Statement of

Karen Huey

Homeland Security Advisor for the State of Ohio

Assistant Director, Ohio Department of Public Safety

United States Senate
Committee on Homeland Security and Governmental Affairs
Subcommittee on Emerging Threats and Spending Oversight

"Addressing Emerging Cybersecurity Threats to State and Local Government"

June 17, 2021

Introduction

Chair Hassan, Ranking Member Paul and members of the Subcommittee on Emerging Threats and Spending Oversight. My name is Karen Huey, and I am the Assistant Director of the Ohio Department of Public Safety. I also serve as Homeland Security Advisor to Governor Mike DeWine and am a member of the Executive Committee of the Governors Homeland Security Advisors Council. We appreciate the opportunity to share Ohio specific concerns and information with you this morning.

The topic of today's hearing is of great concern to many, and although I speak with you today from the state of Ohio, I know many of my colleagues across the country would echo these same concerns.

Our goals are to enhance cybersecurity across the United States and educate Ohio's local governments and businesses on the importance of taking cyber precautions. Predictions of Cybercrime are estimated to exceed $6 trillion USD globally and could grow 15% per year. The Wall Street Journal June, 2021 interview of FBI Director Christopher Wray stated the FBI was investigating about 100 different types of ransomware and compared the current state of cyberattacks with the challenge posed by the Sept. 11, 2001 terrorist attacks. The damage created by cyber-attacks are well known. Today I would like to share how we believe we could structure our limited resources to make the most impact in Ohio. Preventing cyber-attacks requires dedicated resources, coordinated strategies, and local commitment. Reports of cyber

intrusions and hacks are common, and the amount of time and resources necessary to recover from a cyber-attack is substantial. It can take months to rebuild systems to eventually make a local government, school system, utility, or business whole again. When successful, our state and local governments, critical infrastructure and businesses will have the tools to prevent future cyber-attacks.

Ohio is investing in and making strides in our efforts to strengthen cybersecurity. The Ohio National Guard has brought together more than 30 public, private, military and educational organizations to form the Ohio Cyber Collaboration Committee, known as OC3. The OC3's mission is to provide a collaborative environment to develop a stronger cybersecurity infrastructure and workforce. OC3 has established four subcommittees to help it achieve its primary goals: the Charter & Governance Public Awareness subcommittee, the Education/Workforce Development subcommittee, the Cyber Range subcommittee, and the Cyber Protection and Preparedness subcommittee. These committees are composed of Ohioans with a wide range of cyber and educational expertise dedicated to making Ohio a leader in how to integrate public-private partnerships into solving the cybersecurity problem.

While I have time to share only highlights, I definitely want to mention OC3's great progress with its Cyber Range Institute, which is a virtual training ground and testing site designed to enhance cybersecurity in Ohio. The Range was developed for and used by the Ohio National Guard, schools: from K through 12 and Universities, governments and businesses to train our cybersecurity workforce, to conduct research, test emerging technologies and host cybersecurity exercises and competitions.

Ohio designed a mechanism to bring existing cyber talent to the fight by authorizing the Ohio Cyber Reserve. Formulated by the OC3's Cyber Protection and Preparedness Subcommittee and authorized by the Ohio general assembly in 2019, the Ohio Cyber Reserve consists of a volunteer force of trained cybersecurity civilians, with the goal to function as a military reserve. They are organized in regional teams under the command of the adjutant general. The Cyber Reserve may be called up by the governor to assist government, critical infrastructure, businesses and citizens in a variety of cyber needs. Regional teams are being created and trained, with future duties to include assessing entities for cybersecurity vulnerabilities and making recommendations aimed at reducing cyber threats.

OC3's education and Workforce Development Subcommittee has done substantial work. It was responsible for identifying critically needed skills and it developed training and educational paths to provide skilled workers in the field of cybersecurity. This subcommittee was responsible for encouraging further development of cybersecurity in both K-12 and higher education. Finally this subcommittee trains users at all levels in good cyber hygiene and best cyber practices.

What constraints are we and local governments facing? As this subcommittee is aware, states have been receiving Homeland Security grant funding since 9-11. It has allowed us to build fusion centers, harden targets, identify critical infrastructure and form relationships across sectors that never worked together before. A great example of this occurred last week in Ohio and highlights one serous situation where the federal government's support to the states, locals and territories was felt.

