MINNESOTA IT SERVICES

Minnesota Upsizes its Cybersecurity Umbrella: Expanding Protections to Counties, Cities, and Tribal Nations

State of Minnesota: Minnesota IT Services

Category: Cybersecurity
Initiated: August 2020
Completed: December 2021

Kendall Johnson
Director of Communications
kendall.johnson@state.mn.us
(C) 651-334-1760

Executive Summary

Minnesota IT Services (MNIT) protects the private data of Minnesotans against ever-evolving cyber threats and attacks. It prevents bad actors from exploiting vulnerabilities to steal information or disrupt the delivery of essential services. MNIT's security operations teams serve state and local governments statewide, tracking and analyzing cyber threats, and deploying advanced security protections and incident response throughout Minnesota.

MNIT pioneered the use of the Statewide Security Monitoring Initiative (SSMI) in 2020 to help local governments become self-sufficient and self-supporting in cybersecurity efforts. The federally funded program provides next-generation cybersecurity tools and services to participating county governments, port cities, and tribal nations to ultimately fortify the cybersecurity of the entire state. It focuses on improving the situational awareness of and response to cybersecurity incidents that impact local governments in the state.

In 2022, the SSMI program grew and strengthened by incorporating advanced tools and introducing new programming. New services include endpoint protection, vulnerability management, incident response, log collection and monitoring, and risk and compliance. The expansion led to an increase in the number of participating entities in the program, including some quasi-governmental agencies (not qualified to receive federal grant funding) that participate in the program to help keep their data secure.

The expansion also included a new Security Operations Center (SOC) Cyber Navigator program, which coordinates responses to emerging cyber threats and active incidents wherever they occur. This has encouraged proactive communication with local/tribal nation partners about threat intelligence and incident response.

By safeguarding the smallest of local government entities, MNIT is helping protect the state, making Minnesota a trusted steward of sensitive data. The partnerships also ensure that government services, regardless of their position in the service delivery chain, remain available and protected for the people of Minnesota.

Why it matters: Expanded services and advanced tools revolutionized Minnesota's statewide cybersecurity program, raising maturity levels and capabilities for counties, cities, and tribal nations and decreasing cyber-attacks.

The Need for A Big Cyber Umbrella

Minnesota is one of the few states in the U.S. with a dedicated, statewide network—Minnesota's Network for Enterprise Telecommunications (MNET)—that connects branches of government, plus all 87 counties and 1,500+ locations that serve cities, public safety, health care, Minnesota's 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. A tiny breach in the system could jeopardize the security of the entire state.

As cyber-attacks have grown in sophistication and frequency over these last few years, Minnesota knew it needed to strengthen all parts of MNET and put more entities under its protection. The increased reliance on government technology, hybrid work, and the rise of ransomware incidents have also evolved the security operations model. In these dynamic environments, advanced threats are difficult to pre-empt because they often don't have defined indicators that security analysts look for.

Minnesota protects a variety of data including sensitive data, personally identifiable information (PII), protected health information (PHI) personal information, intellectual property, and access to government and industry information systems. Hackers' ability to move laterally within the IT environment while evading detection can potentially maximize the damage, with disastrous results for communities and governments.

Envisioning a worst-case scenario, MNIT introduced new features to SSMI participating counties, including endpoint protection, vulnerability management, incident response, log collection and monitoring, and risk and compliance. This advances a strategy defined in MNIT's Strategic Plan – to bolster successful state cybersecurity efforts and combat the cybersecurity threat facing IT infrastructure, data, and systems that Minnesotans depend on.

Bolstering Cybersecurity Across Minnesota

What is the Statewide Security Monitoring Initiative?

The SSMI program creates a layered approach to security starting with secure access to MNET – providing 24/7 endpoint protection monitoring services. SSMI offerings provide partners with both external and internal vulnerability scans. This enables faster and more consistent communication about emerging cybersecurity threats throughout the state.

MNIT ensures a secure and resilient infrastructure for Minnesota by utilizing advanced resources, analyses, and security tools, alongside a communication protocol that covers all counties, port cities, and tribal nations.

The program helps:

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

Services are provided to local governments through a mix of grant funding and local government cost sharing to increase adoption while building a sustainable path to maintain services over time. The redesigned program includes SOC briefs and alerts, security monitoring, and incident response, as well as the detailed list below.

