

**House Consumer Protection, Technology and Utilities Committee  
Informational Meeting on *Utility Cybersecurity***

**September 1, 2026**

**Testimony of:  
Craig Fahnestock, Deputy Executive Director of Member Services**

Good morning, Chairman Burgos, Chairman Metzgar, and members of the House Consumer Protection, Technology and Utilities Committee. Thank you for your invitation to provide testimony on *Utility Cybersecurity*.

My name is Craig Fahnestock, and I am testifying on behalf of the Pennsylvania Municipal Authorities Association (PMAA), which represents nearly 700 municipal authorities across the Commonwealth. Authorities provide essential services, including drinking water treatment and distribution, wastewater collection and treatment, solid waste management, and other community projects to roughly six million people in Pennsylvania. PMAA also has more than 500 associate members, including accountants, engineers, solicitors, cybersecurity specialists, and professional services consultants who provide expert support to our member authorities.

Cybersecurity is no longer solely an information technology issue. It is a water supply, wastewater, public health, environmental, and public-safety issue.

Pennsylvania's water and wastewater infrastructure increasingly relies on interconnected information technology (IT) and operational technology (OT), including supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), pumps, valves, sensors, chemical feed systems, and other equipment that controls the treatment and movement of water and wastewater.

A successful cyberattack against these systems can do more than compromise data. It can interfere with the physical operation of a facility, disrupt treatment or distribution, create environmental compliance issues, interrupt service, and undermine public confidence.

PMAA believes Pennsylvania should build upon the significant resources and requirements already in place while providing municipal authorities with the funding, technical assistance, workforce resources, and flexibility necessary to implement effective cybersecurity protections. Our objective should be straightforward: Pennsylvania needs cyber-resilient water and wastewater systems, not simply cyber-secure computer systems.

**Municipal Authorities and the Services They Provide**

1000 North Front Street, Suite 401, Wormleysburg, PA 17043  
717-737-7655 . 717-737-8431 (f) . [info@municipalauthorities.org](mailto:info@municipalauthorities.org)

[municipalauthorities.org](http://municipalauthorities.org)

Under the Municipality Authorities Act (MAA), a municipal authority serves as an alternate vehicle for accomplishing public purposes that might otherwise be carried out directly by boroughs, cities, townships, or counties. Authorities may be created by a county, city, town, borough, township, or school district, either individually or jointly. They are governed by locally appointed boards and operate as independent public entities focused on the services for which they were created.

Authorities frequently serve multiple municipalities, creating operational efficiencies and economies of scale that extend beyond political boundaries. Most importantly, authorities finance their operations through user fees and charges rather than general tax revenues.

Under the MAA, municipal authorities also operate within a distinct statutory framework for establishing the rates and charges necessary to support the services they provide. Section 5607(d)(9) of the MAA authorizes an authority to fix, alter, change, and collect rates and other charges for its facilities at reasonable and uniform rates to be determined by the authority. Those rates may be established for purposes including paying the expenses of the authority and the construction, improvement, repair, maintenance, and operation of its facilities and properties, as well as meeting its debt and contractual obligations.

Regardless of size or geography, the mission of every municipal authority is the same: to deliver high-quality, reliable, and safe services at an affordable cost. Once established, an authority assumes responsibility for all aspects of its operations, relieving the creating municipalities of complex and highly technical responsibilities, while operating independently of other traditional components of local government budgets. This model is particularly well-suited to providing regional services because it combines operational expertise and efficiency with transparency, local governance, and insulation from day-to-day political pressures, while maintaining a clear focus on serving the best interests of the communities involved.

In addition to the MAA, municipal authorities must comply with numerous state and federal requirements, including environmental protection, public health, labor, operator certification, emergency preparedness, procurement, ethics, open records, financial management, and many other areas. Authorities must not only meet these current regulatory obligations but also plan and budget for future requirements as they emerge. This extensive regulatory environment underscores the complexity of authority operations and highlights the importance of protecting the systems that support essential public services.

### **Cybersecurity Is Now a Water Supply, Wastewater, and Public-Safety Issue**

Water and wastewater systems are critical infrastructure. At the same time, these systems are increasingly connected to information networks and, in some cases, directly or indirectly exposed to the internet. The question is no longer whether a cyberattack is possible. The question is whether an authority can continue safe operations when an attack occurs.

