DANILO BURGOS, MEMBER
197TH LEGISLATIVE DISTRICT

106 IRVIS OFFICE BUILDING
P.O. BOX 202197
HARRISBURG, PENNSYLVANIA 17120-2197
(717) 772-2004
FAX: (717) 780-4784

635 WEST ERIE AVENUE
PHILADELPHIA, PENNSYLVANIA 19140
(215) 223-1890
FAX: (215) 223-1959

House of Representatives
COMMONWEALTH OF PENNSYLVANIA
HARRISBURG

COMMITTEES

CONSUMER PROTECTION, TECHNOLOGY & UTILITIES, CHAIR
POLICY COMMITTEE

CAUCUSES

PHILADELPHIA HOUSE DELEGATION
WELCOMING PA CAUCUS, CO-CHAIR
ASIAN PACIFIC AMERICAN CAUCUS
CLIMATE CAUCUS
COMMUNITY COLLEGE CAUCUS
EMERGING TECHNOLOGIES CAUCUS
LGBTQ EQUALITY CAUCUS
OIL & GAS CAUCUS
PA COMMUNITY PHARMACY CAUCUS
PA LEGISLATIVE LATINO CAUCUS
PA SAFE CAUCUS
PENNSYLVANIA LEGISLATIVE BLACK CAUCUS
WOMEN'S HEALTH CAUCUS

House Consumer Protection, Technology and Utilities Committee

Subcommittee on Utilities

Informational Meeting Agenda – Utility Cybersecurity

September 1, 2026

9:30am

515 Irvis Office Building

Call to Order

Subcommittee Chairman Gallagher

Opening Remarks

Majority Subcommittee Chairman, Rep. Gallagher

Republican Subcommittee Chairman, Rep. Williams

Panel #1 (Regulators and Cybersecurity)

Pennsylvania Public Utility Commission - Stephen DeFrank, Chairman

Federal Resources Corporation - Jeremy Young, CEO

Member Q and A

Panel #2 (Water Utilities)

Pennsylvania Municipal Authorities Association - Craig Fahnestock, Deputy Executive Director of Member Services

National Association of Water Companies PA Chapter - Sumit Nair, Chief Information Officer, Essential Utilities

Member Q and A

Panel #3 (Electric Utilities)

Energy Association of Pennsylvania - Brian Harrell, Chief Security Officer, First Energy

PJM - Steve McElwee, Vice President and Chief Security Officer

Member Q and A

Panel #4 (Gas Utilities)

Essential Utilities (Peoples Natural Gas) - Sumit Nair, Chief Information Officer, Essential Utilities

Philadelphia Gas Works - Qian (Jackie) Zhou, Director of Cyber Security, Information Services

Member Q and A

Closing Remarks

Majority Subcommittee Chairman Gallagher

Republican Subcommittee Chairman, Rep. Williams

Adjournment

Prepared Testimony of

Stephen M. DeFrank

Chairman, Pennsylvania Public Utility Commission

before the

House Consumer Protection, Technology and Utilities Committee

September 1, 2026

Pennsylvania Public Utility Commission

400 North Street, Harrisburg, Pennsylvania 17120

Telephone: (717) 787-4301

http://www.puc.pa.gov

Introduction

Good morning, Chairman Burgos, Chairman Metzgar, Subcommittee Chairmen Gallagher and Williams, and members of the House Consumer Protection, Technology and Utilities Committee. My name is Stephen M. DeFrank, Chairman of the Public Utility Commission (Commission or PUC). I appreciate the opportunity to testify before the Committee today at this informational meeting and briefing on the critical topic of utility cybersecurity mandates, ratepayer cost allocation, and regulatory oversight.

The Commission is charged with ensuring that essential utility services remain safe, reliable, and affordable for all residents and businesses across the Commonwealth. As critical infrastructure systems increasingly rely on interconnected digital networks, cloud environments, industrial control systems, and operational technology (OT) to deliver essential electric, natural gas, water, wastewater, and steam services, safeguarding these assets against sophisticated cyber threats is fundamental to both utility reliability and public safety.

At the same time, Pennsylvania ratepayers deserve secure, resilient utility services without bearing unreasonable or excessive financial burdens for baseline security compliance. Balancing robust critical infrastructure protection with consumer affordability and ratepayer protection lies at the heart of the Commission's mission.

I am pleased to highlight the Commission's proactive cybersecurity initiatives as I discuss the history and scope of the Commission's cybersecurity oversight, the role of the Office of Cybersecurity Compliance and Oversight (OCCO), the proposed rulemaking to enhance utility cybersecurity requirements and incident reporting, and ratepayer protection and cost allocation principles.

