State & Local Cybersecurity Grant Program (SLCGP)

Legislative Commission on Cybersecurity | 22 November 2024

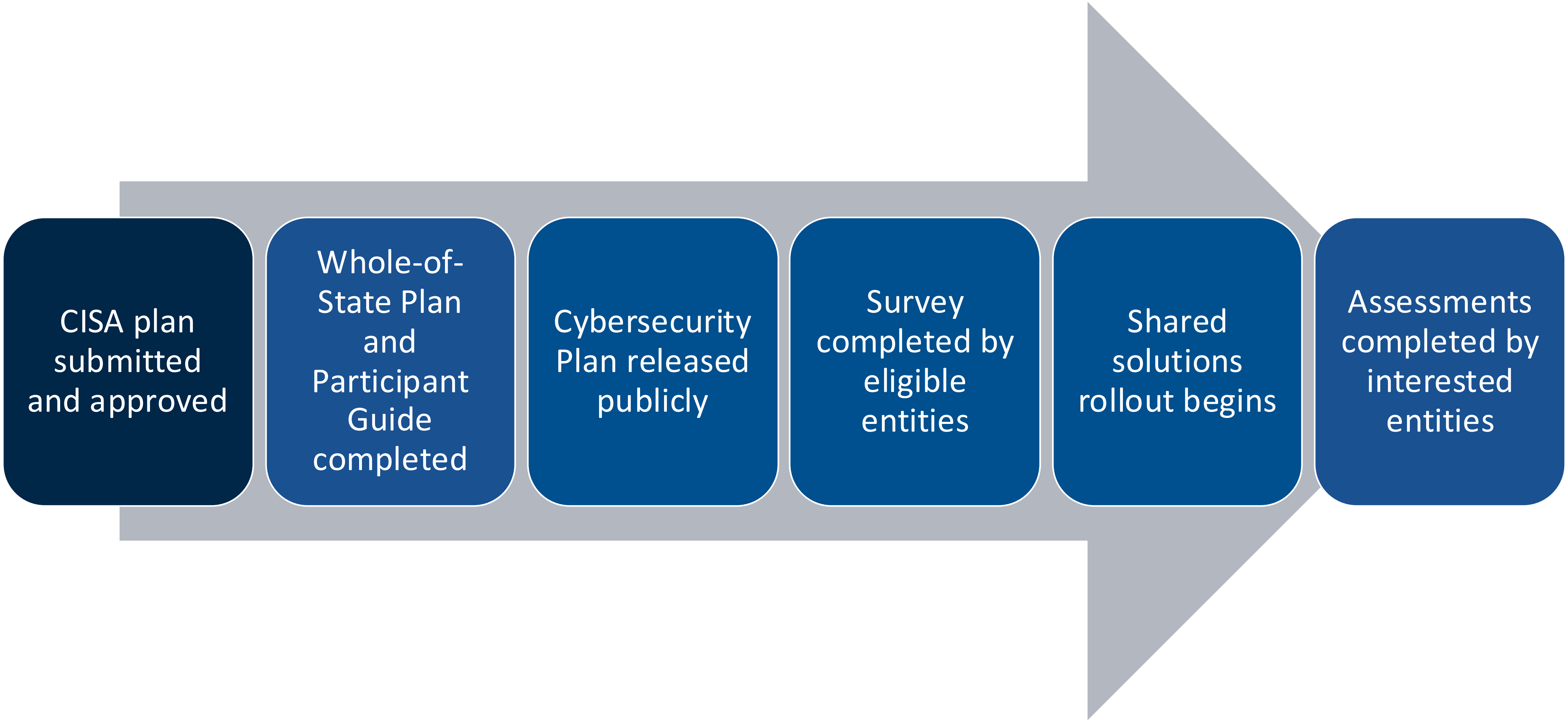
John Israel | Assistant Commissioner, Chief Information Security Officer

MINNESOTA IT SERVICES

Agenda

- Overview: SLCGP and Whole of State Plan
- Minnesota Cybersecurity Task Force
- Engagements
- Project Status
- Budget Status
- Future Projects
- Cybersecurity Incident Reporting Law & SLCGP

State and Local Cybersecurity Grant Program Update



CISA plan submitted and approved

Whole-of-State Plan and Participant Guide completed

Cybersecurity Plan released publicly

Survey completed by eligible entities

Shared solutions rollout begins

Assessments completed by interested entities

The Whole-of-State Approach

MINNESOTA

Whole-of-State Cybersecurity Plan Participant Guide

September 2023

The whole-of-state approach presents a strong, united front against cybersecurity threats, by bringing together the knowledge, resources, and experiences of everyone responsible for cybersecurity across our state.

