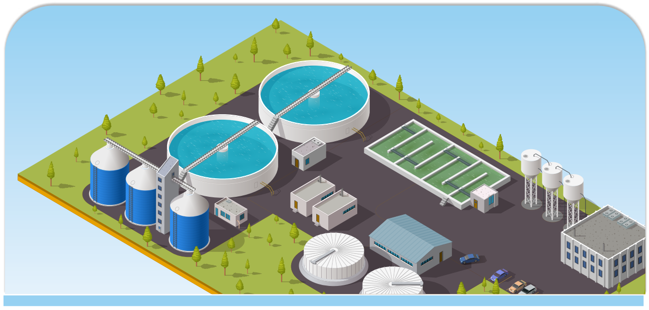
Every organization is at a different place in its cybersecurity maturity. We will provide the services and resources that participant organizations need to improve, starting with a baseline cybersecurity assessment. We will roll out resources, equipment, and training to bring as many organizations as possible 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.

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 bring together cybersecurity information that has been kept in separate silos.



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.

Why is this important to you?

The Internet has given Minnesotans better access to government but at the same time, it has given bad actors opportunities to inflict disastrous events.

As a concerned Minnesotan, this plan explains to you the work being done behind the scenes to make sure our cities, counties, Tribal Nations, and schools are safe and protected.

This Whole-of-State Cybersecurity Plan ensures that:

1. The private information you entrust to governments is protected from data breaches that can affect your reputation, your career, and your finances.
2. Information about our children is of the highest priority and will be kept safe and protected.
3. The public infrastructure you rely on keeps running, from transportation like buses and light rail to water, electric, and power facilities.

This continued security modernization effort establishes a shared plan that encourages participants to adopt sustainable and evolving systems.

We will:

- Harness our collective cybersecurity strengths and opportunities.
- Analyze what we learn to find solutions.
- Grow the Minnesota cybersecurity community, collaborate, and share technology and information about industry changes and emerging threats.
- Continue to build up security capabilities to form a foundation for emerging technology.

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. As one of the first states in the nation to partner with county governments, Minnesota's SSMI program has expanded program offerings, and now includes port cities and Tribal Nations. The program helps:

- Reduce the state's cybersecurity risk profile.
- Improve equity by offering grant subsidies to counties, port cities, and Tribal Nations that participate in the program.
- Make next-generation cybersecurity tools affordable for program participants, especially those with small budgets.

SSMI partners benefit from threat monitoring and response from MNIT's Security Operations Center (SOC) and coordination with the Minnesota 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.

Through SSMI, Minnesota coordinated $4.4 million of federal funds which resulted in a layered approach to security. Part of SLCGP funds will be used to evolve and expand SSMI programs.

Report of the

TECHNOLOGY ADVISORY COUNCIL

January 9, 2023

MINNESOTA IT SERVICES

STRATEGIC PLAN

2023-2027

Designing tomorrow's government today

Published: June 2023

Technology Advisory Council

The Technology Advisory Council (TAC) is a permanent body that advises MNIT and executive branch agencies on technology initiatives. TAC's January 2023 Report recommended that MNIT, the TAC, the Legislative Commission on Cybersecurity, and the Minnesota Cybersecurity Task Force collaborate to provide safe, reliable, and secure environments for Minnesota government services.

Objectives from MNIT's 2023-2027 Strategic Plan

MNIT's strategic objectives 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:

- Actively engage with state, local, territorial, and Tribal (SLT) entities in Minnesota to build and implement a whole-of-state cybersecurity framework and provide services and products with the highest value.
- Make sure all SLTs get the most up-to-date cybersecurity alerts and information.
- Create a cybersecurity outreach and educational program.
- Implement a zero-trust framework, which means that every user is authenticated, authorized, and continuously validated.

Plan funding

Funding for the Whole-of-State Cybersecurity Plan will come from several sources.

First, 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 grant funding 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.

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 projects and programs 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 entities to share the costs and benefits of shared solutions and approved efforts.

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.