Modern water and wastewater facilities rely on both IT and OT. IT systems may include email, billing, customer information, finance, human resources, and administrative computer networks. OT systems may include SCADA, PLCs, human-machine interfaces, pumps, valves, pressure controls, chemical feed systems, sensors, treatment equipment, and other technologies that control the physical operation of a facility.

The distinction matters. A ransomware attack affecting a billing system is serious. But a cyberattack that interferes with a PLC controlling a pump, valve, pressure system, or treatment process can create consequences involving public health, environmental compliance, public safety, and the continuity of essential service.

The Pennsylvania Department of Environmental Protection's (DEP's) current cybersecurity guidance cites a March 3, 2026, Environmental Protection Agency (EPA) alert warning that Iranian government-affiliated and aligned cyber actors have previously exploited internet-exposed OT devices at U.S. water and wastewater systems, in some cases, forcing temporary reversion to manual operations and causing operational impacts.

On April 7, 2026, EPA, in coordination with the Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency, Department of Energy, and U.S. Cyber Command's Cyber National Mission Force, issued a joint cybersecurity advisory warning of ongoing exploitation of internet-connected OT, including PLCs, across multiple U.S. critical infrastructure sectors, including water and wastewater systems. The advisory was subsequently updated on July 22, 2026.

For municipal authorities, cybersecurity can no longer be treated solely as an IT concern. It must be viewed as an essential component of operational resilience, public safety, and responsible infrastructure management.

### **The Threat Environment Continues to Evolve**

The threat environment is becoming more sophisticated. Emerging risks now include the use of artificial intelligence (AI) tools to generate highly convincing phishing emails, impersonation attempts, and other social-engineering attacks. At the same time, attackers increasingly exploit vulnerabilities in internet-connected devices, remote-access technologies, and OT, creating risks that can extend far beyond administrative systems.

Supply-chain vulnerabilities present another growing concern. Municipal authorities frequently rely on outside SCADA integrators, IT providers, managed service providers (MSPs), software providers, equipment manufacturers, and other vendors. This means an authority can have a reasonably secure internal environment while still facing risk through a trusted third party.

These evolving and interconnected threats mean that municipal authorities must plan not only for prevention but also for the full lifecycle of a cyber incident. Effective cybersecurity now requires authorities to identify and reduce vulnerabilities, establish clear response and recovery procedures, and understand their dependence on vendors. In this environment, resilience means not only preventing attacks but also maintaining safe, reliable services when prevention fails.

### **Pennsylvania's Existing Cybersecurity Framework**

It is important to recognize that Pennsylvania and the federal government have already established significant cybersecurity-related requirements and resources for the water sector. The existing framework includes:

1. Pennsylvania emergency preparedness requirements
2. Pennsylvania cyber incident-reporting requirements
3. Mandatory security training for certified operators
4. Federal America's Water Infrastructure Act of 2018 (AWIA) requirements

## 5. State and federal guidance, technical assistance, and training

### **1. Pennsylvania Emergency Preparedness Requirements**

Pennsylvania's drinking water regulatory framework includes requirements for emergency planning and operational preparedness. DEP also provides emergency preparedness resources for water and wastewater facilities and maintains 24-hour emergency contacts for public water systems.

### **2. Pennsylvania's One-Hour Cyber Incident-Reporting Requirement for Public Water Systems**

DEP's current cybersecurity guidance states that a cyberattack qualifies as a situation with the potential to affect water quality or quantity and directs public water systems to report the incident to DEP within one hour of learning of a cyberattack pursuant to 25 Pa. Code § 109.701(a)(3)(iii). DEP also directs systems experiencing a cyberattack to report the incident to the Pennsylvania State Police and encourages reporting to the federal government.

### **3. Mandatory Security Training for Certified Operators**

Pennsylvania's Water and Wastewater Systems Operators' Certification regulations require all certified operators to complete DEP's system security course, "Securing Drinking Water and Wastewater Facilities." The requirement applies to all classifications of certified operators, including operators with grandfathered certificates. Operators must complete the course within the applicable certification cycle, and failure to complete the required training results in loss of the operator's certification.