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

Whole-of-State Cybersecurity Plan

MINNESOTA

Minnesota's Cybersecurity Plan

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

September 2023

Allows leaders at every level of government to work together, share resources and information, and leverage federal and state funding. They work collaboratively on cybersecurity issues to create a united front against threat actors.

- Focus on fundamentals
- Keep governance top-of-mind
- Coordinate early and often
- Stress communication and relationship building
- Remove barriers to compliance

Minnesota Cybersecurity Task Force

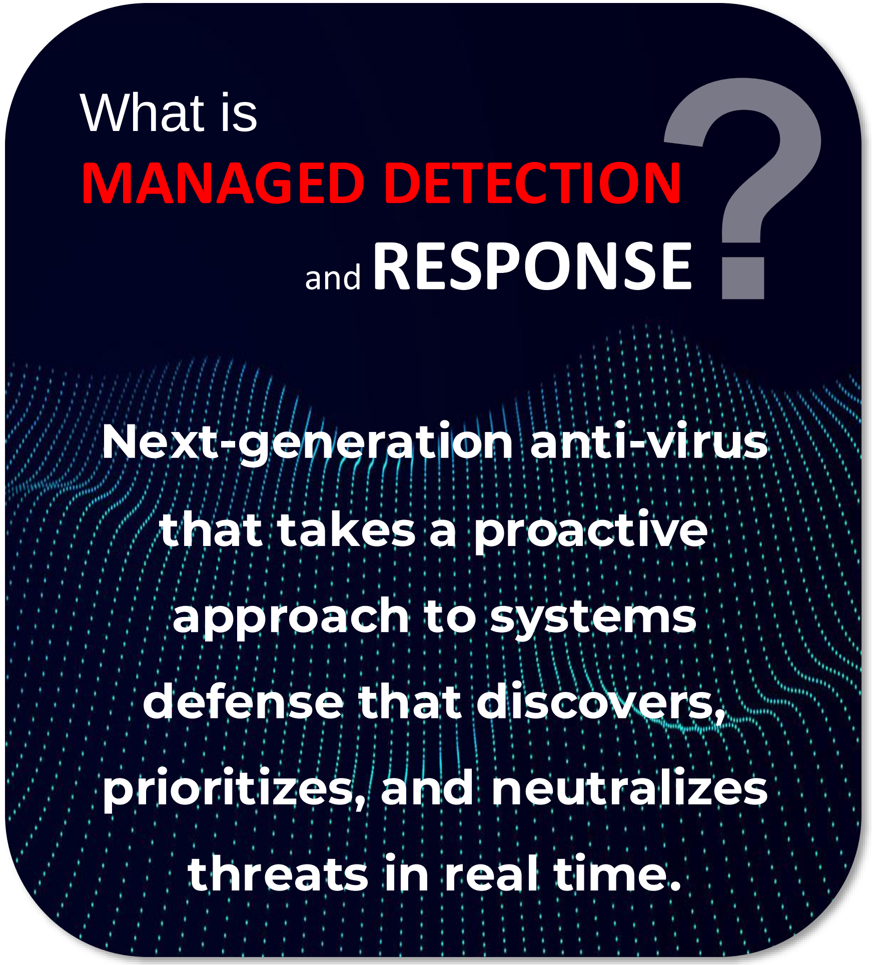
SLCGP required the creation of Minnesota's Cybersecurity Task Force

- Appointed in October 2022
- 1+ monthly meeting November 2022-present
- 15 members of SLT and private sector
- Ex officio members
- Alignment with TAC and LCCS

- Counties
- Cities/townships
- Tribal Nations
- Education and Health
- National Guard
- Critical Infrastructure
- Other cybersecurity / IT

Current Initiatives

- **Cyber Navigator Program**
- **Managed Detection and Response (MDR)**
  - Six-month early adopter program
  - Full remediation services
  - 24/7 threat hunting & investigation
- **Risk Assessment Pilot**
  - Basic cyber hygiene
  - University graduate assistance
  - Governance group
- **Vulnerability Management**
  - Internal and External scans
  - Vulnerability analyst expertise to focus fixes



What is **MANAGED DETECTION** and **RESPONSE** ?

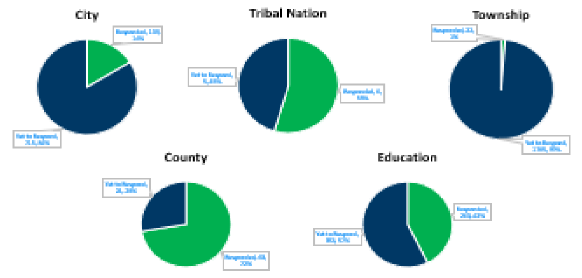
Next-generation anti-virus that takes a proactive approach to systems defense that discovers, prioritizes, and neutralizes threats in real time.