History and Scope of the Commission's Cybersecurity Oversight

The evolution of the Commission's cybersecurity framework spans more than two decades. The Commission's formal involvement in physical and cyber utility preparedness primarily began in the wake of the events of September 11, 2001. In House Resolution 361 of 2001, the House of Representatives directed the Commission and the Pennsylvania Emergency Management Agency (PEMA) to evaluate security protections across the Commonwealth's critical utility infrastructure.

In 2005, after the Commission's entry of initial orders regarding physical and cybersecurity planning and self-certification,[1] the Commission promulgated public utility preparedness regulations at 52 Pa. Code Chapter 101 to require jurisdictional utilities to develop and maintain written physical security,

[1] *See e.g., Physical and Cyber Security Program Self Certification Requirements for Public Utilities*, Docket No. M-00031717 (Order entered December 9, 2003).

cybersecurity, emergency response, and business continuity plans verified via an annual Self-Certification Form.[2] The following year, Act 156 of 2006, also known as the Public Utility Confidential Security Information Disclosure Protection Act, was signed into law ensuring that sensitive vulnerability assessments, emergency response plans, and security filings are safeguarded from public disclosure for the protection of life, safety, and public utility facilities.[3]

In 2009, the Commission clarified that all distribution infrastructure assets must be covered in utility cyber plans.[4] Shortly thereafter, in 2011, cyber-attack reporting was incorporated into the Commission's utility accident reporting regulations.[5] The Commission later updated its steam safety regulations in Chapter 61 to require cyber plans and reporting for jurisdictional steam utilities.[6]

The Commission created an internal Cyber Team in 2012 with members from the Office of Executive Director, the Bureau of Audits, the Office of Management Information Systems, the Bureau of Technical Utility Services, the Bureau of Technical Utility Services, the Law Bureau, and the Office of Communications.

The Commission has also worked closely with other agencies and organizations on cybersecurity measures. For instance, the Commission convened multi-agency collaborations with the Federal Energy Regulatory Commission (FERC), the Federal Communications Commission, the Pennsylvania State Police (PSP), and the Governor's Office of Homeland Security (GOHS). In 2014, the Commission formed the Critical Infrastructure Interdependency Working Group and released its first edition of Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities. In 2015, the Commission entered into a formal Memorandum of Understanding with the PSP to actively participate in the Pennsylvania Criminal Intelligence Center (PaCIC) Fusion Center and, in 2016, the Commission initiated cross-sector Black Sky emergency exercises.

The Role of the Office of Cybersecurity Compliance Oversight

The Commission took the important step of formally establishing the OCCO and appointed a dedicated Director to lead the agency's cybersecurity oversight initiatives in 2018. The OCCO serves as the Commission's principal technical advisor on all external utility cybersecurity matters.

The OCCO handles incident response and emergency coordination by serving as the

---

[2] *Rulemaking re: Public Utility Security Planning and Readiness*, Docket No. L-00040166 (Revised Final Rulemaking Order entered March 10, 2005).
[3] 35 P.S. §§ 2141.1, *et seq*.
[4] *Cyber Security Plans Required by 52 Pa. Code §§ 101.1, et seq*., Docket No. M-2009-2104273 (Order entered August 3, 2009).
[5] 52 Pa. Code §§ 57.11, 59.11, 65.2.
[6] 52 Pa. Code §§ 61.11, 61.45.

Commission's immediate contact for utilities during active cyber incidents and directing the Commission's Cybersecurity Incident Response Team. The OCCO Director is the Chairman's designee for cybersecurity matters on the Governor's Emergency Management Council during activation of the Commonwealth Response Coordination Center and leads agency execution under the Pennsylvania Cyber Incident Index. The OCCO also conducts rigorous After-Action Reviews following incidents.

Additionally, the OCCO actively monitors real-time threat intelligence feeds from PaCIC, PEMA, GOHS, the Cybersecurity and Infrastructure Security Agency (CISA), FERC, National Electric Reliability Cooperation's (NERC), and multi-sector Information Sharing and Analysis Centers (ISACs) (E-ISAC, ONG-ISAC, Water-ISAC, MS-ISAC), coordinating the issuance of immediate Secretarial Letter advisories and alerts to vulnerable utilities. For example, in March 2026, the Commission issued a Secretarial Letter to all jurisdictional utilities and licensed electric generation suppliers and natural gas suppliers to share recommendations due to the potential for increased cyber activity targeting domestic critical infrastructure. More recently, in July 2026, the Commission issued a Secretarial Letter to all jurisdictional water and wastewater utilities regarding recommendations to prevent the exploitation of OT systems.

