NJBIA
New Jersey Business & Industry Association

10 W Lafayette Street
Trenton, NJ 08608-2002

609-393-7707
www.njbia.org

To: Members of the Assembly Science, Innovation and Technology Committee

From: Raymond Cantor, Vice President of Government Affairs

Date: February 7, 2022

Re: NJBIA Testimony on Cybersecurity

On behalf of the New Jersey Business & Industry Association, whose members employ one million people in the State of New Jersey, I want to thank you for the opportunity to testify before you today on the issue of cybersecurity. We greatly appreciate the fact that you are taking on this important issue and seeking input from the business community. We are also especially glad to see that this committee has been continued and we look forward to working with you on helping New Jersey to reclaim its place as the innovation state.

NJBIA's members include some of the largest technology and communications providers in the nation, as well as the all the mid-size and mom-and-pop businesses that rely on that technology. For the technology companies, cybersecurity is a priority and a major challenge they are continuing to address as threats emerge. For our smaller companies, especially manufacturers, more needs to be done to ensure that they have the knowledge and the resources to address this growing threat to our economy.

Cybersecurity is a major issue for small businesses. According to the Small Business Association, 88% of small business owners in a recent survey responded that they felt their business was vulnerable to cyberattack. These businesses often lack the knowledge and the resources to adequately protect themselves.

I want to make three points: 1) Our state can best address the threats of cyberattacks by a public-private partnership, where information is shared, rather than a proscriptive set of regulations; 2) There is a need for more information to be shared and training to be done to ensure our businesses are prepared to face this threat; and 3) We need to address the workforce problem where tens of thousands of cybersecurity jobs are unfilled, making us more vulnerable to ransomware and other cyber-attacks.

Public/Private Partnership - We would advise this committee not seek to pass proscriptive legislation which would only lead to inflexible standards in a dynamic world and check the compliance box. It is a waste of resources and can lead to a patchwork of regulatory efforts across the nation.

Rather, we would suggest that a public-private partnership be developed where information is shared, best practices are discussed, and plans are made for prevention and response. Along these lines, we would support AJR 66 and SJR12 that would create a bi-partisan advisory board made up of members of the public and private sectors. The stated purpose of such a board is to: "advise the [state] on cybersecurity concerns, promote awareness, develop effective policies and solutions, and obtain consensus on enterprise-wide initiatives that advance the cybersecurity of information assets and technology resources."

Need for Information – Despite a growing threat of cyberattacks, and the significant list of publicly available resources, there remains a lack of awareness and knowledge by many smaller businesses on how to protect themselves and their customers. Our technology companies do a good job of working with their customers to promote awareness and fend off attacks. There are also public-private partnerships that exist, such as the National Cybersecurity Alliances that coordinates Cybersecurity Awareness Month, the "STOP THINK CONNECT," "Lock Down Your Login," and other public awareness campaigns. Still, given the growing threat, more needs to be done.

Manufacturers who contract with the Department of Defense also have a special need to enhanced security and many of the smaller companies may lack the resources to meet the DOD Cybersecurity Maturity Model Certification. This lack of resources may prevent many companies from being able to compete for bids. New Jersey may want to work with the business community to help facilitate a better understanding of these requirements. NJBIA partners closely with the New Jersey Manufacturers Extension Program (NJMEP), who is a leading expert on these new DOD rules and regulations. NJBIA, NJMEP and the Legislative Manufacturing Caucus can continue our partnership to support New Jersey manufacturers with this cybersecurity issue.

Workforce Development - With these attacks a growing concern for many businesses, it is alarming that there is a workforce gap which persists in this key sector.

Within the last month, the National Academy of Public Administration released a report acknowledging estimates that "half a million cybersecurity positions across the public and private sectors remain unfilled, and that the gap is only expected to grow." NJBIA has been a leader in promoting workforce development issues and we have a formal cooperative partnership with our community colleges to promote workforce development issues across a wide range of business sectors. New Jersey should support cybersecurity and digital citizenship curriculum development at the K-12 and university levels. This committee should continue to engage stakeholders in this area to understand the cybersecurity workforce needs in the state and how to address this gap.

We once again thank this committee and the Chairman for holding this hearing and inviting us to participate. We look forward to continued engagement on this issue.