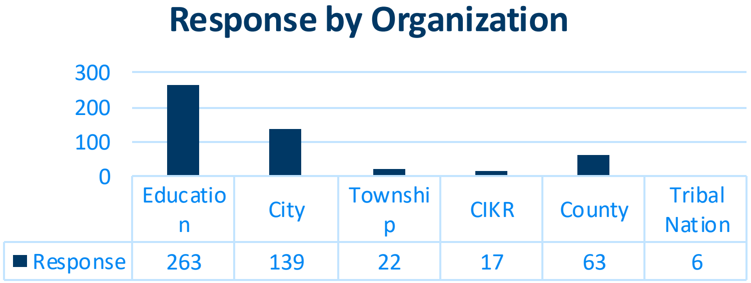
Engagement

Task Force uses surveys and outreach efforts to drive project development

Cyber Navigators in 2024:

- 1,500+ connections with local government and K12
- 500+ responses to SLCGP survey
- 100+ threat intel share via SLT platform
- 50+ speaking engagements with local government and K12 entities
- 34+ formal water/wastewater engagements



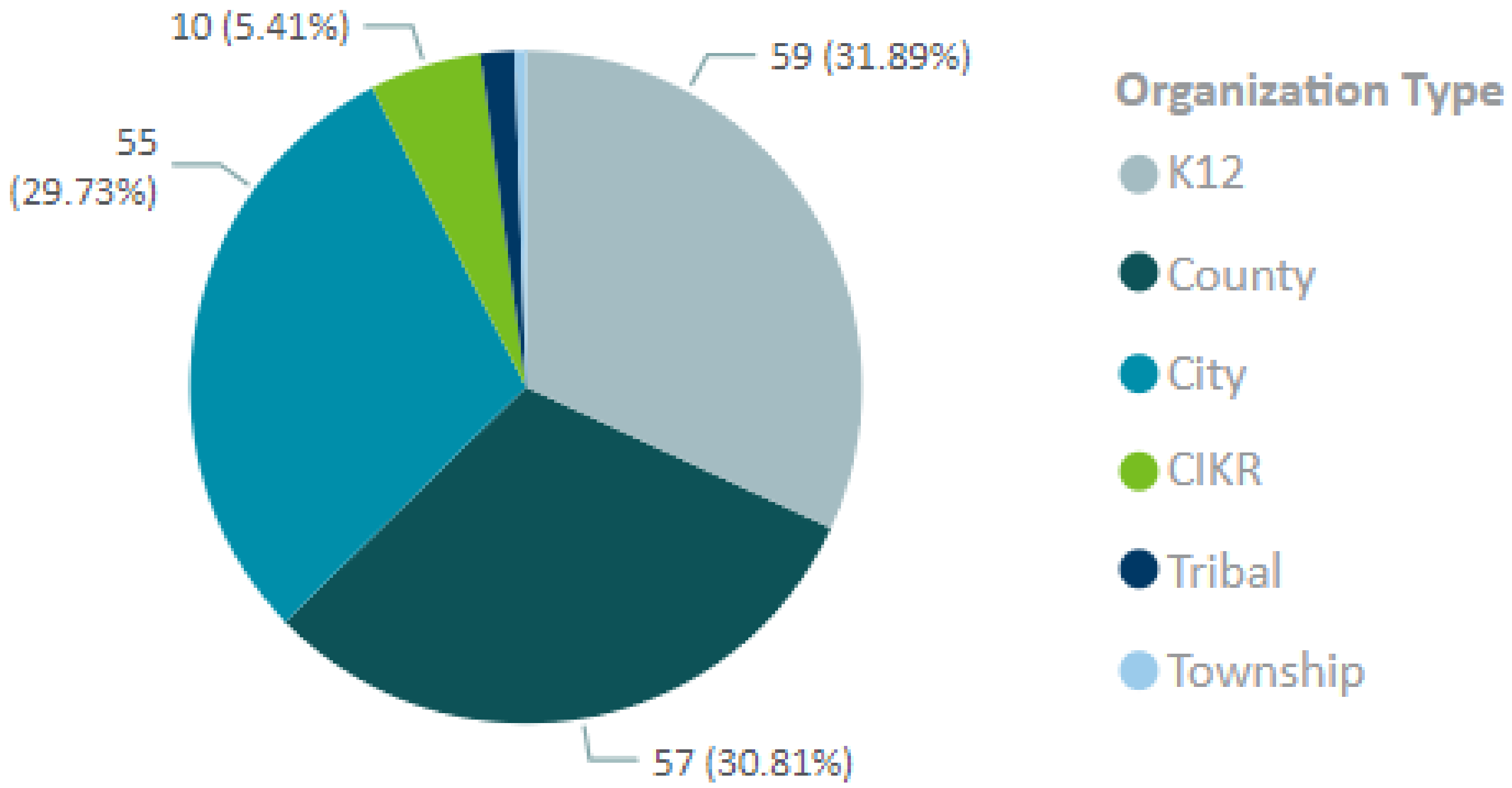


	Education	City	Township	CIKR	County	Tribal Nation
■ Response	263	139	22	17	63	6

★	● **Endpoint monitoring protecti...**	298
★	● **Threat Intelligence**: Tools that ...	290
★	● **Network Services**: Monitoring t...	286
★	● **Security and Risk assessments...**	276
★	● **Vulnerability management**: To...	218
	● **Training for IT staff**: Technical ...	211
	● **Training for general staff**: Phis...	198