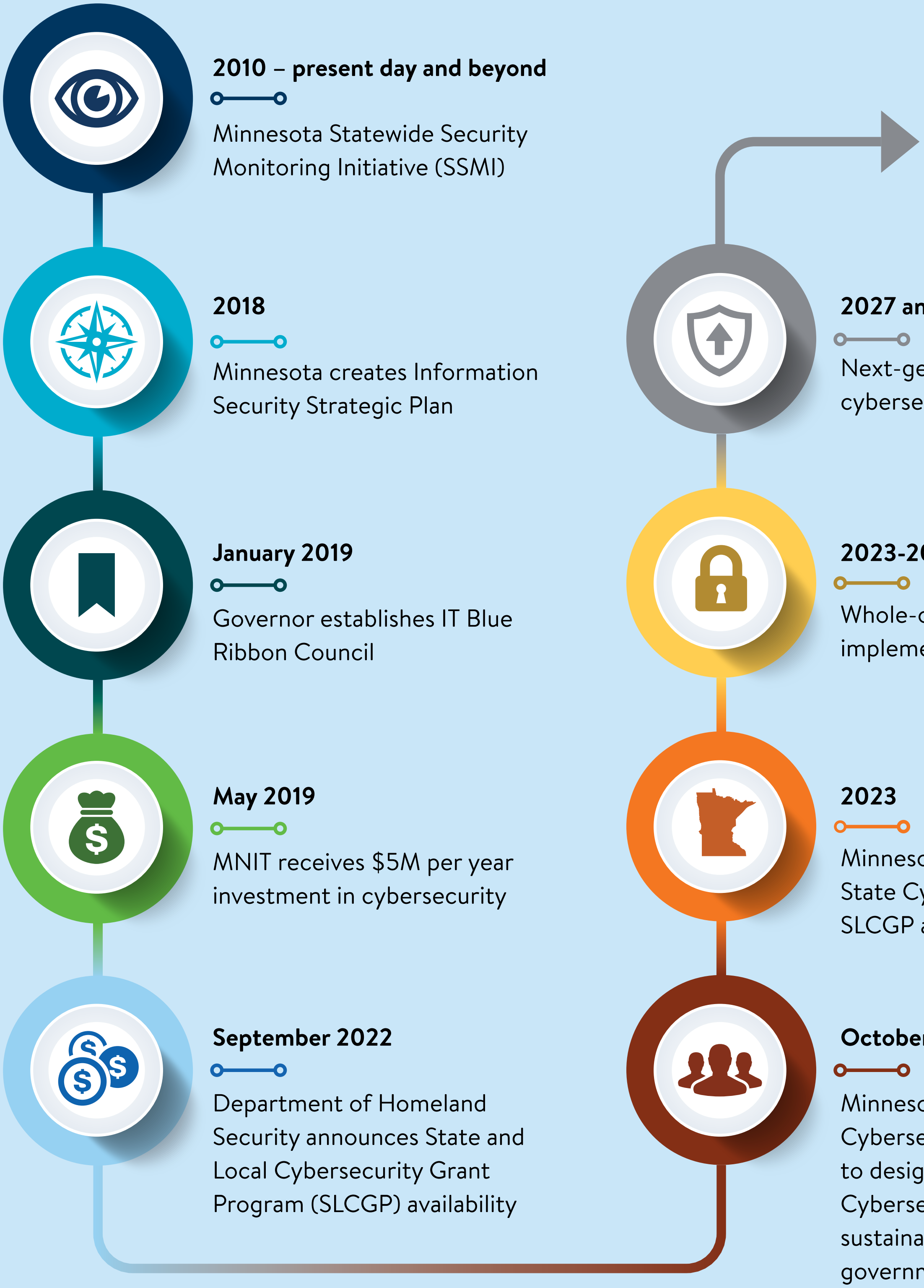
How the funds will be used

This funding will:

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 security 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 successful existing programs. During the plan's timeframe, new efforts will be developed to transition the cybersecurity program into a sustainable and evolving framework.



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 Minnesota government cybersecurity

