

March 28, 2017

Senator Mary Kiffmeyer, Chair
Senate State Government Finance and Policy and Elections Committee
3103 Minnesota Senate Building
Saint Paul, MN 55155

Senator Kiffmeyer,

I write to express the concerns of the Office of MN.IT Services related to Senate File 605, the Senate's State Government Finance omnibus bill. As the state agency charged with securing and protecting citizen data and all state agency technology systems, we are particularly concerned that Senate File 605 provides insufficient funding to address immediate cybersecurity needs and cyber threats facing the state. To the extent that Senate File 605 does fund cybersecurity, it largely does so by redirecting existing IT spend from other functions and projects that are critical to the accountable, efficient, and secure delivery of information technology for Minnesota state government.

Consolidating and reducing the State's current datacenter footprint down to a more manageable number is the only cost-effective route to ensuring more secure data center operations - a critical step in bolstering Minnesota's cybersecurity defenses. While the funding mechanisms are problematic, as will be discussed later in this letter, MN.IT appreciates the commitment demonstrated in the bill to funding the data center consolidation initiative, which we estimate will cost roughly \$14 million to achieve in the upcoming biennium. Because the bill mandates the reduction of state data centers from 27 to six during the upcoming biennium, it would essentially mandate that nearly all funding provided in the bill for cybersecurity be spent on data center consolidation.

Data center consolidation, however, is only half of an interdependent, two-part initiative. Data center consolidation is an enabler of improved cybersecurity because it makes implementation of a robust security environment more cost-effective and sustainable. As such, in order to realize the security benefits of data center consolidation, the consolidation must occur alongside investment in cybersecurity tools and services that are fully integrated into consolidated data center operations and IT delivery. These items make up the unfunded portion of MN.IT's cybersecurity change item, as it relates to Senate File 605. As a result, no funding would be available for:

- Needed vendor services including denial of service attack protection, penetration testing, after-hours monitoring, and cybersecurity insurance;
- Advanced cybersecurity tools and their ongoing support; and,
- Cybersecurity staff needed to take action and address vulnerabilities based on the information those security tools provide.

658 Cedar Street, St. Paul, MN 55155

As it relates to the cybersecurity funding that is included in the bill, several problematic mechanisms are employed in order to make the investment. The first mechanism for funding cybersecurity in Senate File 605 is a redirection of \$10 million in already-dedicated IT project dollars from the Information and Telecommunications Technology Systems and Services Account. Most of the projects the bill would de-fund are already in flight and are needed projects to modernize, upgrade or replace systems in order to address identified security issues and support reliable, efficient government operations. Redirecting these projects' existing funding would leave those projects unfinished, create additional risk and security gaps in state systems moving forward, and negate the value of project investments already made.

The second mechanism for funding cybersecurity is an increased general fund appropriation to MN.IT. While the bill does provide \$2 million in new general fund money, it also mandates a reduction in MN.IT's general fund appropriation for the upcoming biennium totaling \$3 million as a result of personnel cost reductions. Language is included in the bill to mitigate this \$3 million reduction by providing for transfers of consolidation savings, but because MN.IT is a chargeback agency, any IT personnel savings that result from consolidation would simply result in reduced charges for agencies. It is unclear how the transfer authority could be utilized without overcharging agencies, violating federal cost allocation requirements, and accruing federal liabilities that would have to be repaid. As a result, the net impact of the two proposals is thus a million dollar reduction in MN.IT's general fund appropriation.

Moreover, this \$3 million mandated reduction would limit MN.IT's options in cost-effectively meeting increased demand from state agencies for IT services and support. Many state agencies are pursuing modernization of aging IT systems, some of which are decades-old. Statutorily-mandated total personnel cost reductions would tie MN.IT's hands in determining how technology projects and information technology services are delivered, likely requiring the State to bring in vendors or contractors for IT work that could be more cost-effectively provided by a state employee.

Lastly, the bill would provide funding for cybersecurity by requiring that \$2.6 million of MN.IT's base general fund appropriation of \$5.2 million be spent on cybersecurity. MN.IT's base general fund appropriation supports leadership and oversight functions that are critical to making continued progress in the IT consolidation initiative, in addition to funding the Minnesota Geospatial Information Office, which coordinates inter-governmental cooperation in the use of geospatial technology and ensures the availability of valuable geographic information systems data to local government, higher education and the private sector. This redirection of base general fund dollars to cybersecurity would simply shift costs to MN.IT's rate package, resulting in increased costs for agencies paying for MN.IT's rate-based services.

The Governor's proposed investment in roughly \$27 million for the upcoming biennium (and roughly \$5 million per year ongoing) reflect the level of investment needed for MN.IT to effectively secure state information technology infrastructure and respond to growing cyber threats targeting citizen data and government systems. Redirecting funds from other important functions creates additional risk and simply shifts the cost of cybersecurity investment to agency operating budgets.

In addition to the \$27 million proposed by Governor Dayton to bolster cyber defense of the State's IT infrastructure, the Governor also proposed investments to secure the software applications that run on MN.IT's

IT infrastructure. Included in this cybersecurity investment package was roughly \$18.2 million for the biennium to increase security, support disaster planning and recovery, and ensure optimal operation of Minnesota Management and Budget's enterprise systems. These systems support accounting, payroll processing, and human resource functions for the entire executive branch and house a large volume of sensitive financial and personal data.

In 2015, systems performing similar human resources functions at the federal level at the Office of Personnel Management were breached, resulting in the theft of roughly 21.5 million personal records and costing the federal government over \$133 million for identity theft protection services alone. MMB's enterprise systems, including SWIFT (the Statewide Integrated Financial Tools) are the backbone to operation and delivery of state government functions and services. SWIFT was first implemented in 2011, has not been upgraded since that time, and will soon be out of software support, making it increasingly vulnerable to intrusion and potential breaches. The State of Minnesota wisely invested in this industry-leading enterprise resource planning software – software that is utilized by leading private sector companies across the globe to support business functions of similar size and complexity. But, like any of our counterparts in the private sector, the value of this investment for the State can be maintained only if we continue to invest in the maintenance and periodic upgrade of the software in alignment with the vendor's timeline for product improvement and support. Failure to upgrade such a product on a reasonable timeline will eventually result in the need for a full replacement of the system – an outcome that would require significantly more resources than those being requested this session.

While cybersecurity threats have existed for some time, the volume and sophistication of those threats has grown exponentially in recent years. With so much of government functions and services reliant on information technology systems, there is little risk of overstating the potential impact to state government of a catastrophic breach or takedown of state technology systems. These risks must be recognized in terms of their financial impact, their impact to ongoing delivery of critical government services, and their impact to the public's trust in their government.

I encourage you and your fellow committee members to reconsider full funding of the Governor's proposed investments in cybersecurity. As always, I am available to answer questions or provide any information you may need as budget deliberations continue.

Sincerely,

A handwritten signature in black ink, appearing to read "A. Baden Jr.", written in a cursive style.

Thomas A. Baden Jr.
Commissioner and State Chief Information Officer

CC: Sen. Jim Carlson, Sen. Julie Rosen, Sen. Richard Cohen