The Authorities
PENNSYLVANIA MUNICIPAL AUTHORITIES ASSOCIATION

Joint Public Hearing

Senate Local Government Committee

Senate Communications and Technology Committee

Public Hearing on *Cybersecurity Issues for Local Governments and Municipal Authorities*

January 31, 2024

Testimony of:

John Berti, IT and Telecom Manager, Wyoming Valley Sanitary Authority

Good afternoon, Majority Chairwomen Brown and Pennycuick, Minority Chairmen Kearney and Dillon as well as members of the Senate Local Government Committee and the Senate Communications and Technology Committee. Thank you for your invitation to provide testimony on *Cybersecurity Issues for Local Governments and Municipal Authorities.*

My name is John Berti, and I am the IT and Telecom Manager at the Wyoming Valley Sanitary Authority (WVSA). I have been with WVSA for 24 years and maintain its data network across five locations. With a service area of 36 municipalities, WVSA provides wastewater treatment services to more than 172,000 residents in Luzerne County.

Today, I am testifying on behalf of the Pennsylvania Municipal Authorities Association (PMAA) which represents over 700 municipal authorities across the Commonwealth, the vast majority of which provide drinking water and wastewater treatment services to more than six million citizens. If you live in Pennsylvania, you are likely within the service area of at least one authority. In addition, PMAA has over 500 associate members, such as certified public accountants, cybersecurity experts, engineers, and solicitors, who provide services to authorities.

I am a past president of the Authorities Association. Also, I have served as Region 3 director as well as been

active on several PMAA committees over the years.

To provide some background, an authority, by virtue of the Municipality Authorities Act (MAA), is an alternate vehicle for accomplishing public purposes rather than through direct action of local governments, such as boroughs, cities, and townships. Municipal authorities may provide services to the community and finance its services by means of user fees. Authorities also commonly serve more than one municipality and in so doing provide operational efficiencies and economies of scale by serving beyond political boundaries. Irrespective of how many communities they serve, the mission of municipal authorities is to provide excellent quality, reliable, and safe services at an affordable cost to the customers of their local community, whether that be large or small. Furthermore, the operation of authority projects and services does not compete with other traditional components and associated costs of local government. To reiterate, for these reasons, the authority model is perfectly suited for providing services on a regional level.

To bolster this viewpoint, it is important to understand the governing structure of a municipal authority. Authorities can be created by any county, borough, city, or township, functioning singly or jointly with one or more other local governments. Once created, the authority manages all aspects of the authority's operation, freeing the municipality of these critical and complex responsibilities. Authorities are governed by a municipally appointed board of directors, and authority meetings are conducted in public, complying with the open meeting requirements of the Sunshine Act. It is also important to note that in the MAA, an authority cannot "duplicate or compete with existing enterprises serving substantially the same purposes." These features ensure that authorities act in a transparent manner, separated from local political influences, but governed locally with full public access, and operate only in the best interests of the communities they serve.

Aside from the MAA, municipal authorities are governed and regulated under numerous other state and federal laws including, but not limited to:

- Safe Drinking Water Act
- Clean Water Act
- Clean Streams Law
- Sewage Facilities Act
- Plumbing System Lead Ban and Notification Act
- Terrorism Infrastructure Disclosure Protection Act
- Public Health Security and Bioterrorism Preparedness and Response Act

- Water Resources Planning Act
- Underground Utility Line Protection Law (PA One Call)
- Water and Wastewater Systems Operators' Certification Act
- Storage Tank and Spill Prevention Act
- Construction Code Act
- Municipalities Planning Code
- Procurement Code
- Prevailing Wage Act
- Separations Act
- Public Official and Employee Ethics Law
- Public Employee Relations Act
- Right-to-Know Law
- Sunshine Act
- Municipal Records Act
- Intergovernmental Cooperation Act

In addition to state and federal laws, authorities must meet all current regulatory requirements as well as plan, prepare, and budget for future requirements once identified by state and federal agencies.

PMAA members, both large and small, each have different means and resources when handling cybersecurity threats. Cybersecurity is an ongoing process and everyone working for a municipal authority has a role to play. Water and wastewater systems provide vital services and are considered critical infrastructure. Furthermore, municipal authorities handle sensitive information that needs to be protected; this includes information on customers and employees as well as technical data on the system itself. Because most municipal authorities rely on automated and distributed system control, any system shutdown because of a cyber-attack can result in public health hazards, environmental dangers, and permit violations.

