BEFORE THE SENATE GOVERNMENT OVERSIGHT & REFORM COMMITTEE
PROPONENT TESTIMONY ON SB 220
Wednesday, January 10, 2018

Chair Coley, Vice Chair Uecker, Ranking Member Schiavoni, and members of the Senate Government Oversight and Reform Committee, thank you for the opportunity to provide testimony in support to Senate Bill 220 (SB 220). My name is Don Boyd and I am the Director of Labor and Legal Affairs for the Ohio Chamber of Commerce.

The Ohio Chamber is the state's leading business advocate, and we represent nearly 8,000 companies that do business in Ohio. Our mission is to aggressively champion free enterprise, economic competitiveness and growth for the benefit of all Ohioans. The Ohio Chamber of Commerce is a champion for Ohio business, so our state enjoys economic growth and prosperity.

We believe this legislation benefits Ohio's businesses and Ohio's business climate by incentivizing businesses to invest in, and maintain, reasonable cybersecurity measures to protect employee, customer, and other private information. The bill creates what is being termed a legal "safe harbor" for businesses who voluntarily invest in and improve their cybersecurity. This "safe harbor" is an affirmative defense that a business would be able to raise in a lawsuit seeking damages under tort law following a data breach. This is a clear distinction to be made from the outset. It does not bar a lawsuit but provides the opportunity for a business to provide evidence that reasonable policies and protections were in place to prevent the breach and, essentially, provides guidance as to what is reasonable. Judges and juries would still decide, depending on the unique facts and evidence of a case, whether the business meets its burden to raise the affirmative defense provided under this bill.

SB 220 lays out the standards under which a business may utilize the safe harbor. The business's cybersecurity program must protect the security and confidentiality of consumers' personal information, protect against any anticipated threats or hazards to personal information, and protect against unauthorized access of personal information that is likely to result in material risk of identity fraud. The bill states that businesses must not only create but maintain a written cybersecurity program that meets the administrative, technical, and physical safeguards for the protection of personal information guidelines or framework created by the National Institute of Standards and Technology (NIST) or other industry cybersecurity framework described in the bill. The bill goes on to provide five factors to evaluate the reasonableness of the business's program including size and complexity of the business, the resources available to the covered entity, and the nature of the personal information to be protected. This allows for scalability across the spectrum of businesses in the state—from small businesses to Fortune 500 companies.

SB 220 then provides eight industry-recognized cybersecurity frameworks that a business may choose to follow for its program. This provides flexibility and accountability. The bill takes into account the differing nature and needs of businesses throughout the state by allowing the business to choose the framework that makes the most sense for that particular business. While providing flexibility, it also provides accountability by requiring businesses to continually update the processes and procedures of their programs as those frameworks are updated. The bill provides businesses with one year from the effective date of any updates to make the necessary changes.

At the same time, SB 220 is truly voluntary and does not create minimum standards that all businesses in the state would be required to follow. Importantly, the legislation explicitly states that the bill does not create a new cause of action against businesses that choose not to institute a cybersecurity program under this section. Those that choose not to would simply be unable to raise the "safe harbor" or affirmative defense in data breach lawsuit.

At the end of the day, everyone wants their personal information to be protected. This bill provides additional incentive for businesses to voluntarily invest in programs to protect personal data and requires routine maintenance of the programs and procedures. This legislation will build upon the work already done to improve Ohio's legal climate. We appreciate the work of Ohio Attorney General Mike DeWine through the CyberOhio Initiative for spurring this conversation and Senators Hackett and Bacon for bringing forward this legislation. We urge your support for SB 220.Thank you for the opportunity to provide testimony and I would be happy to answer any questions you may have at this time.