Threat Intelligence

MNIT utilizes several cyber threat intelligence tools to generate security alerts from clear, dark, and deep web content. Examples include open ports, suspected phishing domains, invalid SPF and missing DMARC records, fake social media accounts, credential leaks, accessible internal login pages, IPS on reputation blocklists, and data for sale. MNIT SOC alerts any organization that is impacted by these alerts. Additionally, the MNIT SOC will assist with malware analysis, including a review of malicious emails, phishing attempts, attachments, and URLs.

Although threat intelligence data is shared with all state, local, and tribal nation (SLT) entities regardless of MNET or SSMI participation, SSMI amplifies the data available to those respective agencies.

Security Information and Event Management

The legacy SSMI firewall purchases and monitoring offering is being replaced with a SSMI Security Information and Event Management (SIEM) solution that will provide a range of security and compliance functions, including inventory tracking and automated inventory management, audit log management, and network monitoring and defense.

External and Internal Vulnerability Management

External, public-facing IP scans are a free service provided by MNIT to help reduce the attack surface of MNET customers. This service includes analyst expertise to focus action on the most impactful results. This service mimics the scanning that is often done by threat actors searching for known vulnerabilities.

Internal Vulnerability Management uses Tenable.io to offer fully credentialed scans. MNIT's dedicated vulnerability management experts configure credentialed vulnerability and compliance scanning and provide risk-based vulnerability management analysis, remediation prioritization, and recommendations. This program provides monthly vulnerability review meetings with participating entities to provide and discuss vulnerability remediation strategies.

Endpoint Detection and Response

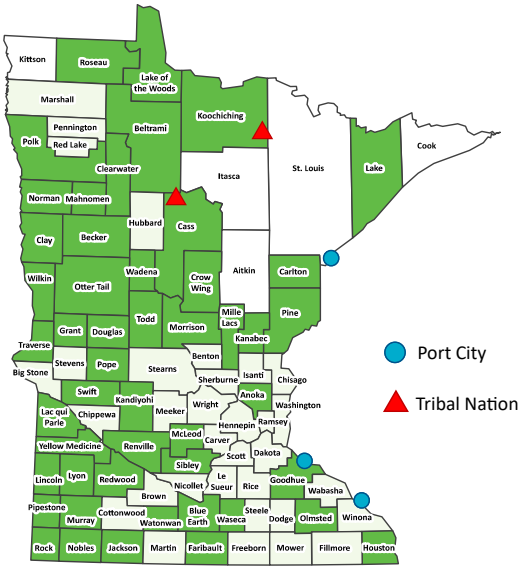
Through SSMI, MNIT offers CrowdStrike Endpoint Detection and Response (EDR) to provide 24/7 endpoint protection, monitoring, and response. The EDR solution watches for behavior rather than scanning for individual files. If one a threat emerges in one area, once it's addressed, all participating entities are instantly protected from the emerging threat. MNIT continues to identify steady funding sources to support this program given its expansion and the overall satisfaction across participating entities.

Cybersecurity Frameworks

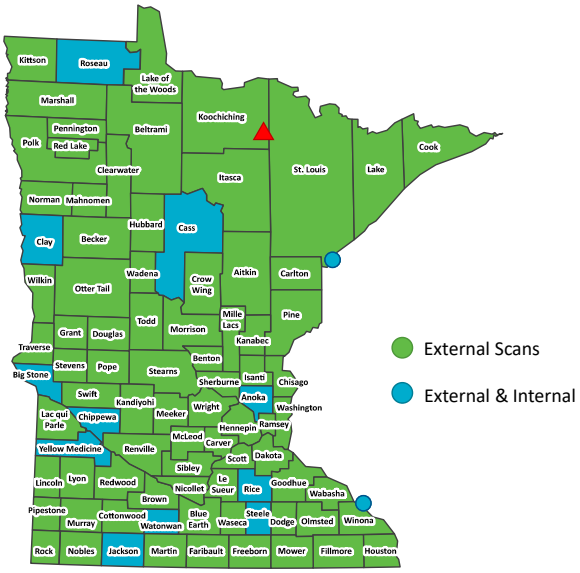
SSMI services complement others available through the Cybersecurity and Infrastructure Security Agency (CISA), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and other free or low-cost services. They all include research, monitoring, and assessments by MNIT's subject matter experts. Implementation of common control standards across state and local government establishes the security that is necessary to avert common threats.

