MIKE DEWINE
OHIO ATTORNEY GENERAL

Administration
30 E. Broad St., 17th Floor
Columbus, OH 43215
614-728-5458
www.OhioAttorneyGeneral.gov

May 16, 2018

The Honorable William Coley
Chairman, Senate Government Oversight and Reform Committee
1 Capitol Square, Statehouse Rm. 140
Columbus, OH 43215

Dear Chairman Coley,

Thank you for allowing me the opportunity to provide more information in support of Senate Bill 220. As the bill has gone through the committee process, I wanted to shed some light on certain points that have been raised by opponents of the bill.

As has been stated in previous testimony, passage of SB 220 will lead Ohio businesses to focus on cyber protections and to invest more resources following comprehensive best practices and industry-specific frameworks. This is a "carrot" instead of a "stick" approach. It prompts business owners and corporate boards to view cybersecurity expenditures as *investments* – not merely as *costs*. SB 220 will improve Ohio's business climate, while also better protecting Ohioans. Companies that invest in strong cyber controls will view Ohio as an ideal state to locate, grow, and thrive.

SB 220 *does not* prevent any citizen from bringing a data breach lawsuit; rather, it provides a legal framework for reviewing such litigation. If SB 220 becomes law in Ohio, our courts will have a comprehensive and logical framework to use to judge those companies that fail to do the right thing. The legislation provides companies that do the right thing a route to argue an affirmative defense. It does not provide an automatic "safe harbor" or protect companies that fail to meet the high bar or negligently fail to protect our personal data.

I would like to discuss the following specific issues that opponents have raised:

- Businesses cannot simply select a cybersecurity plan and state that they are compliant. Businesses have to show action since SB 220 requires a business to "*create, maintain, and comply*" with one of the listed cybersecurity frameworks. This language requires businesses to evaluate and implement new technologies to continue to safeguard their data to qualify as a covered entity under the bill. That means that to be reasonably compliant, a business must remain vigilant.

- NIST as industry Standard. While NIST initially started with the federal government, it has expanded to all sectors and industries. According to the 2018 Information Security Budget and Staffing Outlook provided by the Corporate Executive Board Company (CEB), 82% of organizations used the NIST cybersecurity framework in 2017 compared to only 8% in 2015. According to the survey, the next most popular frameworks were ISO 27000 (61%), NIST 800-53 (43%), and CISC SC (37%). All of these frameworks are included in SB 220. Additionally, each of the cybersecurity frameworks that are

listed in this bill were vetted by the CyberOhio Legal Subcommittee, which consists of legal and technical professionals from across the state.

- Comprehensive cybersecurity frameworks. NIST, along with the other frameworks listed, offers common language and practices that are used across all sectors. Cybersecurity is not as simple as "checking a box" or performing a one-time evaluation. Instead, businesses are required to work on cybersecurity each and every day. The comprehensive frameworks listed cover everything from locking your office doors to recovering your information after a data breach. Essentially, the frameworks cover all aspects of a business' cybersecurity practice.

- Reasonable compliance. It is inappropriate to say that businesses don't know what "reasonable" means. In addition to the expansive history of the term "reasonable" throughout traditional tort law, 13 other states already require businesses to implement "reasonable cybersecurity practices."

- Equifax. SB 220 will not protect wrongdoers, such as Equifax. According to evidence at this time, Equifax had multiple failings in its cybersecurity program, ranging from failing to update its systems to failing to act on notices of potential problems. Thus, small businesses and consumers will still have the ability to collect from companies that do not reasonably comply with the listed frameworks.

- HIPAA. HIPAA is a comprehensive information security framework. HIPAA's privacy rule also establishes appropriate safeguards that healthcare providers and others must achieve to protect health information. Additionally, HIPAA'S breach notification rule prohibits unauthorized disclosures of protected health information. HIPAA is listed in SB 220 because it is a requirement for all healthcare organizations. Thus, if an organization is following HIPAA, it will have a comprehensive security framework. Part of the reason there are more reports of data breaches from organizations under HIPAA is because the statute actually requires notification in several instances.

- SB 220 still allows consumers to recover. Opponent testimony has implied that consumers will not have a right to recovery in a data breach. The "safe harbor" is not automatic; businesses would be required to prove that they were reasonably compliant. This is not a motion to dismiss issue, rather, it will be decided by the trier of fact at trial. Additionally, consumers can still recover through non-tort options, such as breach of contract or statutory violations under Ohio's Consumer Sales Practice Act.

- Guidance for courts. Courts and judges are already deciding cybersecurity cases but they do not have any guidance from the General Assembly regarding what is an appropriate framework. This legislation seeks to concentrate arguments for the plaintiff, defense, and courts so that all businesses in Ohio will have guidance going forward as opposed to a patchwork of different decisions.

- Risk management. A bedrock principle of cybersecurity is risk management, meaning companies have to evaluate their systems and decide which information to protect or where to allocate their resources. Even under current law, consumers do not have the right to tell companies which information should be protected or valued more. To make sure that there is a baseline for businesses to protect the most important information at a minimum, SB 220 contains Ohio's definition of "personal information" (Social Security numbers, credit card numbers, etc.).

- Who should use NIST? The NIST Cybersecurity Framework is for organizations of all sizes and sectors and can be customized for use by any type of business, no matter what the company's level of cybersecurity expertise. A small organization with a low cybersecurity budget or a large corporation with a big budget are each able to approach cybersecurity in a way that best fits their business. It is this flexibility that allows the Framework to be used by organizations that are just getting started in establishing a cybersecurity program while also providing substantial value to organizations with established cybersecurity programs.

- SB 220's frameworks protect against the latest cyber threats. Cyber threats can change each day and a business following any of the frameworks listed in SB 220 will be able to help better protect themselves from evolving cyber threats. To help combat this ever-changing problem, the frameworks contain extensive industry-recognized security controls that guard against fluctuating cyber threats. Examples include anti-malware software, updates to computer systems, employee training, and password safety. Each of these controls helps protect businesses no matter what the latest cyber threat may be.

The legislation before you is the result of nearly two years of work by my office's CyberOhio Advisory Board -- a group of leading cybersecurity experts with very diverse backgrounds. I look forward to continuing to work with interested parties as the issue of cybersecurity evolves. I strongly urge passage of Senate Bill 220 and thank you for your leadership and the opportunity to address the concerns that have been raised in Committee.

Very respectfully yours,

Mike DeWine
Ohio Attorney General