2023

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

2023-2027

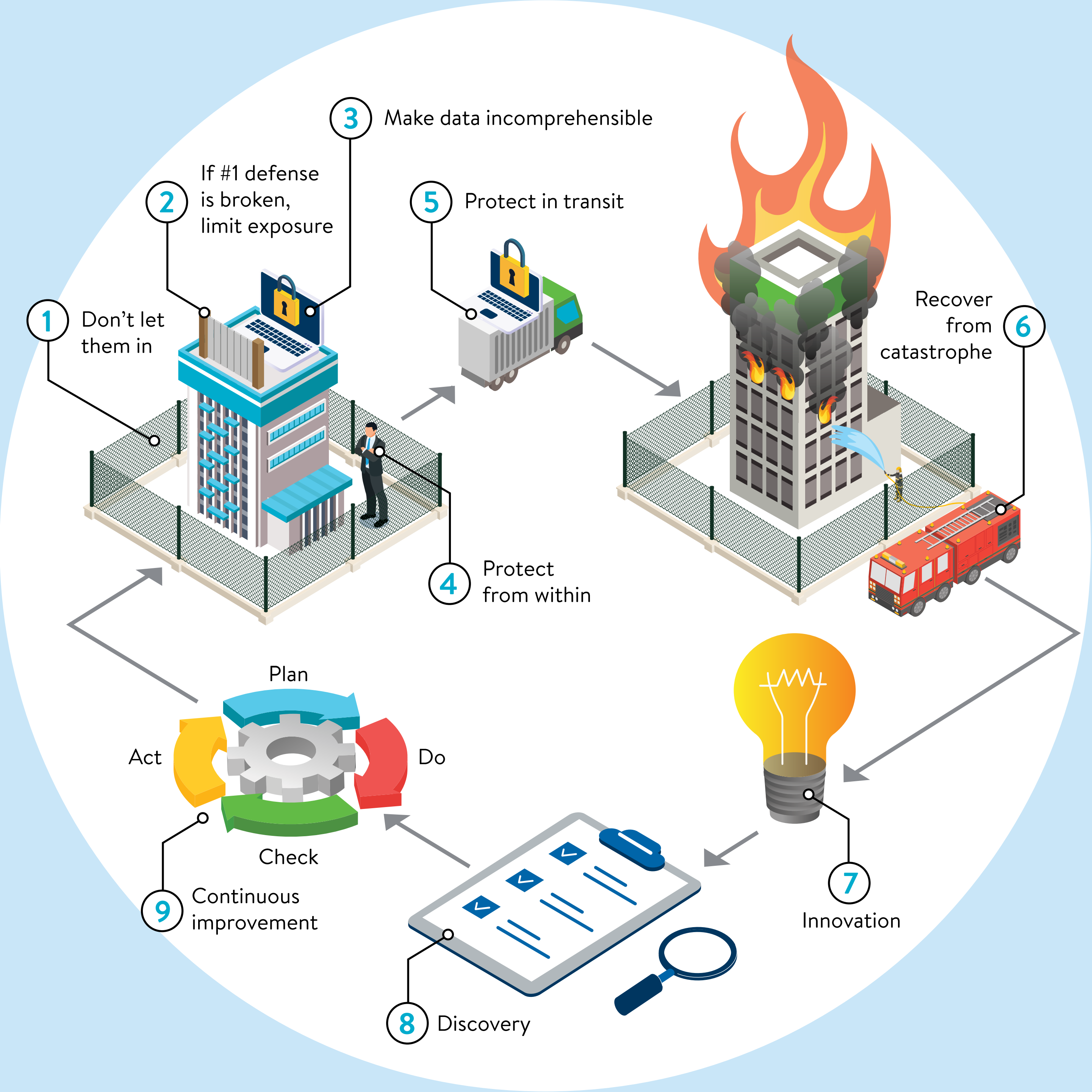
Whole-of-State Plan implemented with SLCGP funds

2027 and beyond

Next-generation cybersecurity evolution

How cybersecurity works

Here's an easy way to think about cybersecurity protections, from beginning to end. The illustration and steps below describe the cybersecurity elements the plan will address for all Minnesota governments and schools.



Moving into the future together

One Minnesota

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 promotes servant leadership and seeks to form collaborative partnerships between state agencies and communities.

Local and state governments, Tribal Nations, as well as public health and safety organizations, must embrace the idea that we are all responsible for cybersecurity. Every single one of us has a role to play to keep data secure for Minnesota and Minnesotans.

Minnesotans' role in cybersecurity

This plan is about what Minnesota governments are doing for you. However, cybersecurity is everyone's concern and there are some things that you can do to protect yourself and your loved ones. Think about cybersecurity protections in the same way you protect your car and your home by locking the doors.

Here are some recommendations from Ready.Gov. Visit their website for more information:

- Limit the personal information you share online.
- Keep software applications and operating systems up-to-date.
- Create strong passwords and change them regularly. Use a password manager and two methods of verification.
- Watch for suspicious activity that asks you to do something right away, offers something that sounds too good to be true, or needs your personal information.
- Use antivirus and anti-malware solutions.
- Do not click on links in texts or emails from people you don't know. Scammers can create fake links to websites.
- Remember that the government will not call, text, or contact you via social media about owing money.

We are all in this together. Thank you for your help. You can follow Minnesota's progress on our website.

mn.gov/mnit

This document is available in alternative formats to individuals with disabilities by calling 651-201-1118 or emailing mnit.receptioncentral@state.mn.us