In terms of utility training and preparedness, the OCCO participates in national exercises, including CISA training, NERC GridEx, and the Electric Infrastructure Security Council's Black Sky drills, and leads Commission-wide incident simulations. The OCCO also conducts dedicated cybersecurity training programs, seminars, and conferences to help assist resource-constrained small and mid-sized utility systems with developing and implementing Governance, Risk, and Compliance programs.

In an advisory role, the OCCO delivers annual cybersecurity threat assessments and advises Commissioners and the Executive Director on state and national policy, legislation, and emerging technologies. The OCCO also advises Commission staff on formal proceedings involving utility failures to comply with cybersecurity obligations under the Commission's regulations and the Public Utility Code. Additionally, the OCCO advises the Commission on the reasonableness and prudency of cost recovery claimed in base rate cases for utility cybersecurity capital expenditures, software investments, and incident response claims. Further, the OCCO collaborates with the Bureau of Audits to design inspection protocols, under 66 Pa.C.S. § 516, ensuring that periodic management audits of large electric, natural gas, and water utilities evaluate cybersecurity programs against the appropriate standards. The OCCO also works with the Office of Legislative Affairs to shape regulatory priorities and the Law Bureau in coordinating cybersecurity rulemakings.

Proposed Rulemaking to Enhance Utility Cybersecurity Requirements and Incident Reporting

On June 18, 2026, the Commission voted 5-0 to approve a comprehensive Notice of Proposed Rulemaking (NOPR).[7] Guided by the OCCO's technical analysis, this rulemaking transitions from a self-certification to an objective, verifiable regulatory framework.

Evaluations, Programs, Standards, and Plans

The NOPR modifies Commission regulations by removing cybersecurity from 52 Pa. Code Chapter 101, which remains dedicated to Physical Security, Emergency Response, and Business Continuity, and creating a new Chapter 103 regarding Evaluations, Programs, Standards, and Plans to impose objective standards grounded in the National Institute of Standards and Technology protocols. Specifically, Chapter 103 would incorporate the following:

- NIST Cybersecurity Framework guidance on standards, guidelines, and practices to help organizations manage and reduce cybersecurity risk;
- NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organization (NIST SP 800-53) regarding security and privacy controls designed to protect information systems and organizations from diverse threats; and
- NIST Special Publication 800-82, Revision 3: Guide to Operational Technology (OT) Security (NIST SP 800-82), which is designed to protect hardware and software that monitors, manages, or controls physical equipment and processes given that traditional IT security standards focus on protecting data confidentiality and cannot be copied directly over to industrial settings where human safety and continuous equipment availability are the top priorities.

The NOPR also aims to bridge IT networks and operational environments to avoid a burdensome "one-size-fits-all" mandate. In this regard, Chapter 103 establishes a tiered classification framework based on the number of customers a public utility serves and its digital risk profile, which would be as follows:

- **Class 1 (100,000+ customers):** Required to conduct annual evaluations using CISA's Cybersecurity Evaluation Tool (CSET) across NIST CSF,

[7] *Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting*, Docket No. L-2022-3034353 (Order entered June 24, 2026).

SP800-53, and SP 800-82, and maintain seven formal programs: governance, security management, vulnerability management, risk management, threat management, incident response, and recovery management.

- **Class 2 (3,300 to 99,999 customers):** Required to conduct annual CSET evaluations under NIST CSF and maintain the same comprehensive core security programs.
- **Class 3 (< 3,300 customers) & Class 4 (Common Carriers with IT/OT/PI):** Required to conduct annual CSET NIST CSF assessments and maintain an annually updated cybersecurity plan, vulnerability assessment, risk mitigation plan, incident response plan, COOP, and disaster recovery plan.
- **Class 5 (No IT, OT, or PI):** Exempt from program requirements upon filing an annual verification confirming air-gapped operations or absence of digital systems.

