MIKE DEWINE
OHIO ATTORNEY GENERAL

Administration
30 E. Broad Street, 17th Floor
Columbus, OH 43215
Office 614-728-5458
Fax 614-466-5087

www.OhioAttorneyGeneral.gov

Senate Bill 220 – Data Protection Act
Senate Government Oversight and Reform Committee
Proponent Testimony – Kimberly Murnieks
January 10, 2018

Chairman Coley, Vice Chairman Uecker, and members of the Committee – thank you for the opportunity to discuss Senate Bill 220, otherwise known as the Data Protection Act. My name is Kim Murnieks, and I am the Chief Operating Officer for Ohio Attorney General Mike DeWine's office.

The number one priority of the Ohio Attorney General's Office is straightforward: Protecting Ohio's Families.

In September 2016, Attorney General DeWine announced the launch of CyberOhio, a collection of cybersecurity initiatives aimed at helping Ohio businesses and consumers fight back against data security threats. The goal of CyberOhio is to help foster a collaborative legal and technical cybersecurity environment to help Ohio businesses thrive. Attorney General DeWine believes that by helping protect Ohio businesses, we protect the privacy and security of Ohio consumers.

To ensure that CyberOhio's efforts are directed appropriately, Attorney General DeWine created the Cybersecurity Advisory Board. The Board is composed of cybersecurity industry experts and business leaders from both the private and public sector, including organizations both large and small. The Board meets quarterly and provides guidance for all initiatives at the Attorney General's Office on cybersecurity.

One of CyberOhio's primary goals is to recommend legislation that will help improve the legal cybersecurity environment in Ohio for businesses and consumers. Senate Bill 220 before you today is the first legislative recommendation that the Advisory Board has made.

The purpose of the Data Protection Act is to encourage businesses to voluntarily adopt strong cybersecurity practices to protect customer data.

To receive the benefit of the Act, a business must implement and maintain a comprehensive cybersecurity program. To provide guidance to businesses, the Act lists eight different industry-recognized cybersecurity frameworks that a business can follow when creating its own cybersecurity program. Businesses are only required to incorporate one of the frameworks into the business' cybersecurity program. Further, businesses are free to choose whichever framework best fits their needs.

Since the cybersecurity needs for a business varies with the size of the business and the type of industry that the business engages in, the Act is "scalable" to the needs of the particular business. In other words, the requirements of the Act depend on the size and scope of each business. The Act lists five factors that a business' cybersecurity program can depend on: (1) the size and

complexity of the business; (2) the nature and scope of the business's activities; (3) the sensitivity of the personal information to be protected; (4) the cost and availability of tools to improve information security and reduce vulnerabilities; and (5) the resources available to the business. Additionally, each of the eight industry-recognized cybersecurity frameworks mentioned in the Act are designed to be scalable as well.

It is important to note that the Act does not create a minimum cybersecurity standard that can be violated and consequently added to a lawsuit against a business owner. In fact, the Act specifically states that it shall not be read to impose liability on businesses who do not comply with the Act's provisions. Instead, if a business implements and maintains a strong cybersecurity program but is still the victim of a data breach, the Act will provide it with an affirmative defense to a lawsuit alleging that a data breach was caused by the business's failure to implement reasonable cybersecurity controls.

The intent is to provide an incentive for businesses to achieve a higher level of cybersecurity through voluntary action. When companies who hold data invest more resources to safeguard that data, Ohio consumers are better protected. Finally, this Act is not meant to serve as an absolute shield for businesses from plaintiff's complaints, but rather, serves as a starting point for this discussion. It is our hope that it will provide guidance and structure to the courts when trying to resolve disputes that involve data breaches.

Chairman Coley and members of the committee, thank you again for your time and attention to this matter. We would also like to thank Senator Hackett and Senator Bacon for their leadership on this legislation. I would be happy to answer any questions you may have.