STATE OF MINNESOTA
Executive Department

Governor Tim Walz

Executive Order 22-20

Directing State Agencies to Implement Cybersecurity Measures to Protect Critical Infrastructure in Minnesota

I, Tim Walz, Governor of the State of Minnesota, by the authority vested in me by the Constitution and applicable statutes, issue the following Executive Order:

The critical infrastructure that protects the health and safety of Minnesotans is facing increasingly sophisticated cyber attacks. Addressing this risk requires both the public and private sectors to coordinate our efforts and harden cyber defenses. Ongoing geopolitical conflicts and the proliferation of organized criminal networks engaged in nefarious cyber activities means that we must strengthen our cyber defenses across our critical infrastructure. We must do all that we can to enhance cybersecurity, especially for critical infrastructure in both the public and private sectors.

My administration has focused on cybersecurity since 2019. We have expanded protections for county governments and school systems through collaborative cybersecurity monitoring programs. The Blue Ribbon Council on Information Technology, which I established in February 2019 via Executive Order 19-02, issued strong recommendations on protecting technology infrastructure and seeking opportunities for increased cybersecurity funding. Collaborations between my administration and the Legislature led to the formation of the Legislative Commission on Cybersecurity, as well the first dedicated funding for state government cybersecurity enhancements in 2019. The Minnesota Fusion Center—a section of the Bureau of Criminal Apprehension ("BCA") at the Department of Public Safety ("DPS")—has cemented strong partnerships between Minnesota's Department of Information Technology Services ("MNIT"), the FBI, and the U.S. Department of Homeland Security, particularly its Cybersecurity and Infrastructure Security Agency ("CISA"). These advancements have made Minnesota more secure, but there is more to do.

State agencies must continue to monitor and reduce cybersecurity risks to critical infrastructure within our state to protect the life, safety, and property of all Minnesotans. Minnesota's critical infrastructure is operated and owned by both the public and private sectors, and we have a shared responsibility to defend it. To elevate Minnesota's critical infrastructure cybersecurity defenses in an evolving threat landscape we need to educate, support, and encourage operators and owners of critical infrastructure to continuously improve their information security programs. In

anticipation of potential cyber threats, state agencies must understand internal risks, as well as risks to Minnesota-based critical infrastructure owners and operators. By taking steps to understand our current cybersecurity posture, we can identify cybersecurity needs and enhance our capabilities to safeguard our interconnected critical infrastructure.

For these reasons, I order as follows:

1. For the purposes of this Executive Order, the terms below are defined as follows:

    a. "Critical Infrastructure" means the 16 critical infrastructure sectors identified by CISA because their assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

    b. "Critical Infrastructure Provider" means an entity that provides services in a Critical Infrastructure sector at such a scale that a cyber attack against the entity would result in a broad-based impact on resource, supply, or service availability within that sector.

    c. "Cyber attack" has the definition used by the Computer Science Resource Center at the National Institute of Standards and Technology: "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."

    d. "Fusion Center" is the Minnesota Fusion Center in the Bureau of Criminal Apprehension as established by the U.S. Department of Homeland Security and authorized in Minnesota under Executive Order 19-22.

    e. "Information Sharing and Analysis Centers" or "ISACs" are trusted entities established by critical infrastructure providers and first authorized by Presidential Decision Directive-63, signed May 22, 1998. Sector-specific ISAC information is available through the National Council of ISACs.

    f. "State agencies" means the departments and agencies listed in Minnesota Statutes 2021, section 15.06, subdivision 1, as well as the Office of Higher Education and the Department of Military Affairs.

2. State agencies must continue to monitor and reduce cybersecurity risks to protect the life and safety of Minnesotans and safeguard property. By September 29, 2022, all state agencies must:

    a. Patch all critical vulnerabilities identified by CISA as Known Exploited Vulnerabilities and implement a plan to maintain compliance with state vulnerability management standards for ongoing vulnerability management.

b. Work with MNIT to document any exceptions for vulnerabilities that cannot be patched in compliance with standards and develop a security plan to reduce risk.