Standalone Incident Reporting Framework

To guarantee real-time situational awareness during critical events, the NOPR removes cyber accident-reporting language from 52 Pa. Code §§ 57.11, 59.11, 61.11, 61.45, and 65.2 of the Commission's regulations and establishes Chapter 104 to govern cybersecurity incident reporting across jurisdictional utilities. Specifically, Chapter 104 proposes to include reportable thresholds encompassing incidents on utility networks or connected third-party systems causing service outages, compromise or loss of control of IT/OT assets, PI exfiltration, lateral network risk, or public danger. It also proposes strict reporting timelines to require verbal reporting to the Commission within 72 hours of discovery, immediate 24-hour reporting for ransomware attacks including disclosures of ransom payments and extortion mitigations, and 24-hour reporting to the PaCIC. Further, the NOPR includes a non-duplication provision to authorize utilities to submit copies of reports filed with federal agencies (such as CISA, DOE-417, the Transportation Safety Administration, or NERC) to satisfy Commission requirements, thus preventing administrative burden during an active incident.

Ratepayer Protection and Cost Allocation Principles

The Commission's fundamental role is to ensure regulated utilities are making necessary investments to provide baseline cybersecurity without over investing in their system. With the OCCO's technical support, the Commission evaluates cybersecurity expenditures under established ratemaking principles, which include baseline operational duty of care, capital investments in grid and OT resilience, and cost allocation prudency.

Routine software patch management, multi-factor authentication, identity governance, basic employee training, and baseline NIST compliance are standard costs of running a utility effectively. Ratepayers should not be subject to special surcharges, riders, or capitalized rate-base treatment for baseline operational hygiene. Instead, ratepayers should only pay for prudent cybersecurity expenses on a dollar-for-dollar normalized level where the shareholder shoulders the risk for price spikes or excess spending. Extraordinary capital additions must involve tangible, verifiable enhancements to OT and supervisory control and data acquisition systems, such as physical and logical network segmentation, automated failover architecture, hardware cryptographic modules, and zero-trust engineering.

Because cybersecurity is often a shared corporate service, the Commission reviews cost allocation methodologies to ensure security costs are allocated between regulated and non-regulated entities fairly so ratepayers only pay their portion of the costs. When utilities seek rate recovery or accounting treatment for cyber programs, the Commission exercises its statutory authority to ensure that every rate made, demanded, or received is just and reasonable. Utilities must prove that cyber investments are prudent, non-duplicative, cost-effective, and fully operational in protecting Pennsylvania assets before costs can be recovered from ratepayers. Further, under 66 Pa.C.S. §§ 504–506 and 516, the Commission examines utility plans, programs, and physical facilities during regular management audits.

Conclusion

Securing Pennsylvania's critical utility infrastructure against modern cyber threats is essential but must be accomplished without placing unreasonable financial burdens on Pennsylvania families and small businesses. The Commission's regulatory framework, supported by the OCCO's technical and ratemaking expertise, holds utilities accountable for maintaining reasonable cyber fitness while ensuring cost recovery is reserved strictly for prudent, verifiable resilience investments.

The Commission looks forward to any collaboration and further discussion with the legislature on these vital issues. Thank you for the opportunity to testify and I welcome any questions the Committee members may have.

Written Testimony of Jeremy Young

Pennsylvania House Consumer Protection, Technology & Utilities Committee

Regulators & Cybersecurity Panel

September 1, 2026

About Jeremy Young

Jeremy Young is the Chief Executive Officer and President of FRC, a Pennsylvania-headquartered technology and professional services company serving government and public-sector organizations.

Mr. Young has spent more than 25 years in the technology industry, with experience spanning cybersecurity, data, infrastructure, technology distribution, professional services, and public-sector technology.

Since becoming CEO of FRC in 2018, Mr. Young has led the company's evolution from a traditional technology reseller toward a broader mission-focused technology, cybersecurity, professional services, and solutions organization.

Mr. Young is based in Pennsylvania and has focused significant attention on expanding technology employment, cybersecurity capabilities, workforce development, and economic investment within the Commonwealth.

His perspective before the Committee is informed by FRC's work supporting public-sector organizations and by his broader experience working with cybersecurity manufacturers, technology companies, government contractors, and organizations responsible for protecting sensitive and mission-critical environments.

About FRC

FRC is a Pennsylvania-headquartered technology and professional services company that supports federal, state, local, education, and other public-sector organizations.

The company helps government customers identify, acquire, implement, integrate, and support technologies and services across areas including cybersecurity, data, artificial intelligence, infrastructure, professional services, and mission support.

FRC works across the technology ecosystem, connecting government requirements with commercial innovation while helping customers address security, modernization, compliance, operational, and mission challenges.

The company is headquartered in Erie, Pennsylvania, with operations supporting customers throughout the United States.

