Ohio House Armed Services, Veterans Affairs, and Homeland Security Committee

The Honorable Terry Johnson, Chairman

Major General Mark E. Bartman
Adjutant General of the State of Ohio
Proponent Testimony on House Bill 747
November 27, 2018

Chairman Johnson, Vice Chair Kick, Ranking Member Craig, and members of the House Armed Services, Veterans Affairs, and Homeland Security committee,

I am Major General Mark Bartman, the Adjutant General of the State of Ohio and I would like to thank you for the opportunity to provide proponent testimony in support of HB 747. Under the framework of the Ohio National Guard, this bill seeks to establish the Ohio Cyber Reserve, a civilian force drawn from private sector cyber security experts, organized and nested under the Ohio National Guard, whose mission is to deter, mitigate, and protect critical infrastructure across the State of Ohio from cyber threats.

Almost every day we read of new cyber threats in the media. Foreign governments, criminal enterprises, and malicious

individuals threaten our data, our privacy, and our critical infrastructure.

A few recent examples include Russian hackers gaining access to major electrical utility controls and Iranian operatives stealing $3 billion in intellectual property from 144 U.S. university computer systems. We are under constant assault from cyber criminals.

And Ohio is not immune.

Just this year, a malicious virus wiped data from Riverside, Ohio's public safety servers, and, recently, hackers breached a large central Ohio property management group's servers and stole the personal information of nearly 70,000 senior citizens.

Ohio's citizens, governmental entities and critical infrastructure are at risk, and Ohio's cyber experts are over missioned and understaffed. Small local government entities, such as villages, townships and some counties, do not have the resources or expertise to deal with these cyber threats. Ohio's critical infrastructure needs more protection, especially smaller utilities and emergency services.

Ohio needs a way to tap into the wealth of cyber talent that exists throughout the state and connect that talent to the needs of Ohio, but in a way that is sustainable from a budget perspective, and that provides proper command and control of the response.

We have an opportunity to lead the nation by example in forming a civilian force of cyber warriors to ensure our cyber ecosystems are safe from threats.

Other states have attempted to create a Cyber Reserve type organization with mixed results. Michigan has created an organization called the Michigan Cyber Civilian Corps (MiC3). It is made up of volunteers from the Cyber Security industry designed to work with government, education, private sector organizations, and volunteers to create and implement a rapid response team to be activated under a Governor declared Cyber State of Emergency and to provide mutual aid to government, education, and business organizations. The Michigan Cyber Civilian Corps has been used to mentor students, but has never been used for a cyber incident due to concerns about liability and a lack of official status for its volunteers. They are looking at legislation to try to correct some of those problems.

Wisconsin has built three Cyber Responses Teams (CRTs) of expert government personnel to respond to incidents. Team members are made up of cybersecurity professionals from the Wisconsin Division of Enterprise Technology, other state agencies, and local and county government. This fixes some of the liability problems, but using existing government employees does not grow the pool of responders. It also does not support the educational and mentoring initiatives needed to grow the cyber security workforce pipeline.

HB 747 addresses those shortfalls and sets up a strong cybersecurity response for Ohio.

We believe creating a volunteer firefighter-style Cyber Reserve made up of trained volunteer civilians nested under the Adjutant General's Department will meet the needs of the citizens of Ohio, the Governor, and will help mitigate future threats.

It will be legislatively modeled after the Ohio Military Reserve as outlined in the ORC, Chapter 5920. The Adjutant General's Department will develop appropriate policies to support and regulate the teams.

Costs associated with building and maintaining the Cyber Reserve would require an initial allocation from the State of Ohio of $450,000 in state fiscal year 2019, and then $620,000 and $820,000 in the following two fiscal years.

We will actively recruit volunteers from Ohio's private and public institutions to fill Cyber Response Teams. Companies and cyber professionals have already shown tremendous interest in being involved with the Ohio Cyber Reserve.

These volunteers will be highly vetted with appropriate background checks and training requirements. They will be organized into regionally-based teams. They will be provided training, equipment and credentials and will work out of Ohio National Guard armories.

When fully trained and validated, the teams will be available for call up to assist in cyber response.

The teams will be based in 1 of 5 regions throughout the state. The budget allocations mentioned support two, ten person teams per region and can be expanded based on need, funding, and willing volunteers. We will start with two teams in central Ohio in FY 19 and expand to the rest of the state in FY 20. Each team will have additional volunteers working their way through the training pipeline.

Similarly to how our National Guard is placed on state active duty during a natural disaster, the Governor will be able to call upon the Ohio Cyber Reserve when there are not enough local resources to counter malicious cyberattacks on critical IT infrastructure.

Volunteers who are not yet fully trained, but who have been vetted, can be used to support student mentoring efforts under the Ohio Cyber Collaboration Committee (OC3). They can work primarily with High School STEM teachers to aide in establishing cyber clubs. Additionally, these individuals will engage in community outreach to local civic leaders to establish organizations such as Cyber Explorer Clubs. While the Cyber Reserve members are in training status, they will not be paid. The Cyber Reserve members will have three primary missions: Assist, Educate and Respond. When activated, they will be paid as state civilian employees and will respond to cyber incidents side-by-side with National Guard Cyber Response Teams. They may be called to assist in providing cyber security assessments to underfunded municipalities and designated critical infrastructure organizations.

All of this will work just as our current process does to bring Ohio National Guard members on State Active Duty. Their pay will be based on an equivalent state employee IT position that corresponds with the volunteer's skill level. The estimated daily cost of employing an entire Cyber Response Team is $3,000. Compare this to the average cost of a single data breach for a company in the United States of over $4 million, and the estimated dollar loss in 2015 due to cybercrime worldwide of

over $3 trillion. It is estimated that on average an advanced threat goes undetected on a victim's network for more than eight months before an incident actually occurs. The Cyber Reserve will work to find these breaches, as we say in the military, to the left of the bang, or before the incident.

The Ohio Cyber Reserve is a unique approach to solving a problem that is vexing our nation. Under this bill, Ohio will lead the way for others to follow as we seek to protect our critical assets from cyber harm.

I respectfully ask for your support of House Bill 747 and welcome any questions you may have at this time.