December 16, 2020

The Honorable Nilsa Cruz-Perez
Senator – District 5
231-L Market St.
Camden, NJ 08102

Internet Association Opposes New Jersey's Mandated Government Spyware Bill (S1965)

Dear Senator Cruz-Perez:

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 hold S1965, 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 (30+ as of the submission of this letter): 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 New Jersey state government would require contractors to install 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 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.

Take for example, the New Jersey Office of Innovation, currently working on a number of projects, including playing "a crucial role in the development and deployment of the State's Contact Tracing technology infrastructure."

Considering the user-centered and data-driven approach that must be undertaken for any responsible development of software applications, something the Office of Innovation is nationally famous for implementing in the state's work as well, there is a great deal of information that New Jersey's residents have and will continue to share with the state's employees and its contractors, allowing the development of an intuitive and effective user experience. This requires user research, which necessitates interacting with users, talking with New Jersey's residents and, in some instances, watching them interact with

government services being delivered to them online or via mobile devices. In the case of the COVID Alert NJ App, this may include health-related data and information that would come up unintentionally and organically as part of the research.

Even further to the point, any contractors who are supporting the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC), will expose a variety of invaluable pieces of data for cyber criminals as a result of the mandated government spyware.

These contractors 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. Beyond the 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 through other means.

These two possibilities are very real and very dangerous.

Adding fuel to this fire - and representing one step forward before taking two steps back - is the impact of this law to the 21st Century Integrated Digital Experience Act, A2614 and its Senate companion S2723. Digitizing the forms being used by New Jersey's residents and adopting the modern technology necessary to support such an effort could very realistically make New Jersey a national leader, if not world leader, in delivering modern and digital government services. This is a positive and laudable step forward.

Should A2614/S2723 and S1965 both pass, the state's residents will no longer benefit from the ability to obtain the best in digital services, as their interactions with the state will always be subject to the government mandated spyware being proposed in S1965. Similarly, the state itself will no longer benefit from the ability to obtain the best in IT cost savings and avoidance, as the cost of working with the state of New Jersey will be higher and the talent pool limited to only those individuals who are willing to work for a company that will require them to do their work on computers that include this spyware.

These would be two very real and critical steps backwards, as S1965 is all cost and no benefit.

A2614/S2723 not only present the state of New Jersey with a large step forward, but it also presents the state with the opportunity, along with the staff at the Office of Innovation, the NJCCIC, and all the other forward thinking agencies and departments that rely on contractor support, to achieve the very same goals without any of the dangerous risks presented by the type of government mandated spyware that would be required under S1965.

As A2614 outlines, commercial cloud solutions and emerging technologies such as artificial intelligence and machine learning will become available to the state in such a way that the use of these technologies will be promoted and prioritized. Through the use of anonymized logging as well as the increased use of the pay-as-you-go service model that is prevalent with commercial cloud-based solutions, the state will never be in the dark about what they are getting for what they are spending while residents and businesses will be confident that whatever they share will be safe.

Government contractor oversight is a very important goal. Government mandated spyware 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 not only the privacy and security concerns we have with S1965 but also on the ways in which A2614/S2723 can provide the state with an even more optimal outcome when it comes to contractor oversight along with a myriad of other benefits.

Very truly yours,

John Olsen
Director, State Government Affairs Northeast

Omid Ghaffari-Tabrizi
Director, Cloud Policy

Cc: Senator Shirley Turner
Assemblywoman Carol Murphy