★	● **Enhanced logging**: Tools that ...	195
	● **Identity and access managem...**	177
	● **Third party risk management**: ...	154
	● **Multi-Factor Authentication (...**	114
	● **Adoption of a .gov domain**: A ...	72
	● I don't know	34
	● Other	27

MDR Adoption

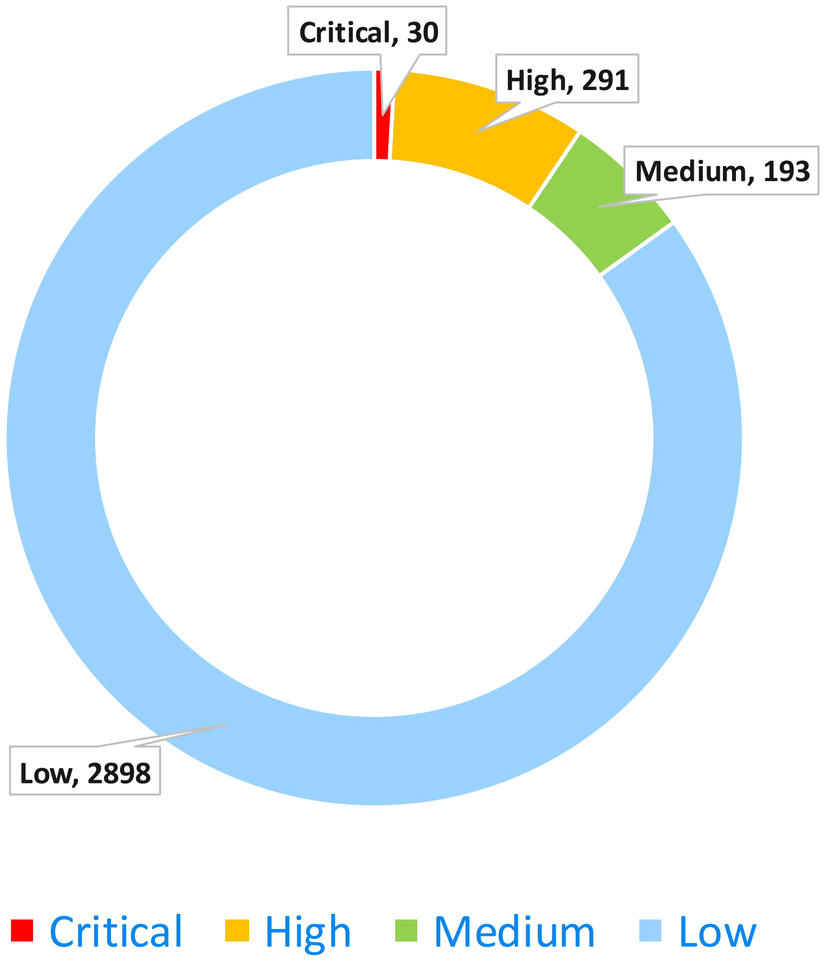
185 organizations and counting | >50,000 endpoints protected



*Twenty-six additional organizations engaged in enrollment process

MDR Response

Incidents prevented by MDR: Past 90 Days



MDR Strategic Plan

- Government Partners Manager leading expansion strategy
  - Targeted outreach based on gaps in partnerships
    - Ex. Cities/townships with populations 10,000-20,000
  - Pilot groups to test modules
  - Cybersecurity Incident Reporting Law provides opportunities to expand MDR coverage
- Awaiting release of 2023 SLCGP funds