Introduction

Chairman Burgos, Chairman Metzger, members of the Committee, and fellow panelists:

Thank you for the opportunity to discuss cybersecurity, critical infrastructure, regulatory oversight, and the responsibility we have to protect Pennsylvania consumers and ratepayers. I would like to begin with one central recommendation:

Pennsylvania should increasingly move from measuring cybersecurity spending and compliance activity to measuring cybersecurity outcomes.

For a regulated utility, it is not enough to say:

- We purchased cybersecurity technology.
- We completed an annual assessment.
- We met a compliance requirement.
- We increased our cybersecurity budget.

The more important questions are:

- What are we protecting?
- What are our most significant risks?
- Are the controls designed to mitigate those risks actually working?
- How quickly are deficiencies being corrected?
- And are ratepayer-funded cybersecurity investments measurably reducing risk?

That is the accountability model I believe Pennsylvania should pursue.

Why Now?

- The cybersecurity threat environment is changing rapidly.
- Attackers increasingly have access to automation and artificial intelligence that can accelerate reconnaissance, phishing, vulnerability discovery, exploitation attempts, and other malicious activities.
- The defender may have thousands of employees, devices, applications, identities, suppliers, systems, and potential vulnerabilities to protect.
- An attacker only needs one successful path.
- That asymmetry makes point-in-time cybersecurity assessment increasingly inadequate.
- A security control that worked when it was audited six months ago may not be working today.
- A supplier considered secure last year may have been compromised yesterday.
- A configuration change can create a new vulnerability.
- A newly deployed application can expand the attack surface.

And the adoption of artificial intelligence can introduce entirely new categories of operational, privacy, security, and governance risk.

Cybersecurity therefore needs to become a continuous risk-management discipline rather than a periodic compliance exercise.

Pennsylvania Does Not Need to Start From Scratch

The Commonwealth does not need to invent a cybersecurity model independently. The Federal Government has spent years developing cybersecurity frameworks, programs, standards, and lessons learned that Pennsylvania can build upon.

CISA Continuous Diagnostics and Mitigation

The Cybersecurity and Infrastructure Security Agency's Continuous Diagnostics and Mitigation program helps federal agencies improve visibility into their cybersecurity posture.

The fundamental concept is straightforward:

- What is on the network?
- Who is using it?
- What is vulnerable?
- What is happening?
- Which risks matter most?
- What should be fixed first?

The program uses automated information collection, dashboards, risk scoring, and prioritized remediation to help federal agencies move beyond periodic assessments toward continuous visibility. Pennsylvania does not need to recreate the federal architecture. But the principle is highly applicable to critical infrastructure:

Risk changes continuously. Our understanding of risk should as well.

CISA Cybersecurity Performance Goals

CISA has also developed Cross-Sector Cybersecurity Performance Goals specifically for critical infrastructure. These provide a prioritized baseline of cybersecurity practices intended to reduce meaningful risk across both information technology and operational technology.

The important policy principle is prioritization.

- Not every cybersecurity control has identical value.
- Not every vulnerability creates identical risk.
- Not every organization has unlimited resources.

The goal should therefore be to identify and continuously address the cybersecurity practices that provide the greatest reduction of material risk.

NIST Cybersecurity Framework 2.0

The National Institute of Standards and Technology Cybersecurity Framework provides another strong foundation. Its six core functions are:

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

These provide a common taxonomy for managing cybersecurity risk without prescribing particular technologies or manufacturers.

NIST CSF 2.0 also places greater emphasis on governance and cybersecurity supply-chain risk.

Pennsylvania could use this framework as a common regulatory language while allowing utilities flexibility in determining how they achieve required cybersecurity outcomes.

Federal Continuous Monitoring and Risk Management

Federal cybersecurity programs also increasingly emphasize continuous monitoring. Under federal risk-management practices, cybersecurity controls are assessed, risks are documented, deficiencies are tracked, and systems are continuously monitored.

The important lesson is:

- Compliance establishes a baseline.
- Continuous monitoring helps determine whether the baseline remains effective.
- These concepts should complement one another.

Those requirements address areas including:

- Asset categorization
- Electronic and physical access
- System security management
- Vulnerability assessment
- Configuration management
- Information protection
- Incident response
- Recovery planning
- Supply-chain risk

Those standards continue to evolve as threats and technology change. This demonstrates another important principle; Cybersecurity regulation cannot remain static while the threat environment changes continuously.

Lessons From Other States

Pennsylvania can also learn from approaches already being used by other states.

New York

New York has strengthened cybersecurity requirements for major regulated utilities through requirements involving risk assessments, cybersecurity programs, access controls, authentication, intrusion detection, incident response, and recovery.

