Ohio House Technology and Innovation Committee
HB 230 (Ray, Hall) State Information Technology Systems
IP Testimony
Wednesday, May 19, 2021

Chairman Frazier and VC Hall, and members of the House Technology and Innovation Committee - Thank you for the opportunity to testify before you today regarding HB 230, and the importance of Cybersecurity in the public sector. I am Bob Scalise, Partner at Tata Consultancy Services (TCS) running our North American Risk and Cyber Strategy practice. I have over 25 years of experience in cyber security, having most recently served as 3 years as a Managing Director in KPMG's Cyber Advisory practice. Prior to KPMG, I spent 10 years at Ernst & Young (EY) in their cyber and risk consulting practices. My background also includes 10 years of leading and managing security and technology teams in industry, for a division of Cisco. And while I've called Atlanta my home for the past 23 years, my real home is still the Midwest, having been born and raised in the Chicago area and obtaining my undergraduate degree from the University of Notre Dame.

I'm here today to bring my perspectives on cyber security for your consideration as you deliberate this important legislation. As the State considers how to move forward in this arena, we are encouraged by the contents of HB230 and the various areas it addresses. Specifically, we believe it is important to establish an office of information technology which oversees and promotes state agency coordination. Having this office accountable to the Governor gives it the right access (much like a Chief Information Security Officer having access to executive management and the Board.) Equally important is the establishment of key positions with delineated responsibilities around information security and privacy, in the positions of Chief Information Officer and Chief Privacy Officer.

This office, as well as those key positions, will be instrumental as the State looks towards modernizing and standardizing its IT infrastructure, patching and updating security, and migrating to the Cloud. Close coordination of State agencies and aligning on a single cybersecurity posture during that transition will be critical to its success. In cybersecurity, the more standardized systems and technology can become, the easier it is to keep them all updated and current, and the easier it is to hire people who specialize in those areas.

We also believe that it's especially important to grow Ohio's cyber efforts in the State. Leveraging the State transformation as an example, establishing educational programs around cybersecurity, especially re-skilling and upskilling programs, will drive digital competitiveness in the State and fill a growing void in cyber talent that exists today. Growing this talent pipeline is especially important to the many companies that are headquartered in Ohio which will be competing for talent nationally and internationally.

Finally, we strongly support the establishment of a cyber and fraud advisory board, especially in light of recent developments around fraud and increased ransomware attacks in general to help guide and oversee these efforts and bring important perspectives to the table. We see public/private partnerships in cybersecurity across all critical infrastructure players as key to the success of defending networks and keeping data safe.

The State of Ohio has an opportunity to take a leadership position in cybersecurity. As you continue your efforts to defend and modernize networks, increase efforts around developing cyber talent and establishing an advisory board, it is important to note that working together with the private sector, as well as across State agencies and law enforcement will be very important.

Thank you for the opportunity to appear before the Committee today, I am happy to answer any questions at this time.