March 25, 2019

Re: Industry Coalition Opposes State Tracking Software Mandates Over Privacy and Security Concerns

An Open Letter to Governors, State Lawmakers, State IT Leaders, and Procurement Officials:

On behalf of our collective business organizations representing contractors across industries providing goods and services to state governments and issue advocacy organizations, we respectfully oppose the legislation requiring government contractors to purchase and install monitoring software on computers used to perform state work that has recently been introduced in several legislatures. Although the exact language varies from state to state, each bill is based on model language being pushed by a single company, ostensibly as a mechanism to increase transparency and oversight in state contracting. While we are supportive of improved transparency and oversight, we are concerned that these bills would present significant privacy and data security risks for both contractors and state governments. As such, we strongly urge legislators to reject these measures.

The specific type of software mandated in these bills automatically collects data on all work performed by the contractor on a computer, including in many instances tracking total keystrokes and mouse event frequency and recording screenshots at least once every three minutes. The software would capture everything including sensitive data like passwords, personal health information, and other personally identifiable information with no mechanism for redaction before being recorded or stored. Furthermore, the legislation would effectively mandate the installation of third-party spyware on state-owned and personal/privately-owned devices for the sole purpose of reclassifying sensitive data for time-keeping purposes.

In many instances these bills would require contractors to store data collected by the software for years after the fact, at great expense and additional risk. For example, a contractor working 40 hours a week would generate 800 screen shots per week. These screenshots, together with any keystroke and mouse data collected, would then have to be secured, stored, backed-up, and made available for real-time access by the state. At a time when most states and businesses have worked together to implement stronger data protection standards, this legislation would undermine existing progress, raise costs, and needlessly expose public and private information to new threat vectors.

It is also unclear who would audit the tracking software to determine whether it is operating as intended. To ensure a level playing field, state agencies would need to monitor and audit software implementation across all professional or technical contractors performing work for the state on computers. This would require additional auditing resources to cover contractors used by the state for engineering, surveying, accounting/financial, legal, environmental, and insurance-related

services, just to name a few. These bills make no appropriation to cover the added costs to the state for such compliance monitoring.

As a result, these bills would likely lead to higher costs for states and taxpayers in two ways. First, the costs associated with purchasing the software and data storage required under the bills could be prohibitive, particularly for smaller vendors, and could result in reduced competition and higher overall costs. Second, vendors that are able to purchase the software and willing to accept the increased privacy and security risks would inevitably build those additional expenses into their bids and pass the costs on to the state.

Lastly, while we understand and support efforts to improve transparency and oversight in government contracting, we do not believe the proposed legislation would accomplish these goals more effectively and at a lower cost than other existing methods for accountability and oversight available to the state. Rather than focusing on process as this legislation proposes, states should evaluate vendors using outcome-driven methods incorporated directly into contracts or acquisition cycles. Adding mechanisms for transparency and oversight at the onset of the RFP process and clearly defining project evaluation methods would achieve the underlying goal of this legislation at lower costs and without the added risks presented by inviting third-party tracking software into public and private IT environments.

Although similar legislation has been introduced across much of the country, we are unaware of any state that has enacted these requirements – and for good reason. We appreciate state leader's thoughtful consideration of our concerns, and respectfully urge you not to move forward with these bills as they would jeopardize the privacy of your constituents, introduce new security risks to state and vendor computer networks, impose impractical and unnecessary requirements on state contractors, and lead to added costs for the state.

Sincerely,

ALEC Action
American Council of Engineering Companies
America's Health Insurance Plans
American Institute of Certified Public Accountants
Associated General Contractors of America
Association of Government Accountants
Computing Technology Industry Association
DHI – Door Security and Safety Professionals
Information Technology Industry Council
National Society of Professional Engineers
NetChoice
Security Industry Association
TechNet
Technology Councils of North America