MDR Feedback

> The implementation process unfolded precisely as communicated, swift and flawless. Thank you for your efficiency! This added layer of oversight brings us a sense of security as we conclude each day, recognizing the imperative nature of round-the-clock monitoring and remediation for cybersecurity incidents in today's digital landscape.
>
> ***– Minnesota city***

> We were not currently using a third-party MDR other than the built-in security features within each platform and those in place at a firewall level of detection. It has only been a few weeks since the sensors were installed and already had instances where the MDR stopped a user from accessing a bad URL.
>
> ***– Minnesota K12***

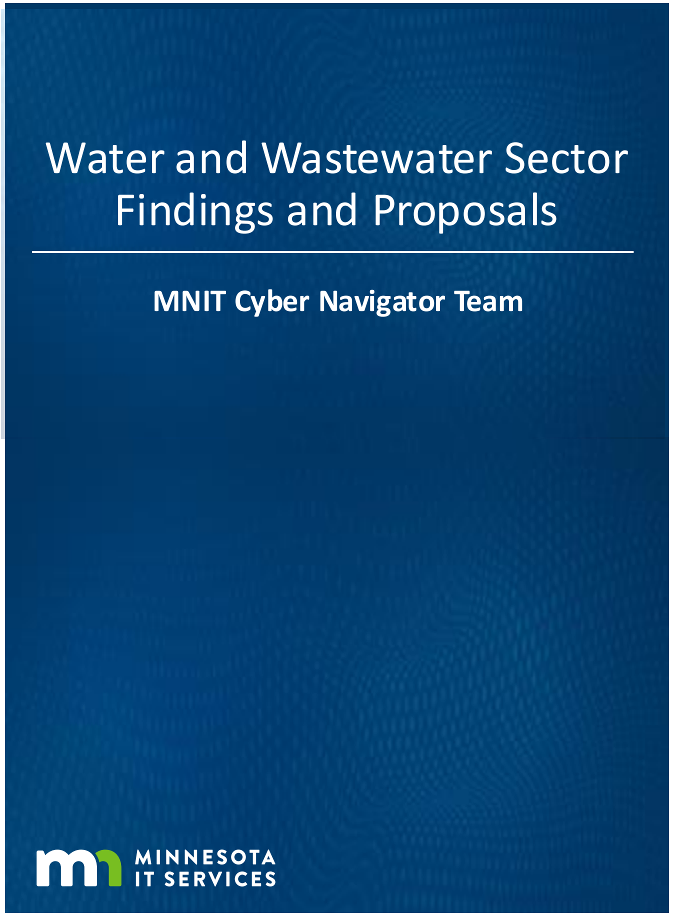
> Genuinely appreciate working with [MDR vendor]. Their SOC has been wonderful. Also appreciate having access to [training]. That is helping to make sense of that environment. Looking forward to doing more with vulnerability management.
>
> ***– Minnesota county***

Cyber Navigator Team

- December 2023: Team grows from one to four.
- Broadens to K12, cities/towns, critical infrastructure.
- Expands and strengthens partnerships.
- Strengthens current partnerships (counties, port cities, Tribal Nations).

Initiatives: Year Two+

- Critical infrastructure – water & wastewater
- MDR strategic plan
- Risk assessments
- .gov adoption
- Cyber threat intelligence
- Vulnerability management expansion
- Cybersecurity Incident Reporting Law – Navigator team leads intake and response

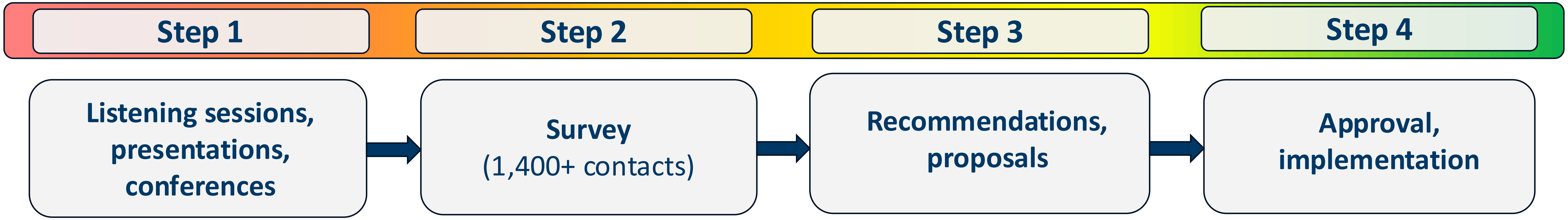


Water and Wastewater Sector Findings and Proposals

MNIT Cyber Navigator Team

MINNESOTA IT SERVICES

Water and Wastewater



Step 1
Listening sessions, presentations, conferences

Step 2
Survey
(1,400+ contacts)

