Ohio Utilities Protection Service
Proponent Testimony
Substitute Senate Bill 52
House Transportation & Public Safety Committee
May 7, 2019

Chairman Green, Vice Chairman McClain, Ranking Member Sheehy, and members of the House Transportation and Public Safety Committee, thank you for the opportunity to provide proponent testimony on behalf of Substitute Senate Bill 52, which would create a civilian cyber security reserve force in order to protect state, county, and local government agencies, in addition to critical infrastructure and Ohio citizens, from cyber attacks. My name is Alice Miller, Director of Community Affairs for the Ohio Utilities Protection Service, now doing business as OHIO811.

Ohio Utilities Protection Service's key responsibility is to facilitate the "call before you dig" process within Ohio. We manage over one million incoming excavation notifications each year, resulting in almost seven million notices being sent to our members, Ohio's utility providers – whether a large company, a municipality, or small city. Additionally, our Community Affairs Department helps protect Ohio's underground infrastructure beyond the call before you dig process by working with local, state, and federal agencies and associations on various infrastructure protection initiatives. Due to our broad interest in protecting Ohio's critical infrastructure, we support Substitute Senate Bill 52: the organization of a civil cyber security reserve force.

We all know the important role companies the size of American Electric Power, Columbia Gas, AT&T, and others play in providing essential services to Ohio homeowners. However, it is important to recognize that smaller utility companies, municipalities, and cooperatives produce and/or distribute energy, both electric and gas, treat and distribute water, maintain sewer systems, traffic systems, and communication systems for millions of Ohioans. While all of these are important services, let's just look at electricity. According to American Municipal Power there are eighty-three cities in Ohio that distribute electricity to businesses and homeowners within their communities. In 2017, 10,050,151 MWh of electric energy were distributed. This is enough energy to power approximately 1.4 million Ohio homes for a year. Additionally, according to the Ohio Electric Cooperatives, 25 co-ops provide electricity to 380,000 businesses and homes in 77 of the 88 Ohio counties. For more than a million Ohioans who depend on these "smaller" providers, protecting these resources is vital.

Securing the computer systems used to facilitate these services is an ongoing challenge. While some municipalities, particularly the larger ones, have a strong, resilient cyber security system in place, many do not. This is best illustrated by looking at the first-ever nationwide survey about cyber security practices and experiences among municipalities and counties. While the survey looks at municipalities and counties with populations over 25,000, it is safe to say that smaller entities would have the same, and perhaps less, cyber security protection than those identified.

The 2016 International City/County Management Association (ICMA)/University of Maryland's County Cyber Security Survey found the following: 26% of those responding said their system had been attacked *once or more each hour*. 18% cited at least once a day. An attack is defined as "an attempt by any party to gain unauthorized access to any component of your local government's information system for the purpose of causing mischief or doing harm". Additionally, nearly 32% do not know if the attack was initiated externally or internally. A breach was defined as "an incident

that resulted in confirmed disclosure (not just exposure) to an unauthorized party." 2.8% of those responding said their system had been breached hourly or more. Even more concerning is that nearly 28% don't know if their system is being attacked, and 41% don't know if their system is being breached. More often respondents did not know the types of attackers that attacked their system, nor did they keep track of attacks, incidents, or breaches.

When the survey looked at barriers to achieving cyber security, the top three factors identified were: lack of funds, insufficient number of cyber security staff, and inability to pay competitive salaries for cybersecurity personnel. Actions taken to improve cyber security included an audit of cybersecurity practices – almost 39% performed an audit annually and nearly 28% never. Following a breach, 42% never used a forensic service, which could help them understand the scope of the breach and how to prevent one in the future. While many IT and cybersecurity personnel work diligently to keep their systems, the systems we depend upon, safe and secure, Ohio Utilities Protection Service believes the cyber security gaps identified above may be reduced or eliminated by the formation of the Ohio Cyber Reserve.

Features of the Ohio Cyber Reserve model that will benefit Ohio's smaller utility companies, municipalities, and energy cooperatives include essential training, education, and security assessments. These are the rudimentary steps needed by any entity trying to protect their system from intrusion, yet as the ICMA survey shows, are not being taken by many due to lack of funding and/or knowledge. Of course, even with due diligence systems can be compromised. Therefore, the ability of the experts within the Ohio Cyber Reserve to respond to cyber incidents is critical and may reduce the collateral and cascading damages caused by a cyber incident or breach.

Therefore, Ohio Utilities Protection Service urges you to approve Substitute Senate Bill 52 and support the development of an Ohio cyber reserve in order to protect Ohio's infrastructure, an infrastructure that is critical. Chairman and members of the committee, thank you for your consideration on this important issue.