Ohio's dedicated federal homeland security intelligence officer shared information about two Chinese video surveillance technology companies whose products have been banned for purchase or use by federal government agencies since 2018. Despite the federal ban, dozens of these systems were purchased in Ohio, including some school districts, and at least one hospital. In turn, Ohio Homeland Security (OHS) drafted a situational awareness bulletin designed to alert Ohio entities that these companies are likely using their products to provide U.S. customer data to the Chinese government for espionage and surveillance operations. OHS shared the bulletin using the relationships built with homeland security grant funding, including OHS' contact and information system, and forwarded to all Ohio Intelligence Liaisons and Ohio Public Private Partnership members. Almost immediately, responsive emails and phone calls from concerned representatives from Ohio entities that had purchased these products were being received and addressed. High level technical mitigation information has already been shared and CISA personnel are working on a plan with the affected entities that will include a more detailed risk management solution.

Ohio uses homeland security funding to support traditional capabilities, such as interoperable communications, search and rescue capabilities, hazmat, and information and intelligence sharing. Local entities used homeland security funding to build out capabilities to prepare for and respond to critical incidents to sustain a level of preparedness. Current funding is also used to support three fusion centers across the state of Ohio. In addition, we use these funds to support local projects across the eight homeland security regions. With the inclusion of cyber as a priority, Ohio's local governments are struggling even more to address the traditional preparedness needs while also prioritizing cyber projects. As homeland security funding has been static or reduced in the past cycles, forcing cyber into the homeland security grant process reduces already limited funding even further.

As the seventh largest state, with a population over 11 million, Ohio currently receives $6.7 million in homeland security funding. The current carve out for cybersecurity is less than $340,000.

I would assert that continued use of a small portion of homeland security grant dollars both takes away from the needs of traditional homeland security efforts and minimizes the importance of cybersecurity and its impact on state and local governments.

We would urge Congress to consider a dedicated grant program that will enhance Ohio's ability to focus on cybersecurity capabilities. Ohio's annual Stakeholder Preparedness Review identifies gaps in cybersecurity including planning staffing, equipment, training and exercising. Due to sporadic and uneven funding, Ohio's local governments find it challenging to formulate plans that address many of those gaps. Cyber-attacks are not limited to our major cities, and developing strong prevention, education and tabletop exercises will take time and resources.

In light of the resource constraints already mentioned and the increasing volume of cyber incidents, a dedicated program will help ensure we remain prepared for traditional terrorist events and cyber threats, without having to choose between them. It allows state and local Homeland Security efforts to remain focused on terrorism and safety while allocating additional funds to cyber to ensure both state and locals are prepared to respond and mitigate the damages from a cyber-attack.

Dedicated grant funding can be used to develop more robust cyber capabilities at the state level to provide guidance and assistance to local entities that lack the funding and infrastructure to implement cyber programs on their own, or who look to the state for leadership, guidance, and standards.

Three main areas identified for dedicated funding:

1. The state would share industry developed standards with its local governments, critical infrastructure and small businesses. The state would also offer assessments of current systems to improve where gaps are identified and direct local governments to resources. This is especially important for smaller local governments and businesses that do not have resources. In addition, the state would use existing homeland security procedures to ensure that any funding source created would receive monitoring to ensure compliance with grant requirements and appropriate infrastructure to manage grant funding.
2. The state would provide education and training to local governments, critical infrastructure and business entities that will include cyber exercises, end-user training, resources and guidance documents.
3. The state would make improvements to existing secure communication platforms that will be used to gather and disseminate important timely cyber information regarding threats to trusted partners.

Additionally, Ohio recommends that if cyber is a separate funding source, that federal guidance require as a condition of funding that local governments and businesses share indicators of compromise with the state to include: offender IP addresses, offender email addresses, the source of infection, if known, occurrence timelines and investigator contact information. Understanding the scope of the problem will identify better strategies, prevention and mitigation plans. If adopted, we also strongly recommend federal protection of the entity's information related to the existence and details of the cyber incident. Governments and businesses alike will be reluctant to share news or details of cyber incidents when the information could be shared publicly.

Ohio recommends that a dedicated funding source for cybersecurity be set aside or granted in addition to existing homeland security grant funds to build and sustain cybersecurity programs and projects over multiple grant years. This will allow Ohio to develop longer term strategies in partnership with our CISA Cybersecurity Advisor and other federal, state and local partners, ensuring the dollars allocated are a wise investment and produce measurable results.

In closing, many states, just like Ohio, recognize the importance of responding to cyber incidents and building a level of preparedness with our local governments. Our hope is that a dedicated cyber grant program can be created to help state and local governments thoroughly develop robust cyber capabilities to be able to combat the sophisticated efforts of cyber criminals. With many demands on budgets it is difficult to divert such resources or make an impact with only small amounts of funding scattered across the state. We also highly encourage adding a requirement of after action reporting so we can all learn from and be better prepared for incidents in the future.

We appreciate this subcommittee's commitment to addressing cybersecurity threats to state and local governments and hope to continue working with you to implement some of the strategies recommended in the testimony presented today. On behalf of the State of Ohio, thank you for the invitation to testify.