SSMI Participation

EDR



Vulnerability Scans



Proactive Approach to Action

This groundbreaking SSMI program continues a holistic, proactive approach to shoring up Minnesota's network defenses from border to border.

- Partners can choose which elements of the program to use and launch them when their current service licenses expire.
- SSMI participants do not need to be cybersecurity experts to take advantage of the resources offered to them and can focus their efforts where they matter most – whether it is combating a piece of malware, or deciding which vulnerabilities need patching first based on data and expert guidance provided through SSMI resources.
- Participants also do not need a large IT department, as MNIT SOC personnel guide them through the process and assist as necessary.
- MNIT SOC staff provide periodic wellness checks for partner networks and share powerful tools that can be used to remediate issues, bolster defenses, and increase awareness of emerging threats and events. The program continues to evolve to locate and neutralize cybersecurity threats.

Implementing Statewide Cybersecurity Modernization

SSMI expansion planning started with MNIT's Tactical Planning efforts in 2021. MNIT identified several tactics to advance, which align with MNIT's Strategic Plan and the Security Strategic Plan. These tactics drive the strategy of "cybersecurity modernization and managed detection and response."

The roadmap to implement and reimagine SSMI included:

- **Modernize** the current SSMI program to bolster statewide cybersecurity.
- **Negotiate volume pricing** to achieve cost reductions and increase participation across all of Minnesota.
- **Reduce costs** of a top-tier Next-Generation Antivirus (NGAV) program, and threat and vulnerability scanning.
- **Promote participation** through a communications outreach plan. Grant funding helped several entities benefit from many SSMI services. The entities will eventually self-fund these programs within five to seven years.
- **Establish a Cyber Navigator** to interact directly with participants. This dramatically increased inter-agency communication and the sharing of cybersecurity information and resources throughout the state.

Stakeholders Playing Their Part

The SSMI program was led by MNIT SOC and Threat and Vulnerability Management Unit (TVMU) staff. Various departments within MNIT, such as Financial Management, Customer Service, and Communications, played a crucial role in ensuring its success and effectively engaging and recruiting counties, port cities, and tribal nations. Advocacy and oversight were key factors in meeting the program's goals and objectives, while effective communication between MNIT, vendors, and program participants facilitated timely implementation. Throughout the process, maintaining a customer-focused approach to delivering services to local government partners remained a top priority for everyone involved.

Proactive and consistent partner communication along the way ensured that the program matured as it evolved – working with local government partners to identify potential threats quickly to allow real-time protection for them.

Scaling Up

The SSMI redesign was structured with iterative phases, ensuring that it could incorporate best practices that are consistent, sustainable, and successful. The program's approach to continually improve the state's defenses helps address gaps that could lead to service outages or data breaches and can be expanded to include many different types of local government organizations.

Local partners roll out their respective programs with information, tools, and technical expertise from MNIT as needed. They do all the "hands-on" work and learn as they go. As partners' needs evolve, MNIT will expand support.

Future offerings, currently under development:

- Advanced Log Collection/Security Information and Event Management (SIEM) with analytics and metrics.
- Expanded Cyber Navigator program to include additional positions, to match the service demand from expanding partners and sectors.
- Expanded EDR program to include all cities (except port cities), K-12, and public critical infrastructure across Minnesota.
- MNIT SOC service transitioned to a more hands-on approach for threat assessment and remediation.
- Expanded cybersecurity threat intelligence capabilities through additional tools, resources, and memberships.

