Legislative Commission on Cybersecurity

Memorandum

DATE: December 14, 2021

TO: Members of the Cybersecurity Commission

FROM: Michelle Weber, Legislative Coordinating Commission

RE: Options Related to Information Provided During Closed Meetings

Minnesota Statute § 3.888, Subd. 5, provides authority for the Cybersecurity Commission to close meetings when necessary to protect the cybersecurity of the state:

> Subd. 5. **Meetings.** The commission must meet at least three times per calendar year. The meetings of the commission are subject to section 3.055, except that the commission may close a meeting when necessary to safeguard the state's cybersecurity. The minutes, recordings, and documents from a closed meeting under this subdivision shall be maintained by the Legislative Coordinating Commission and shall not be made available to the public until eight years after the date of the meeting.

Agencies have indicated that data shared during a closed meeting may still require safeguarding eight years after the date of the meeting and making that information available to the public could jeopardize the cybersecurity of the state.

Members of the Cybersecurity Commission may want to consider amending the commission's enabling statute, Minnesota Statute § 3.888 to protect information shared during a closed meeting. Options may include:

1) Add detail in the statute about confidentiality obligations of members of the commission:
   a) Write confidentiality obligation of commission members into the statute itself, or specifically authorize the commission to adopt confidentiality obligations.
   b) Specify how confidentiality obligations are to be enforced. One option would be to preclude service on the commission by a person who has violated confidentiality obligations.

2) Add detail about the treatment of confidential information after the specified period, currently set at 8 years in the enabling statute.
    a) Change the amount of time for preserving confidential materials.
    b) Change what happens after the specified period. Options include:
        i) Everything automatically becomes available to the public.
        ii) Only those things for which a request is made become public.
        iii) Everything gets destroyed.
        iv) Preservation/destruction is determined by the LCC retention schedule and policies, but everything nevertheless stays confidential.
        v) A review process is conducted to determine whether individual pieces information can be made available to the public or must remain confidential. If this option is pursued, the legislature should consider who should make the determination and who should have input on the decision.

3) Authorization under the government data practices act allowing agencies to share not-public data with the commission.

The options outlined above may require additional changes to the draft *Rules for Closed Meetings* and *Cybersecurity Commission Confidentiality Pledge for Closed Meetings*.