3. State agencies with regulatory oversight over critical infrastructure providers must utilize their existing authority to the extent necessary and permissible to enable providers to perform their own risk assessments and elevate necessary defenses to counter immediate cyber threats. This includes the following directives:

    a. By October 14, 2022, state agencies with regulatory oversight over critical infrastructure providers must, to the extent necessary and permissible under existing authority, inform and assist critical infrastructure providers in registering their appropriate points of contact with the Fusion Center, so that these providers can receive active threat intelligence briefings, stay informed about the evolving threat landscape, and protect their services to ensure continuity of critical services for Minnesotans.

    b. By November 28, 2022, state agencies with regulatory oversight over critical infrastructure providers must, to the extent necessary and permissible under existing authority, and in cooperation with MNIT, provide guidance to these providers on what to do if a cyber attack is detected.

    c. By December 28, 2022, state agencies with regulatory oversight over critical infrastructure providers must, to the extent necessary and permissible under existing authority, and in cooperation with MNIT, develop criteria for provider cybersecurity self-assessments.

    d. By April 4, 2023, state agencies with regulatory oversight over critical infrastructure must examine their authority, and to the extent necessary and permissible under existing authority, require or encourage critical infrastructure providers to annually certify self-assessment completion and compliance with core cybersecurity best practices.

    e. By April 4, 2023, state agencies with regulatory oversight over critical infrastructure must, to the extent necessary and permissible under existing authority, and in cooperation with MNIT, identify additional assessment capabilities to assist critical infrastructure providers with standardized cybersecurity assessments.

4. DPS and MNIT must work together to ensure that state agencies and critical infrastructure providers are prepared for cyber attacks. This includes the following directives:

    a. By October 31, 2022, DPS and MNIT must review and update the Minnesota Emergency Operations Plan ("MEOP") to ensure that the state is prepared to coordinate statewide resources in response to a cyber attack that impacts critical infrastructure.

b. By December 28, 2022, DPS and MNIT must conduct a cybersecurity-specific tabletop exercise, using the updated MEOP. The exercise must include critical infrastructure entities and state agencies with regulatory oversight over critical infrastructure.

5. MNIT must work to ensure that Minnesota's cybersecurity tools and posture are sufficient to respond to a cyber attack. This includes the following directives:

    a. By December 28, 2022, MNIT must engage with state agencies, Constitutional Offices, and other interested state entities to identify opportunities for collaborative procurement and cybersecurity protections.

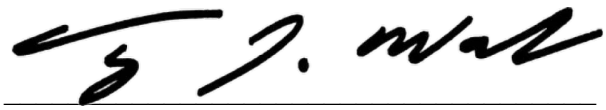
    b. By December 28, 2022, MNIT must develop and implement a vulnerability disclosure program that will allow MNIT to accept, document, validate, and remediate reports of vulnerabilities in government computer systems.

6. State entities not covered by this Executive Order are strongly encouraged to collaborate with MNIT and follow the steps set forth in this Executive Order to protect themselves from cyber attacks. By February 27, 2023, MNIT must develop guidance for such entities. The guidance should include information about reviewing cybersecurity capabilities, vulnerability management best practices, cybersecurity self-assessments, and interactions with the Fusion Center, CISA, and sector-specific ISACs as appropriate.

This Executive Order is effective fifteen days after publication in the State Register and filing with the Secretary of State. It will remain in effect until rescinded by proper authority or until it expires in accordance with Minnesota Statutes 2021, section 4.035, subdivision 3.

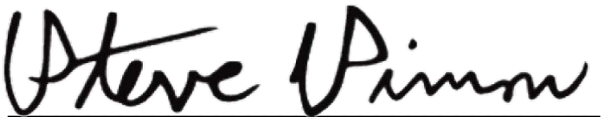
A determination that any provision of this Executive Order is invalid will not affect the enforceability of any other provision of this Executive Order. Rather, the invalid provision will be modified to the extent necessary so that it is enforceable.

Signed on August 30, 2022.



Tim Walz
Governor

Filed According to Law:



Steve Simon
Secretary of State

Document Number: 224183
Filed on August 30, 2022
Office of the Minnesota
Secretary of State, Steve Simon