The important lesson is that utility cybersecurity is increasingly becoming part of normal regulatory oversight rather than being treated solely as an internal technology function.

Connecticut

Connecticut has developed a collaborative cybersecurity review process involving its utility regulator and major electric, natural-gas, and water utilities.

Its approach demonstrates the potential value of recurring regulatory engagement rather than relying exclusively on compliance events following incidents.

New Mexico

New Mexico has established NIST-based cybersecurity requirements for state agencies, including security assessments, compliance certification, and remediation planning.

While state agencies and regulated utilities are different environments, the underlying concept remains relevant, Establish expectations. Assess performance. Identify deficiencies. Require remediation.

NARUC and Department of Energy

The National Association of Regulatory Utility Commissioners and U.S. Department of Energy have also developed cybersecurity baselines specifically for electric distribution systems and distributed energy resources.

These provide states with an important model because they focus on cybersecurity outcomes without requiring regulators to prescribe specific technologies.

Pennsylvania should build on these existing federal and state efforts rather than create an entirely separate cybersecurity framework.

What Pennsylvania Should Consider

I recommend that Pennsylvania consider seven principles.

1. Know What We Are Protecting

Every utility should maintain an accurate and current inventory of its critical:

- Information technology assets
- Operational technology
- Applications
- Cloud services
- Data
- Identities
- Internet-facing assets
- Critical third-party systems and services

This should not simply be a spreadsheet updated annually. Critical asset inventories should be maintained at a frequency appropriate to their risk. The fundamental principle is simple; <u>you cannot effectively protect what you do not know exists.</u>

2. Continuously Monitor Critical Security Controls

An annual assessment can tell a regulator whether a control worked when it was tested. It cannot necessarily tell us whether the control is working today. Pennsylvania should increasingly expect continuous or high-frequency assurance for controls protecting the most important systems and data.

That does not mean every cybersecurity control needs to be tested every second. Monitoring frequency should be proportional to risk. Organizations should be capable of demonstrating that their most important cybersecurity controls remain operational and that failures are identified quickly.

3. Validate That Security Controls Actually Work

There is an important distinction between having a cybersecurity control and knowing that it works. Installing security technology does not prove it will stop an attacker. Having an incident-response plan does not prove an organization can execute it. Having backups does not prove they can be restored successfully. Having multifactor authentication does not necessarily mean it has been implemented everywhere it is required. Organizations should therefore periodically and safely validate whether critical cybersecurity defenses perform as intended against realistic threats. The principle is; Do not simply assume a control works. Test it.

4. Establish Risk-Based Remediation Requirements

Finding cybersecurity deficiencies is only valuable if they are corrected. Pennsylvania should consider establishing risk-based expectations for remediation. A critical vulnerability affecting an internet-facing system should not necessarily have the same remediation timeline as a low-risk vulnerability on an isolated system. The regulatory question should become:

- How serious is the risk?
- How quickly should it reasonably be corrected?
- Was it corrected?
- If not, why not?

This creates accountability without imposing arbitrary one-size-fits-all requirements.

5. Connect Cybersecurity Spending to Risk Reduction

This is particularly important for ratepayers. If a utility seeks recovery for a significant cybersecurity investment, regulators should increasingly be able to understand:

- What risk existed?
- What control addresses that risk?
- What investment was required?
- Was the control implemented?
- Was its effectiveness validated?
- What evidence demonstrates that it works?
- What residual risk remains?

That provides substantially more insight than simply reporting the amount spent on cybersecurity. Ratepayers should support reasonable investments necessary to protect critical infrastructure. In return, regulators should increasingly expect evidence that those investments are producing meaningful risk reduction.

6. Treat Third-Party and Supply-Chain Risk as Utility Risk

Modern utilities depend on an extensive ecosystem of:

- Software providers
- Cloud providers

- Telecommunications companies
- Equipment manufacturers
- Operational-technology vendors
- Managed-service providers
- Consultants
- Contractors
- Artificial intelligence providers

A utility can maintain strong internal security and still inherit significant risk through one of these relationships. Pennsylvania should increasingly expect utilities to understand:

- Which third parties can materially affect critical operations?
- What systems and information can they access?
- What cybersecurity obligations apply?
- How is compliance with those obligations evaluated?
- What happens if the supplier is compromised?

Third-party cyber risk should be treated as part of the utility's overall enterprise risk.

