March 5, 2021

The Honorable Mark Koran
Chair
Senate Technology and Reform
Policy Committee
The Minnesota Senate Building
3101 Minnesota Senate Bldg.
St. Paul, MN 55155

The Honorable Torrey Westrom
Vice-Chair
Senate Technology and Reform
Policy Committee
The Minnesota Senate Building
3201 Minnesota Senate Building
St. Paul, MN 55155

The Honorable Omar Fateh
Ranking Minority Member
Senate Technology and Reform
Policy Committee
The Minnesota Senate Building
2325 Minnesota Senate Bldg.
St. Paul, MN 55155

Internet Association Opposes Minnesota's Mandated Government Spyware Bill (SF737)

Dear Senators Koran, Westrom, and Fateh:

Internet Association (IA) represents over 40 of the world's leading internet companies and supports policies that promote and enable internet innovation, including commercial cloud solutions. Our companies are global leaders in the drive to develop lower cost, more secure, scalable, and innovative cloud services to customers in both the private and public sectors. On behalf of our members, we are writing to urge you to oppose SF737, a bill that mandates state information technology contracts use software to document computer use by contractors. Essentially, state business partners would be mandated to install spyware on their employees' computers.

There is a reason dozens of state legislatures rejected this bill year over year and that the National Association of State Chief Information Officers (NASCIO) made the first such statement in opposition to legislation in over 15 years[1]: the impact of implementing this intrusive legislation extends far beyond the world of government contractors and the procurement space. Private citizen data will absolutely end up being exposed, as will sensitive government data and important cyber security infrastructure information.

As written, the spyware that the Minnesota state government would require contractors to install contains code that will take a screenshot at least once every three minutes while continuously storing keystrokes and mouse movement. In a typical 8-hour workday, a screenshot every 3 minutes equates to

[1] *See* NASCIO, NASCIO Opposes Contractor Monitoring Software Legislation (February 21, 2019)

160 screenshots. Extrapolating that out to a 5-day work week and an estimate that each employee would work for 45 weeks during the entire year, conservatively accounting for sick days and paid time off, that would be a total of 36,000 screenshots and 1,800 hours worth of data. This includes personally identifiable information on both residents and government employees, passwords and login credentials for private state-owned networks, as well as certain private network access points that would expose a state agency's cyber security defenses.

The threat posed by this mandated government spyware bill is not potential or theoretical — it is very real and threatens to undo all the incredible work the state has put into setting the literal example for Cybersecurity and IT Modernization efforts[2] in one swift blow.

Take for example, the Minnesota IT Services (MNIT) Information Enterprise Security Office, currently securing "systems at over 1,300 locations" used by "more than 35,000 users" that "are probed and scanned more than 3 million times per day."[3] Any contractors who are supporting the effort to secure the state's most valuable data from cyber criminals will now be *required* to allow mandated government spyware on their systems and risk the potential leak of data transmitted to that spyware provider.

These contractors and the employees they support in the Enterprise Security Office will be responsible to support the review and response to cyber incidents that impact the state. They are often among the "first responders" when a cyber incident breaks out and are often cleared to work with sensitive data and information. With government mandated spyware, there will be 36,000 screenshots of network maps and documentation of currently open vulnerabilities, along with 1,800 hours worth keystrokes typing out passwords and sensitive reports, that will have to be transferred to and then stored by a third-party.

The cost associated with storing, securing, and maintaining this amount of data will result in the state having to pay an extraordinary amount for data storage that is not even capable of being used as a backup or for any other operational purpose. Having in place a multi-year contract and a mandate or preference for contractors that use this software will require the state to commit to spending that could easily go far beyond what had been budgeted, leaving more critical work, such as upgrades and application development, wanting for funding.

Beyond the cost and privacy concerns, this also provides bad actors with a new target that will most likely lack the same information technology hardening tools and techniques available to the government. Much like the SolarWinds incident has proven, public sector entities that provide access to some of their most sensitive data without ensuring they have the appropriate security controls in place is one of the fastest ways to create exposure to disastrous consequences.

This bill will require tens of thousands of desktops across the state to transmit that sensitive data, at intervals of at least every three minutes, with no feasible way to monitor and detect actions that leave that transmission vulnerable until it will simply be too late to act.

Government contractor oversight is a very important goal. Government mandated spyware that leaves

[2] *See* Governor Tim Walz, Minnesota Leads Nation in Cybersecurity and IT Modernization Efforts (December 21, 2021)
[3] *See* MNIT Enterprise Security Office, Securing the State: What is the Threat to Minnesotans? (accessed February 28, 2021)

the state and its data vulnerable is not the way to achieve this goal.

We thank you for taking the time to consider our concerns. We look forward to the opportunity to expand on the privacy and security issues this will undoubtedly create for Minnesotans.

Most sincerely,

Colleen Daley
Director, State Government Affairs, Midwest

Omid Ghaffari-Tabrizi,
Director, Cloud Policy

Cc: The Honorable Rich Draheim
The Honorable David Osmek
The Honorable Lindsey Port
The Honorable Melissa Wiklund