Improving Funding Access for Cyberinfrastructure in Minnesota

Legislative Committee Handout – SF 3879 (General Obligation Bonding Amendment)

EXECUTIVE SUMMARY

As Minnesota becomes increasingly digital, state and local government systems must evolve to meet rising demand while protecting sensitive citizen data. Cyberinfrastructure now supports essential public services, including tax administration, elections, eligibility systems, and critical infrastructure monitoring such as water treatment systems.

Current systems are fragmented, unevenly funded, and in many cases outdated. While SF 3879 will not resolve all challenges immediately, it provides a critical opportunity to modernize foundational systems and strengthen long-term resilience across state and local government.

KEY CONCERNS

Cybersecurity Risks

Recent incidents highlight increasing vulnerability across jurisdictions:
- Winona County experienced two cyber incidents within one year
- City of St. Paul experienced a major cyberattack in 2025
- Spring Lake Park School District lost instructional time due to a cyber incident in 2026

State-provided cybersecurity tools, including the CrowdStrike contract, have demonstrated the value of centralized, vetted, and cost-effective protection.

Modernization of Legacy Systems

- Systems lack interoperability and modern functionality
- County and agency staff rely on inefficient workarounds
- Cross-agency integration remains limited

Improved systems strengthen service delivery, workforce efficiency, and resident outcomes.
People → Process → Technology

Local Funding Constraints

- Fewer than 150 Minnesota cities have dedicated IT staff
- Many cities require populations of approximately 10,000 residents to support one IT FTE
- Small and rural communities face heightened cybersecurity and operational risk

Data Sharing and Coordination Challenges

- Inconsistent data standards across agencies
- Limited intergovernmental coordination reduces accountability
- Legislative audits repeatedly identify system fragmentation as a barrier to oversight and efficiency

Ahmed Anshur, Kenneth Eban, Sarah Erickson, Nebiha Mohhamed, Kenny Neimeyer

SarahBErickson57@gmail.com

POLICY SOLUTION: SF 3879 CYBERINFRASTRUCTURE MODERNIZATION

SF 3879 proposes a constitutional amendment to authorize General Obligation (GO) bonding for cyberinfrastructure, recognizing IT systems as essential public infrastructure alongside transportation, utilities, and public facilities.

This creates a structured mechanism to address deferred modernization and system risk across Minnesota's state and local government systems.

POLICY RECOMMENDATIONS

1. Authorize GO Bonding for Critical Cyberinfrastructure

- Enable large-scale modernization of legacy systems, including platforms such as MAXIS
- Address deferred maintenance in state and county IT systems
- Support phased implementation to reduce service disruption

2. Establish a Dual Funding Structure for Sustainability

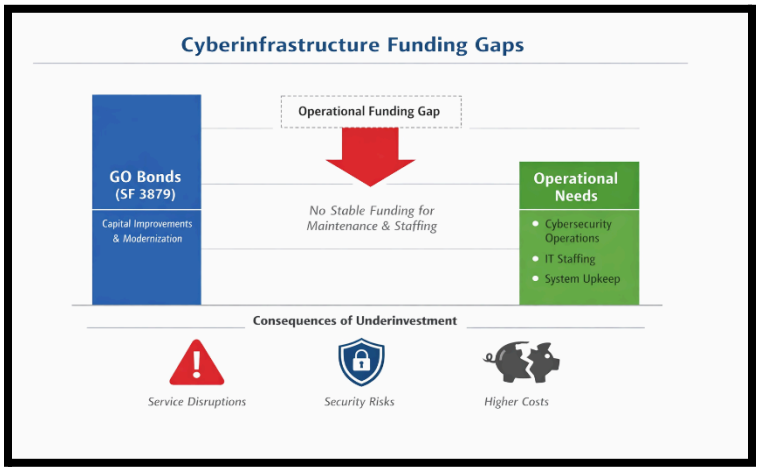
- Pair capital bonding with ongoing General Fund support
- Ensure funding for:
  – System maintenance and upgrades
  – Cybersecurity operations and monitoring
  – IT staffing and retention
- Prevent degradation of modernized systems due to lack of operational funding

5. Improve Data Integration and Accountability Systems

- Invest in interoperable, cross-agency data systems
- Strengthen fraud detection, oversight, and compliance capabilities
- Support real-time reporting and standardized dashboards for decision-making

Minnesota's cyberinfrastructure is essential to delivering public services but remains fragmented, outdated, and unevenly resourced across jurisdictions.

SF 3879 provides an opportunity to modernize foundational systems through GO bonding authority. Building a secure, efficient, and equitable digital government infrastructure for the future will require sustained funding, cybersecurity coordination, data integration, and workforce development.



Ahmed Anshur, Kenneth Eban, Sarah Erickson, Nebiha Mohhamed, Kenny Neimeyer

SarahBErickson57@gmail.com