Step 3
Recommendations, proposals

Step 4
Approval, implementation

MINNESOTA

Whole-of-State Cybersecurity Plan Participant Guide

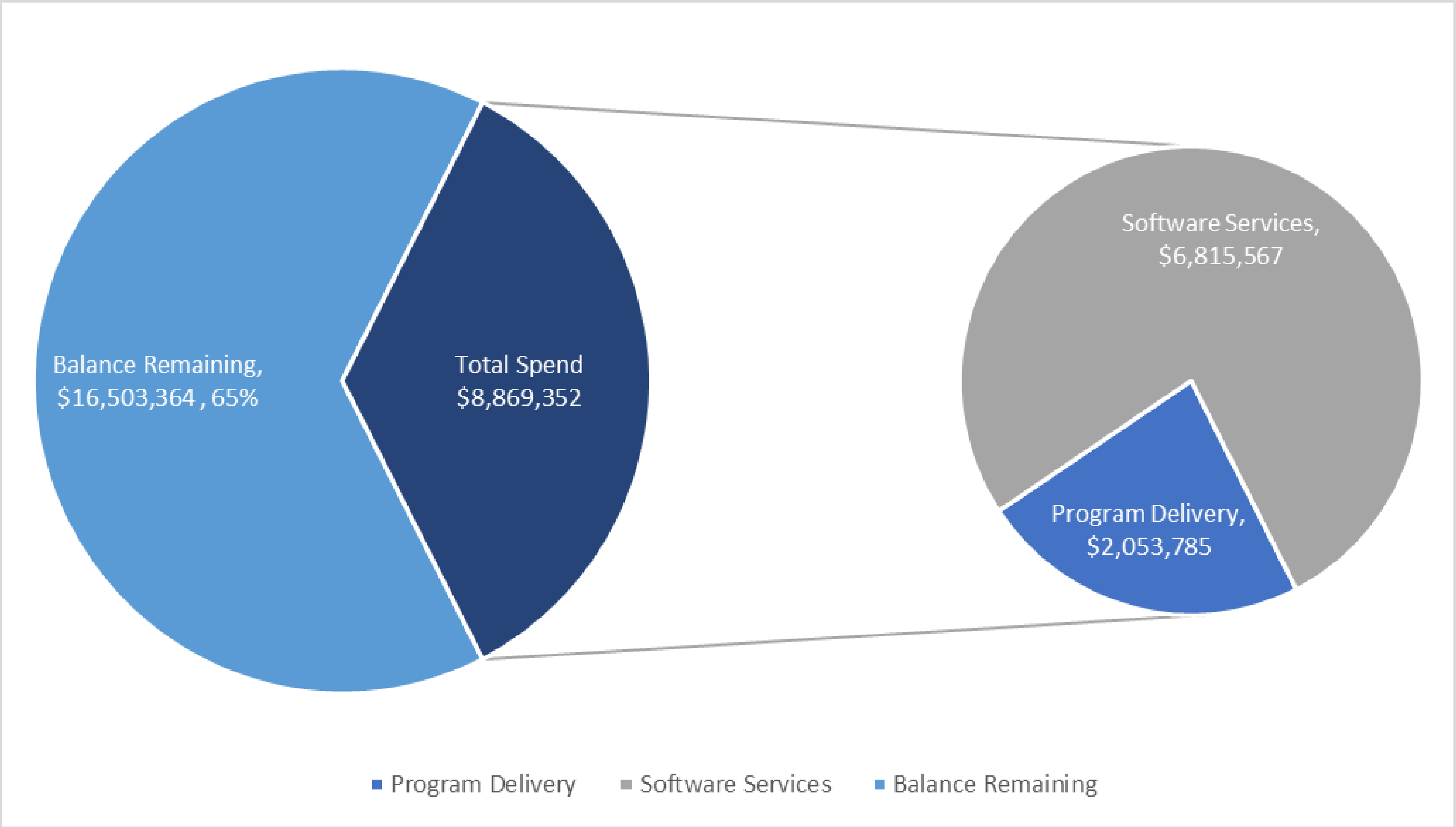
September 2023

4. Strengthen the cyber-resiliency of critical infrastructure

Focus on local government critical infrastructure. The initial program will focus on creating and delivering foundational cybersecurity services for **water and wastewater systems** operated by local and Tribal governments.