7. Establish AI Governance Before AI Becomes Invisible

Artificial intelligence will increasingly become embedded throughout utility operations. Potential uses include:

- Customer service
- Grid optimization
- Predictive maintenance
- Cybersecurity
- Billing
- Forecasting
- Asset management
- Field operations
- Data analytics

The question is no longer whether organizations will use AI. The questions are:

- Where is AI being used?
- What information can it access?
- What decisions does it influence?
- What external providers are involved?
- What risks does it introduce?
- Who is accountable for those risks?

Pennsylvania should encourage utilities to maintain visibility into material AI use and establish appropriate governance based on risk.

The Workforce Problem

Technology alone will not secure Pennsylvania's critical infrastructure. Cybersecurity requires people capable of:

- Managing cybersecurity programs

- Operating security technology
- Understanding operational technology
- Performing risk assessments
- Investigating incidents
- Managing third-party risk
- Governing artificial intelligence
- Interpreting compliance requirements
- Remediating vulnerabilities
- Communicating cybersecurity risk to executives and regulators

This is particularly challenging for smaller utilities, municipalities, authorities, and other critical-infrastructure organizations. Pennsylvania should therefore consider cybersecurity workforce capacity alongside cybersecurity requirements. Otherwise, well-intentioned mandates can become unfunded requirements that smaller organizations struggle to implement effectively. **Shared services, managed services, regional collaboration, workforce-development programs, public-private partnerships, apprenticeships, and continuing education should all be part of the discussion.**

Cybersecurity workforce readiness should itself be considered part of critical-infrastructure resilience.

Protecting Sensitive Cybersecurity Information

There is also an important distinction between regulatory visibility and public disclosure. Regulators need sufficient information to understand whether material cybersecurity risks are being managed. That does not mean detailed network diagrams, vulnerabilities, configurations, or other sensitive security information should become publicly available. Any Pennsylvania reporting model should carefully establish appropriate protections for sensitive cybersecurity information. The objective should be; transparency of risk and accountability without creating a roadmap for attackers.

A Pennsylvania Critical Infrastructure Cyber Assurance Model

I believe Pennsylvania could bring these principles together through a simple continuous assurance model.

- ***GOVERN***- Establish cybersecurity accountability, risk tolerance, governance, and applicable requirements.
- ***IDENTIFY***- Continuously understand critical assets, systems, identities, data, suppliers, and dependencies.
- ***PROTECT***- Implement cybersecurity controls appropriate to the risks.
- ***DETECT AND RESPOND***- Identify malicious activity quickly and maintain the ability to contain and respond to incidents.
- ***VALIDATE***- Test whether critical cybersecurity defenses actually perform as intended.
- ***ASSURE***- Collect evidence demonstrating that critical controls remain operational.
- ***REMEDIATE***- Correct significant deficiencies within defined, risk-based timelines.
- ***TRAIN***- Continuously develop the workforce responsible for cybersecurity and resilience.
- ***REPORT***- Provide regulators with standardized information regarding material risks, control effectiveness, remediation, investment, and residual risk while protecting sensitive technical information.

A Pennsylvania Pilot

I would encourage Pennsylvania to consider piloting this model before imposing broad new requirements. The Commonwealth could work with a small number of willing regulated utilities or critical-infrastructure organizations and identify perhaps 10 to 20 high-priority cybersecurity outcomes.

Those outcomes could be drawn from existing sources such as:

- NIST Cybersecurity Framework 2.0
- CISA Cybersecurity Performance Goals
- Applicable Critical Infrastructure Protection requirements
- NARUC and Department of Energy cybersecurity baselines

The pilot could then:

- Identify critical assets and systems.
- Establish baseline cyber risk.
- Identify the controls protecting those assets.
- Determine which controls warrant continuous or high-frequency monitoring.
- Validate selected defenses against realistic threats.
- Establish risk-based remediation timelines.
- Measure remediation performance.
- Track cybersecurity investment.
- Measure changes in residual risk.
- Develop a standardized regulatory reporting model.

This would allow Pennsylvania to learn before it mandates. It would also provide policymakers with real data regarding cost, effectiveness, implementation challenges, workforce requirements, and actual risk reduction.

Protecting Ratepayers

Ultimately, cybersecurity regulation should balance two responsibilities.

- Pennsylvania cannot underinvest in cybersecurity and expose consumers and critical infrastructure to unacceptable risk.
- Cybersecurity also should not become an unlimited category of spending in which every expenditure is assumed to produce an equivalent public benefit.