Municipal authorities are not unlike any other businesses or governmental agencies subject to attack. Simply put…It's not a matter of if, but when. There are a range of approaches that are available to municipal authorities from fundamental strategies that any authority can implement to collaborating with cyber experts, including PMAA associate members who are consultants and insurance providers.

PMAA recognizes the importance of safeguarding municipal authority operations. We work to educate our

members on the potential of cyber threats, how to manage them, how to prepare to respond to them and how to adapt to the constant changes of the digital cyber world. PMAA provides ongoing education and training on cybersecurity to its members through written communications, i.e., our bi-monthly magazine *The Authority* (October 2023 issue – Cybersecurity Month), electronic communications via sharing information from the Environmental Protection Agency and the Cybersecurity and Infrastructure Security Agency, and interactive communications through webinars, management workshops, and our annual conference. We have associate members that are cybersecurity experts ready to serve authority members with all aspects of cybersecurity issues. Beyond firewalls and encryption, one important element is the human factor. Municipal authority employees, partners, and customers can be a significant line of defense if they are educated and implement cybersecurity awareness and fundamental prevention practices. Here are the five we underscore regularly with our members:

1. **Cybersecurity Awareness.** Learn to recognize potential threats such as suspicious emails and text messages.
2. **Building a Security Culture.** Every authority should have a security culture; all the employees should understand that they have a responsibility when it comes to keeping their systems and information secure. It's not just for the IT department.
3. **Phishing Prevention and Email Hygiene.** Certainly, hardware and software solutions are necessary, but we cannot ignore the human element. A very high percentage of cyber-attacks are let in by people too quick to click.
4. **The Internet of Things Security.** Today, everything is connected – computers, phones, watches, tablets, and printers. Secure practices entail granting limited access and isolation from critical systems. Keep the network segmented between employees, customers, and guests.
5. **Artificial Intelligence (AI) for Good and Bad.** While AI can be a positive force; it can also be used for bad purposes. AI generated videos can be used to manipulate information, spread false narratives, and deceive people.

Cybersecurity and the prevention of cyber-attacks is one of the top priorities at WVSA. We know the threat is growing and constant. In 2019, the IT department at WVSA implemented a "KnowBe4" security awareness service to enhance cybersecurity at our treatment plant. This educational tool is just one of the controls in place at WVSA to prevent cyber-attacks. We know that the most common vehicle for a cyber-attack is through email. Malware is inserted into an email that is deviously designed to be legitimate. "KnowBe4" includes training modules that each user on the WVSA data network must take. In addition, there is a feature that includes a testing service. Emails are designed and sent out to WVSA data users that mimic the most common malicious

emails. Emails that alert us to a UPS or FedEx delivery or the end user won a gift card; these are emails that can easily trick the user to click on a link. These tests on recognizing malicious emails are sent out monthly and the results tell us who must retake the training or, in some cases, have their email privileges suspended for a period.

Funding for implementation of cybersecurity measures is far less costly than the potential cost of a security breach. Currently, Pennsylvania does not have a dedicated funding stream to help municipal authorities pay for the cost of cybersecurity upgrades. The federal government created the State and Local Government Cybersecurity Grant Program to provide funding to help state and local governments address cybersecurity risks, strengthen cybersecurity infrastructure and ensure resilience against threats. According to the Pennsylvania Emergency Management Agency, the federal government has allocated $5.2 million for Pennsylvania to continue and expand cybersecurity prevention tools. At present, this funding is not available to municipal authorities. To start, PMAA members believe municipal authorities should be eligible to receive grants under this program. As these funds are only available through 2026, PMAA members also believe a reoccurring state budget line item for municipal authority cybersecurity infrastructure would be helpful.

In addition, PMAA members also support the creation of a state-wide cybersecurity task force to assist local governments with identifying potential cyber threats and developing effective responses. These efforts would help municipal authorities and other local governments establish the proper safeguards against a cyber-attack.

To conclude, cybersecurity risk management is an ongoing process of identifying, analyzing, evaluating, and addressing cybersecurity threats. Every municipal authority is different when it comes to project type, size, operation, capital, and resources and therefore, needs the flexibility to design a cybersecurity program that works best for their community.

Again, thank you for the opportunity to testify before you today. I am happy to answer any questions.