Representative Doug Green
77 S. High St.
13th floor
Columbus, Ohio 43215

Chairman Green, Vice Chair McClain, Ranking Member Sheehy, and members of the House Transportation and Public Safety Committee,

In my years serving in a senior cybersecurity role within the state government of Ohio, I had the opportunity to interact with state agencies, county and local governments, libraries, schools, critical infrastructure providers and institutions of higher education in Ohio whose networks and computer systems were under attack, whose web sites had been comproimised, or whose data had been encrypted and held for ransom. Few of these organizations had the trained cybersecurity personnel needed to respond to the incident in question. Even those organizations large enough to have dedicated cybersecurity positions had difficulty filling them: there aren't enough skilled cybersecurity professionals available in the job market. Complicating the issue further, research funded by the National Institute for Standards and Technology shows that Ohio's need for cybersecurity professionals is much less geographically concentrated than the national average – these skills are needed statewide.

This bill has a number of provisions which seek to address the issues I saw firsthand duing my time in public service. First and foremost is the creation of the Ohio Cyber Reserve.

While a handful of states have created cyber response teams such as the one proposed in this legislation, none of these teams has ever been called out for a cyber event in their state. When the Ohio Cyber Collaboration Committee (OC3) set out to investigate the formation of such teams within Ohio, we tried to understand why this was the case, and to propose a structure which would address those issues, which may be limiting those states' willingness to call them out when needed.

I have had the privilege to serve as the chair of the OC3 subcommittee which has been working on this proposal for over three years. Working with representatives from government, industry, and higher education, this subcommittee carefully considered the situation and possible solutions. We identified several constraints which would need to be addressed in making such teams effective:

- Volunteers must have an official relationship of some type with the state or they will not be used to respond to an incident
- Experienced volunteers will be difficult to attract if we do not provide them the means to perform this work without risking their primary employment
- Universities and community colleges may provide some willing volunteers, but they will need to work closely with more experienced volunteers
- Organizations under attack are far more likely to accept help from an organization they have interacted with under less stressful circumstances

- Most organizations lacking security personnel would benefit greatly from trusted advisors capable of providing concrete guidance on cybersecurity issues

We set out to find the best solution to address all of these constraints and each of them is addressed in the proposed legislation we are discussing today.

The proposal we are considering volunteer teams organized under the Adjutant General's office. Our subcommittee considered many forms of organization, housed under a variety of state agencies or independently. This proposal was the output of many months of work by a team of people with a deep understanding of the issues, with representatives from government, business, and academia from several regions of Ohio. The Ohio Cyber Reserve as proposed in this legislation is widely agree to be the best way to approach this issue.

There are many benefits to the creation of the Ohio Cyber Reserve, and both OC3 as a whole and the subcommittee reviewed proposals to maximize these benefits, and worked with the Adjutant General's office to advise the legislative process on what would be most beneficial for the people of Ohio. The proposed legislation provides several benefits, including the following:

- The teams will be regionally distributed, allowing impacted organizations to get quick, on-site response to issues
- The advisory role these teams will play in their regions will make organizations in their region more resilient to cyber-attack, while building the trust which will make organizations under attack more likely to utilize their services to the best advantage
- The less experienced members will have the opportunity to grow and learn from more experienced members, relieving the more experienced members of some of the more time-consuming tasks, while enabling the less experienced member to develop the years of experience highly sought by employers
- The availability of an experienced cybersecurity workforce and increased infrastructure resiliency to cyber attack will create an attractive business environment for Ohio

Cybersecurity is consistently rated as one of the most significant risks facing organizations today. We believe that this legislation will prepare Ohio to meet these challenges and position us as a leader in defending its organizations and citizens from these risks.

Robert Pardee
Chair, Volunteer Cyber Response Teams Subcommittee
The Ohio Cyber Collaboration Committee (OC3)