### **4. Federal AWIA Requirements**

Under Section 2013 of AWIA, community water systems serving more than 3,300 people must develop or update Risk and Resilience Assessments (RRA) and Emergency Response Plans (ERP). These requirements encompass cybersecurity. EPA's AWIA materials state that the RRA must include electronic, computer, and other automated systems, including the security of those systems. The ERP must address strategies and resources for improving the physical security and cybersecurity of the system. These requirements are not one-time exercises. Systems must review their RRA at least every five years and subsequently review and, if necessary, revise their ERP, with the required certifications submitted to EPA.

### **5. State and Federal Guidance, Technical Assistance, and Training**

DEP currently strongly encourages systems to reduce OT exposure to the public internet, replace default OT passwords with strong, unique passwords, and implement multifactor authentication (MFA) for remote access to OT devices. EPA and CISA complement this guidance with resources addressing asset inventories, vulnerability assessments, access controls, network security, backups, incident response, and recovery. EPA also offers a free Water Sector Cybersecurity Evaluation Program that provides cybersecurity assessments and risk-mitigation resources and separately provides technical assistance, planning resources, exercises, and information on available funding. CISA provides additional support through resources and services such as Cyber Resilience Reviews and Cybersecurity Performance Goals.

## PMAA's Commitment to Education and Preparedness

PMAA works continuously to educate and support its members in strengthening cybersecurity awareness, preparedness, and response capabilities. Our approach is comprehensive and ongoing, recognizing that cybersecurity is not a one-time initiative but an evolving responsibility. Our efforts include:

- **Interactive education**, including webinars, podcasts, workshops, symposiums, online member community resources, and annual conference programming dedicated specifically to cybersecurity awareness, governance responsibilities, regulatory developments, and implementation of best practices.
- **Access to subject-matter experts**, including professionals specializing in cybersecurity consulting, risk assessments, incident response planning, and cyber insurance coverage tailored to the unique operational and budgetary realities of our members.
- **Electronic communications**, sharing alerts, threat advisories, and guidance issued by federal partners such as EPA, CISA, and other relevant agencies.
- **Written communications**, including cybersecurity-focused articles in our bimonthly magazine *The Authority*, including the October 2026 issue, which will focus on Cybersecurity Month.

Recognizing that cybersecurity is a responsibility we share with the Commonwealth, PMAA has further demonstrated its commitment by adopting the following resolution as part of our 2026 advocacy platform:

### **Resolution 9-26**

*RESOLVED, That PMAA support legislation providing assistance and funding to municipal authorities for the implementation of new and necessary technologies, as well as employee training, to meet ongoing cybersecurity threats.*

Beyond technology controls such as firewalls and encryption, one of the most important elements of cybersecurity is the human factor. Even the most advanced systems can be compromised through human error, social engineering, or insufficient awareness. Employees, operators, managers, board members, contractors, and vendors can serve as a critical first line of defense when properly informed and trained. Accordingly, PMAA regularly emphasizes the following core practices to foster organizational resilience:

1. **Cybersecurity Awareness.** Learn to recognize potential threats such as suspicious emails, text messages, unexpected password reset requests, unfamiliar attachments, and unusual system behavior.
2. **Building a Security Culture.** Cybersecurity is not solely an IT department function. It is an organizational responsibility that extends from executive leadership and board members to frontline staff.
3. **Phishing Prevention and Email Hygiene.** Many breaches begin with a single click. Ongoing simulated phishing exercises and training are essential.
4. **Network Segmentation and Internet of Things Security.** Today, an increasing number of systems and devices are interconnected. Secure practices include isolating operational systems from administrative networks and maintaining segmentation between employees, customers, and guest networks to minimize the impact of a potential breach.
5. **AI for Good and Bad.** While emerging technologies such as AI can improve system monitoring and threat detection, these same technologies also enable more sophisticated scams, impersonation attempts, and automated attacks.

## **The Municipal Authority Cybersecurity Checklist**

At a minimum, PMAA believes every municipal authority should be able to answer "yes" to the following questions:

- Do we maintain an inventory of our IT and OT assets?
- Do we know which systems and devices are exposed to the public internet?
- Have we eliminated unnecessary internet exposure?
- Have we eliminated default passwords and implemented strong authentication practices?
- Does remote OT access require MFA?
- Is vendor remote access appropriately controlled, limited, and monitored?
- Are IT and OT networks appropriately segmented?
- Do we routinely assess and address vulnerabilities?
- Do we maintain protected and, where appropriate, offline backups?
- Can we continue essential operations manually if critical systems are unavailable?
- Do we know which critical functions must continue during a prolonged technology outage?
- Do we have a written cyber incident-response plan?
- Have we tested that plan?
- Do our operators and employees receive appropriate cybersecurity training?
- Do we know whom to contact and how to respond during a cyber incident?
- Do we consider cybersecurity requirements when purchasing new equipment, software, and services?

