Association *of* Minnesota Counties

February 27, 2025

Re: HF 428

Dear House Judiciary Finance and Civil Law Chair, Rep. Peggy Scott and Committee Members:

The Association of Minnesota Counties (AMC), on behalf of Minnesota's 87 counties, **writes to offer concerns about HF 428.**

The public entrusts their local government with both sensitive and routine data and expects that it is maintained in a secure manner. Counties take this responsibility very seriously and have invested millions of dollars in software, hardware, and other systems to protect government data. We know that the Legislature—entrusted by the public as arbiter of statute—takes seriously its role in balancing the need for open government and sound public policy.

Our concerns with HF 428 fall into three broad categories: **cost, security, and feasibility.**

Storage of records and data is expensive, even if most government correspondence is electronic. If HF 428 is enacted, counties will be required to keep correspondence—including emails, text messages, Microsoft Teams (or other similar software) chat messages, and other electronic messages—for three years. An initial estimate by one county, for example, was $98,000 per year to backup email messages alone. This would not include costs for Teams messages or text messages. Rather than continue using a productive piece of software like Microsoft Teams for employees to exchange messages (and participate in virtual meetings), local governments would move away from Teams or look to disable the chat feature for employees rather than incur additional costs to store thousands of messages.

Cyber criminals work around the clock to breach government systems, including local governments. The threats are organized and smart. They look for ways to attack using least effort and the attack vectors are constantly shifting. Local governments are attempting to mature local cybersecurity controls, but the resources necessary for these cybersecurity improvements are difficult to come by. Simply put, we are vulnerable. In this arena, local governments believe the more information available for cyber criminals to steal, the more damaging a breach will be, which will erode the public trust in local government. Specifically, when a breach via phishing attack occurs, attackers will use any email correspondence to gather email addresses to send malicious phishing links to. The threat multiplies exponentially, and quickly.

Finally, AMC along with other local government organizations are concerned about the review, redaction, and production of such an enormous number of records, should a local government receive a data request. We are glad to perform their legal duty in producing such records upon request. But the reality is that combing through thousands of emails, text messages, and chat messages would lead to longer response times to data requests. While data retrieval is a timely task, the real cost is in using professional staff time to redact private and sensitive data from this information.

Thank you for allowing us this forum to express our concerns. We look forward to continued work on this legislation.

Sincerely,

Nathan Zacharias, Technology Policy Analyst
Association of Minnesota Counties