SLCGP Projected Budget Update FFY 2022-2025

Federal Fiscal Year SLCGP Grant FFY 2022-2025



FCC Considerations

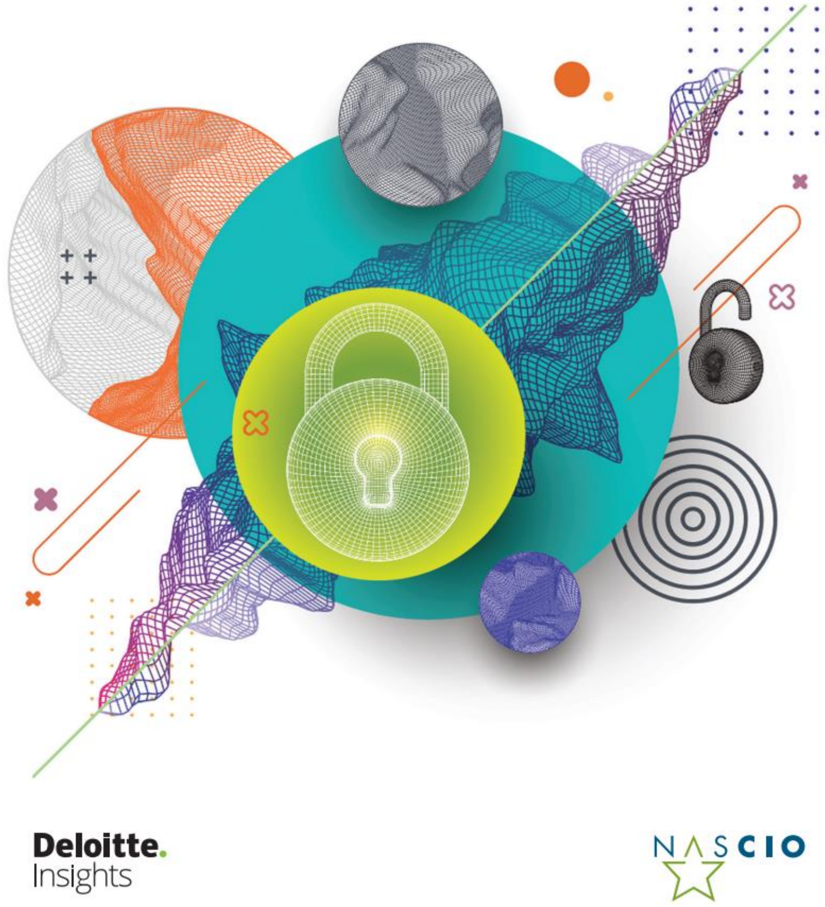
High demand for cybersecurity resources

- FCC’s $200 million, three-year pilot program to boost cybersecurity in schools closed on November 1.
    - FCC said it received 2,734 applications totaling $3.7 billion in requests.
- The high demand comes at a time when cash-strapped schools are increasingly vulnerable to serious cyberattacks, particularly ransomware threats.