This baseline is intended to be a practical foundation, not an endpoint. As the program evolves, PMAA intends to build upon this foundation with the long-term goal of establishing a formal cybersecurity assessment framework for municipal authorities and, ultimately, an accreditation pathway.

### **Cyber Resilience: Maintaining Essential Operations and Workforce Readiness**

Perhaps the most important question for every authority is this: If our SCADA or other digital systems became unavailable at 2:00 a.m. tonight, could our operators safely continue essential operations until those systems were restored? That requires current manual operating procedures, trained operators, emergency contact information, backup communications, appropriate spare equipment, accessible paper-based procedures, independent means of monitoring, and tested procedures for restoring affected systems.

EPA's 2026 National Cyber Drill put this principle into practice. The exercise challenged drinking-water and wastewater utilities to operate and maintain critical functions in an environment where telecommunications and internet access were unavailable or unreliable, along with remote SCADA connectivity, cloud services, and other digital tools. The goal is to test whether utilities can maintain essential functions under progressively degraded conditions and identify dependencies that could prevent them from doing so.

People are just as important as technology. Across the water sector, authorities are investing in workforce preparedness through cybersecurity awareness training, role-based instruction, tabletop exercises, and operational drills.

By investing in workforce education, municipal authorities strengthen one of the most critical elements of their cybersecurity framework: their people. Continuous training, testing, and reinforcement help turn employees from potential points of vulnerability into active participants in system protection and resilience.

## **PMAA's Policy Recommendations**

Based on the considerations outlined above, PMAA respectfully recommends that any statewide cybersecurity legislation involving municipal authorities incorporate the following principles:

- 1. Establish clear eligibility and scope.** Any statewide cybersecurity legislation should clearly define which municipal authorities are subject to the requirements and the specific systems, operations, and information to which those requirements apply. The legislation should avoid broad or ambiguous definitions that could unintentionally subject authorities to requirements that are not appropriate to their size, function, or risk profile. Clear eligibility and scope will allow authorities to develop compliance programs that are appropriately tailored to their operations.
- 2. Use a risk-based, scalable, and framework-neutral approach.** Municipal authorities are not one-size-fits-all. Pennsylvania has authorities serving relatively small communities as well as regional authorities serving hundreds of thousands of customers. Some authorities employ cybersecurity professionals, while others rely on outside IT providers, MSPs, regional resources, consultants, or shared municipal personnel. The systems themselves also vary significantly. A cybersecurity requirement that is reasonable for a large regional system could impose a substantial financial and administrative burden on a small authority without producing a corresponding increase in security. For that reason, any statewide cybersecurity requirements should be risk-based and scalable, defining the cybersecurity capabilities and outcomes expected rather than dictating the technical means by which an authority must achieve them. Legislation should permit authorities to use recognized cybersecurity frameworks, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, where appropriate, while preserving flexibility to use other recognized approaches that are suited to an authority's size, operations, and risk profile.
- 3. Recognize existing compliance.** Any new requirements should recognize cybersecurity programs, policies, controls, certifications, and other compliance measures that authorities may already have in place. Authorities should receive appropriate credit for meeting substantially similar requirements under existing state and federal laws, regulations, standards, grants, contracts, or recognized cybersecurity frameworks, including the NIST CSF 2.0, where applicable. This approach would allow resources to be directed toward addressing actual cybersecurity gaps rather than requiring authorities to recreate processes that already provide meaningful protection.
- 4. Conduct a regulatory crosswalk.** Existing state and federal requirements should first be identified and evaluated before imposing any new cybersecurity requirements. This approach focuses on identifying gaps in the current framework and designing any additional requirements to complement, rather than duplicate, existing obligations. Doing so can provide meaningful protection without creating unnecessary compliance burdens.
- 5. Coordinate with CIRCIA and avoid duplicative reporting.** The federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) establishes a federal framework for cyber incident reporting, and CISA continues its rulemaking process to implement CIRCIA. Any statewide cybersecurity framework should therefore be designed to coordinate with the federal CIRCIA framework and other applicable federal reporting requirements. State-specific reporting requirements

should not create duplicative or conflicting obligations involving different definitions, reporting thresholds, deadlines, agencies, or reporting mechanisms. At a minimum, any statewide legislation should coordinate with CIRCIA and provide a mechanism through which federal reporting can satisfy substantially similar requirements. This approach would allow authorities to focus limited resources on identifying, responding to, and mitigating cybersecurity threats while reducing administrative burdens. The final federal reporting requirements and their effective date should therefore be monitored as the rulemaking proceeds.

