STATE PRIVACY AND SECURITY COALITION

June 25, 2018

Ryan Smith
Speaker of the House
77 S. High Street
14th Floor
Columbus, OH 43215

Chairman Louis W. Blessing III
House Committee on Government Oversight
and Accountability
77 S. High Street
13th Floor
Columbus, OH 43215

Re: <u>Oppose SB220, "Cybersecurity Safe Harbor" Legislation</u>

Dear Mr. Speaker and Chairman Blessing,

The State Privacy and Security Coalition, a coalition of 23 leading communications, technology, retail, and media companies and six trade associations, writes to oppose SB 220, which purports to create an affirmative defense for companies who implement safe harbor programs. Our members offered amendments in the Senate that would have garnered our support for this bill. However, the direction of this legislation has changed dramatically since its introduction, in ways that deviate from FTC recommended privacy practices and create an artificially high bar over which companies must climb to achieve basic protections.

The overarching problem with the bill is that it incentivizes companies to create cybersecurity practices that focus on the wrong priorities in order to avail itself of the safe harbor protection. In particular, the addition of the "restricted information" definition and category – not found in any other state law – is overbroad, comprising "any" information that can be used to "distinguish or trace" or is "linkable to" an individual. This would cause companies to divert cybersecurity resources from protecting sensitive personal information, the type that hackers can use to steal an individual's identity, to attempting to safeguard information that will often be public in nature. For example, this definition would include nearly all user-generated content, including uploaded photographs, videos, and professional information. We ask that this concept be removed from the bill.

Additionally, we proposed amendments in the Senate, and now propose amendments here, that would strike the phrase "reasonably complies with" and replaces it with " reasonably consistent with" as it relates to the National Institute of Standards and Technology (NIST) framework. This is because the NIST Framework[1] is a voluntary, risk-based approach to cybersecurity that sets minimum security principles, based on existing standards, guidelines, and practices, for critical

[1] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

infrastructure organizations to better manage and reduce cybersecurity risk. It is designed to be flexible and dynamic, allowing each entity to assess its own cybersecurity risk and to develop a program that best mitigates that risk. As such, it is not a standard with which organizations can "comply." Rather, organizations structure programs that are ***consistent with*** the NIST Framework.

In fact, the NIST Framework itself recognizes this distinction, stating that "[b]ecause each organization's risk is unique…the tools and methods used to achieve the outcomes described by the Framework will vary." The document also points out that risk management is an ongoing process, and that "[o]rganizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk." Additionally, in defining the five Framework Core Functions, NIST recognizes that a cybersecurity program is "not intended to form a serial path, or lead to a static desired end state. Rather, the Functions can…form an operational culture that addresses the dynamic cybersecurity risk." Thus, we support striking the phrase "reasonably complies with" and replacing it with "is reasonably consistent with" throughout the bill.

Finally, we request that in addition to the exemption for HIPAA-compliant entities, an exemption be added for entities compliant with the Health Information Technology for Economic and Clinical Health (HI-TECH) Act, as that statute also has extensive data security requirements.

We commend the adoption of thoughtful and meaningful safe harbor legislation that provides appropriate incentives for companies, and with the above changes would support SB 220. I would be happy to discuss our amendments or any other proposals at your convenience.

Respectfully,

Jim Halpert
General Counsel
State Privacy & Security Coalition

cc: Senate President Larry Obhof
Senator Bob Hackett
Senator Kevin Bacon