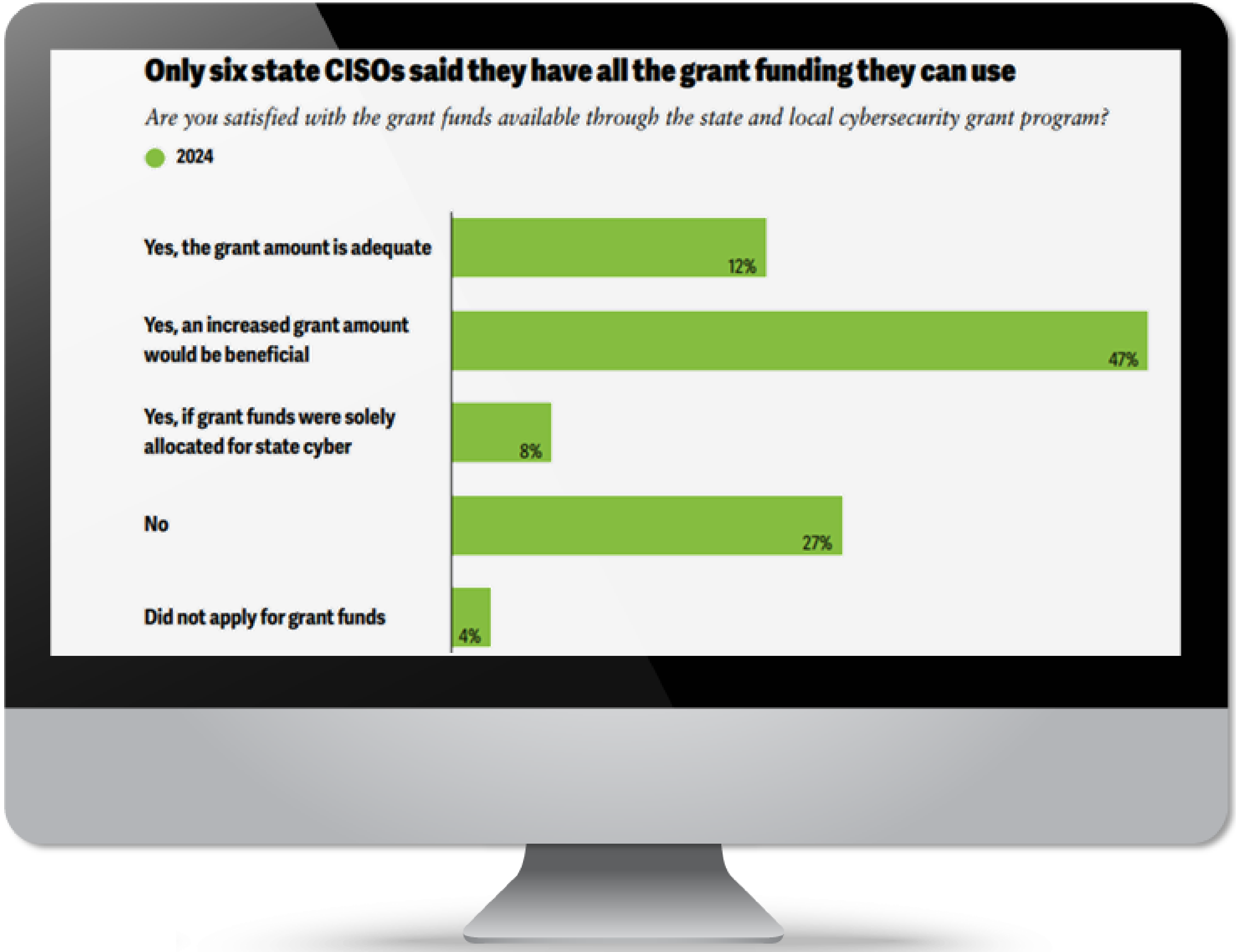
Considerations

Cybersecurity resources in demand

- The 2024 Deloitte-NASCIO Cybersecurity Study noted state’s **have** the authority but lack the **staff and budget** to deliver on their mission
- The study recommended states take a **“whole-of-state”** approach – encompassing local, city, county, and higher education institutions



“The rapidly changing landscape of cyber-threats demands that state(s).. respond with new defensive approaches.”



Only six state CISOs said they have all the grant funding they can use

Are you satisfied with the grant funds available through the state and local cybersecurity grant program?

Cybersecurity Incident Reporting Law

Outlined in section 16E.36 of the Public Safety and Judiciary Omnibus law

- Shared draft form and guidelines with 500+ public entities for comment.
- Used feedback from 60+ entities to create a user-friendly process and ensure necessary information is collected.
- Two webinars attended by 200 partners.
- Direct engagements by Cyber Navigator Team across local governments and K12.

Cybersecurity Incident Reporting: Dates

- **September 30, 2024:**
  Reporting form & instructions were posted on MNIT's website: [mn.gov/mnit/Cybersecurity Incident Reporting]().
  - Form is live and accepting reports.

- **December 1, 2024:**
  Public agencies and government contractors are required to report.

- **January 31, 2026:**
  MNIT and BCA must submit an annual report on its cybersecurity incident report collection and resolution activities to the Governor and Legislative Commission on Cybersecurity.

Cybersecurity Incident Reporting: Who Must Report

Beginning December 1, 2024

The following entities must report an incident that affects them:

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

Why this is important to me?

Information sharing can help prevent attacks

- ○ **Anonymize** and share cyber-threat indicators and cybersecurity incident notifications and relevant defensive measures.
- ○ Share cybersecurity incident notifications with potentially impacted parties through cybersecurity threat bulletins or relevant law enforcement authorities.

Track and identify trends

- Use reported information to track and identify cybersecurity trends.
- Annual reports to the Governor and Legislature will help define cybersecurity needs.
- Data will be incorporated into the State of Minnesota Cybersecurity Threat Assessment.

Cybersecurity Incident Reporting & SLCGP

- SLCGP-funded Cyber Navigator team leads Cybersecurity Incident Reporting intake and response efforts.
- Outreach will provide opportunities to provide tools and services.
- Cybersecurity Incident Reporting data will inform the Cybersecurity Task Force of current trends and gaps.
- Data will help drive project development and identify areas where grant funds are needed most.

Thank You!

John Israel | Assistant Commissioner, Chief Information Security Officer

Brandon Hirsch | Director of Government Relations

MINNESOTA
IT SERVICES