6. **Provide for phased implementation and reasonable compliance periods.** Any new statewide cybersecurity requirements should be implemented through a reasonable, phased approach that recognizes the time necessary for authorities to assess existing cybersecurity capabilities, identify gaps, develop plans, obtain funding, procure equipment and services, modify contracts, hire or train personnel, and implement new controls. Implementation schedules should be appropriately scaled to the size, complexity, and risk profile of the authority and should provide additional time where compliance requires substantial capital investment, procurement, system replacement, or other significant operational changes. The framework should also distinguish between planning and assessment requirements and more resource-intensive implementation requirements and should provide reasonable technical assistance and guidance during the implementation period. Phased implementation will allow authorities to make meaningful progress toward improved cybersecurity without creating unnecessary disruption or requiring rushed investments that may not produce the most effective risk reduction.
7. **Make requirements technology neutral.** Cybersecurity technology changes rapidly. Technology that represents best practice today may be outdated several years from now. Legislation should therefore establish reasonable cybersecurity outcomes rather than prescribe specific products, architectures, or technologies.
8. **Address vendor and supply-chain risk.** EPA provides a Cybersecurity Procurement Evaluation Checklist specifically intended to help evaluate the cybersecurity practices of vendors, manufacturers, integrators, and MSPs. Authorities should know who installed and maintains their systems, who can access them remotely, and what security controls govern that access. This includes addressing appropriate controls such as MFA, limiting remote access, using unique vendor accounts, disabling inactive accounts, logging vendor activity, knowing when vendors connect, and understanding the risks if a vendor is compromised. Title 62's procurement provisions applicable to local authorities should also include language establishing appropriate cybersecurity criteria for the pre-qualification or selection of vendors providing technology, operational, or managed services to municipal authorities. At the same time, authorities should not be held responsible for cybersecurity risks outside their control, particularly vulnerabilities in third-party software, equipment, or services. Therefore, responsibility should be appropriately shared across the supply chain, with each party accountable for risks within its control.
9. **Provide funding and recognize impacts on ratepayers.** Any new cybersecurity requirements should be accompanied by adequate and sustainable funding mechanisms that recognize both initial capital investments and ongoing operating costs, including technology, licensing, monitoring, training, assessments, professional services, personnel, incident response, and system upgrades. Imposing new cybersecurity obligations without corresponding funding could divert resources from other essential services and infrastructure needs. Cybersecurity requirements should also be appropriately scaled for the risks presented and implemented in a manner that avoids placing disproportionate financial burdens on authorities and their ratepayers. Municipal authorities already operate under an established statutory framework for financing the cost of providing their services. Reasonable cybersecurity expenditures that are necessary to protect and maintain those facilities and provide safe and reliable service may therefore

be considered through an authority's existing budgeting and rate-setting processes. At the same time, cost recovery through existing rate-setting mechanisms does not eliminate the impact on ratepayers. Customers may ultimately bear some or all of the costs of the services they receive, and significant new cybersecurity mandates can therefore affect affordability, particularly for smaller authorities or communities with limited financial resources. Any statewide cybersecurity framework should recognize this reality and should provide flexibility, reasonable implementation periods, technical assistance, and opportunities for state and federal funding so that authorities can meet legitimate cybersecurity objectives without imposing unnecessary or disproportionate costs on ratepayers. State and federal appropriations, grants, technical assistance, shared services, and other funding opportunities should be considered as part of any new statewide cybersecurity framework.