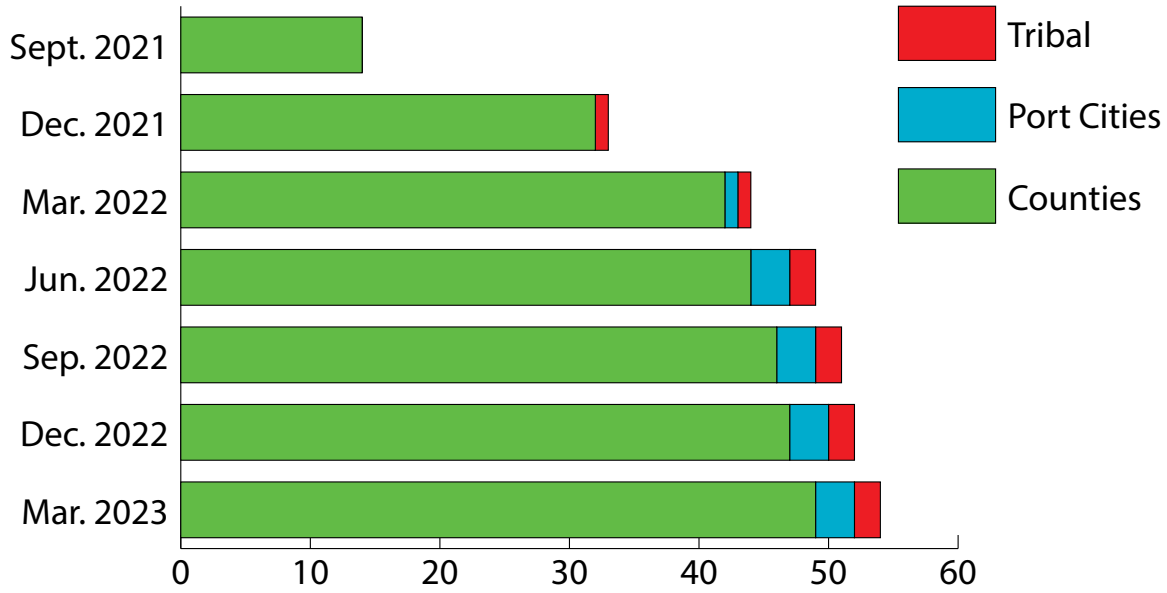
Highlighting SSMI's Success

As of today, 87 of the state's 87 counties have participated or currently participate in the program. The accelerated adoption far outpaces the participation gains under the previous SSMI program and helped MNIT receive a 25% increase in grant dollars to implement the program in 2023.

The accelerated adoption of the program is quickly raising cybersecurity maturity levels and capabilities for participating entities who often have few cybersecurity resources or staff.

- **Decreased Cyber-Attacks**: The success of modernized SSMI can be defined by the things not seen – high-profile cyber-attacks. During the implementation of the project, MNIT and its partners encountered varying levels of cyber incidents. Most organizations found that they had some form of vulnerability or malware within their network and were able to begin immediate remediation. Even deploying the EDR software on all machines within a network in "learning mode" had a sobering effect when vulnerabilities became apparent in their environment.
- **Increased Participation**: As of March 2023, 50 of Minnesota's 87 counties (60%), three port cities, and two tribal nations have joined the MNIT SSMI EDR program. They received training for their staff and equipment to help them maintain their security risk at a low level.
- **Realized Cost Savings**: Partner organizations saved 100% of their software costs in the first year of the redesign. MNIT continues to use SSMI grant funds to subsidize and reduce the software costs to partners.
- **Strengthened MNIT SOC's Cybersecurity Response Capabilities:** Increased abilities while decreasing response time when assisting partners.
- **Created Communication Pathways:** Strengthened and improved relationships throughout the state, augmenting unilateral proactive cybersecurity communication.

Timeline of Participation



Looking Ahead

MNIT plans to move forward with acquiring advanced SIEM software where MNIT analysts will perform threat hunting – giving increased insight not only to the participants but to all MNET entities. The next-generation SSMI program has been built around continually responding to common and emerging cyberthreat vectors while being cognizant of pain points for our partner organizations. MNIT staff will continue to foster and strengthen proactive partner communication to make services better.

Implementing a program of this enormity requires a long-term commitment for many years to come. By engaging with partners, MNIT builds enduring relationships that are based on understanding and listening to their needs. In addition to the increased ability to detect and repel cyber-attacks, maturing these partnerships are one of the most important outcomes.

Partnerships, careful consideration, and extensive planning ensure long-lasting cybersecurity efforts are embedded in the way all Minnesota entities do the business of government and provide services for Minnesotans.