- 10. Preserve local operational decision-making.** Statewide legislation should establish reasonable cybersecurity expectations while preserving the ability of municipal authorities to determine how those expectations are best implemented based on their individual systems, resources, operational needs, and risk profiles. The distributed nature of authority systems can itself provide a resilience advantage by helping to limit the potential scope of a cyberattack or operational failure, particularly where systems are appropriately segmented and independently managed. Any requirements should provide objectives and accountability without unnecessarily dictating local operational decisions and should complement the existing municipal authority structure.
- 11. Protect sensitive cybersecurity information.** Any new oversight or reporting framework should recognize that publicly disclosing cybersecurity information can create a security risk. Authorities should be encouraged to share relevant information with state and federal cybersecurity partners when doing so can strengthen security, while ensuring that sensitive cybersecurity information receives appropriate confidentiality protection.
- 12. Provide good-faith protection.** Cybersecurity measures can reduce risk, but they cannot guarantee that a successful cyberattack will never occur. A cyber incident should therefore not, by itself, establish a violation of a cybersecurity requirement or impose liability on an authority. Likewise, good-faith compliance with a statutory cybersecurity framework, recognized cybersecurity framework, or documented risk management program should not constitute evidence of negligence or fault merely because an incident occurs. Accordingly, any new requirements should establish reasonable risk-management expectations, not impose an expectation of perfect security. Authorities should be encouraged to identify vulnerabilities, report incidents, and seek assistance rather than conceal problems out of fear that acknowledging a vulnerability will automatically create liability. Any protection should be limited to good-faith compliance and should not preclude liability arising from independently wrongful conduct, willful misconduct, or other conduct for which liability is otherwise established under applicable law for third-party actors.
- 13. Measure success by risk reduction.** The effectiveness of any statewide cybersecurity framework should be evaluated based on whether it meaningfully reduces cybersecurity risk and improves the ability of authorities to prevent, detect, respond to, and recover from incidents. Compliance should not be measured solely by the number of mandates adopted. Instead, the framework should encourage authorities to identify and prioritize their most significant risks, address vulnerabilities, strengthen resilience, and demonstrate meaningful improvement in their overall cybersecurity posture. This risk-based approach can also help ensure that limited authority and ratepayer resources are directed toward cybersecurity investments that provide the greatest practical reduction in risk.

## Conclusion

Cybersecurity risk management is an ongoing and dynamic process of identifying, analyzing, evaluating, and addressing threats. Every municipal authority differs in size, operational complexity, and financial capacity. Therefore, flexibility is essential. Authorities must be empowered, not overburdened, with the tools, funding, and technical support necessary to protect critical infrastructure effectively.

Pennsylvania already has important pieces of the framework in place, including emergency preparedness requirements, cyber incident-reporting requirements, mandatory operator security training, federal AWIA requirements, state and federal cybersecurity guidance, technical assistance, vulnerability assessments, and organizations such as DEP, CISA, and EPA that can help authorities prepare for, respond to, and recover from cybersecurity incidents.

As the General Assembly considers additional cybersecurity requirements, it is equally important to recognize the statutory framework under which municipal authorities operate. The MAA provides an existing mechanism through which appropriate cybersecurity costs can be considered as part of the cost of providing safe and reliable service. At the same time, because those costs can ultimately affect ratepayers, cybersecurity requirements should be risk-based, scalable, and accompanied by appropriate flexibility, technical assistance, reasonable implementation periods, and funding opportunities. The goal should not be to choose between stronger cybersecurity and affordable public services. Both can be pursued by establishing reasonable statewide expectations while respecting the independent governance, statutory authority, and existing rate-setting framework of municipal authorities.

A successful approach must ensure that every authority has the resources, expertise, and flexibility necessary to put appropriate cybersecurity measures into practice. Investing in cybersecurity is an investment in the reliability and resilience of Pennsylvania's critical infrastructure and can help reduce the financial, operational, and public consequences of a successful cyberattack. Protecting Pennsylvania's water systems and other essential services is not merely an operational responsibility; it is a foundational obligation tied directly to safeguarding public health, preserving environmental quality, maintaining economic stability, and ensuring the long-term resilience of our communities. When these systems are secure and reliable, they protect families, support local businesses, sustain ecosystems, and reinforce public confidence in government's ability to deliver critical services without interruption.

For these reasons, Pennsylvania's cybersecurity framework should seek to establish meaningful statewide protections while providing municipal authorities with the flexibility, resources, and support necessary to meet those expectations. A balanced, risk-based approach can strengthen cybersecurity without placing unreasonable burdens on the authorities and ratepayers responsible for sustaining these essential services.

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