The better approach is:

Give utilities flexibility in how they achieve cybersecurity outcomes while requiring evidence that those outcomes are being achieved. That creates technology neutrality. It encourages innovation. It gives utilities operational flexibility. It provides regulators with greater accountability. And it gives ratepayers greater confidence that cybersecurity expenditures are producing meaningful benefits.

Conclusion

Pennsylvania does not need to invent this approach from scratch. The Federal Government has moved toward continuous cybersecurity visibility and risk management. CISA has established prioritized cybersecurity performance goals for critical infrastructure. NIST provides a common framework for cybersecurity risk. The electric sector already operates under mandatory cybersecurity requirements. The Department of Energy and NARUC have developed cybersecurity baselines for electric distribution. And other states are expanding regulatory oversight of utility cybersecurity.

Pennsylvania has an opportunity to bring the best elements of those approaches together. The model can be simple:

- Know what we have.
- Know what matters.
- Protect it.
- Monitor it.
- Test it.
- Prove it.
- Fix what fails.
- Train the people responsible for it.
- Measure whether the investment actually reduced risk.

Because ultimately the question for this Committee and Pennsylvania ratepayers should not simply be:

How much did we spend on cybersecurity?

It should be:

Are Pennsylvanians safer because of it?

Thank you for the opportunity to testify.

The Authorities
PENNSYLVANIA MUNICIPAL AUTHORITIES ASSOCIATION

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

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 authorites 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.

Cybersecurity Testimony

Sumit Nair
Chief Information Officer, Essential Utilities, Inc.
Aqua Pennsylvania / Peoples Natural Gas

Pennsylvania House Consumer Protection, Technology & Utilities Committee

Hearing on Cybersecurity in Utility Infrastructure — September 1, 2026

Chairman Burgos, Chairman Metzgar, and Members of the Committee:

Thank you for the opportunity to appear today, and for the Committee's continued attention to the security of Pennsylvania's critical infrastructure. I serve as Chief Information Officer for Essential Utilities, Inc., the parent company of Aqua Pennsylvania and Peoples Natural Gas. I am pleased to appear alongside representatives from the water, gas, and electric sectors, as well as the Public Utility Commission, to discuss how our company approaches cybersecurity risk.

I. No Material Cybersecurity Exposure to Date

To date, Aqua Pennsylvania and Peoples Natural Gas have not experienced a cybersecurity incident that disrupted utility operations, interrupted water or gas service to customers, or resulted in a material financial impact to the company. This reflects our experience to date. It does not diminish how seriously we treat the threat - the cyber landscape facing utilities is real, active, and continuously evolving, and it requires continued vigilance and investment.

II. Cybersecurity Program and Posture

Cybersecurity governance is embedded throughout our organization, from front-line operations to the Board of Directors. Our program is aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework and reflects recognized industry practice across both our information technology and operational technology environments.

At a programmatic level, our approach includes continuous threat monitoring, layered identity and access controls, protections for the operational technology systems that run our water and gas infrastructure, regular independent testing and assessment, workforce awareness training, and tested incident response and business continuity capabilities.

Cybersecurity risk and program progress are reviewed regularly by executive leadership and reported to our Board of Directors. We treat cybersecurity as an enterprise risk that touches operations, finance, legal, and customer service - not solely a technology issue.

III. Financial Considerations

We treat cybersecurity investment as a normal and prudent component of ongoing operating and capital spending required to run safe, reliable utility systems, rather than as an extraordinary or incident-driven cost. To date, we have not recognized any material financial loss, write-off, or extraordinary charge related to a cybersecurity event, and no cybersecurity event has required customer rates to be increased or otherwise adjusted.

.

IV. Public and Customer Impact

Aqua Pennsylvania and Peoples Natural Gas have not experienced a cybersecurity incident resulting in a significant interruption of customer service or a material impact on public health and safety. Maintaining the availability and reliability of water and natural gas services is the central objective of our cybersecurity program, and our strategy is built around operational resilience: the ability to keep delivering safe, reliable service even while confronting an evolving threat environment.

Closing

Cybersecurity is not a destination but an ongoing discipline of assessment, investment, and adaptation. Essential Utilities remain committed to maintaining a strong cybersecurity posture, working with this Committee, the Public Utility Commission, and our industry and government partners, and ensuring the continued safe and reliable delivery of water and natural gas services to communities across Pennsylvania.

Thank you for the opportunity to testify.

FirstEnergy Pennsylvania

Brian Harrell, Chief Security Officer, FirstEnergy Pennsylvania Electric Company

Testimony before the House Consumer Affairs Committee

September 1, 2026

Introduction

FirstEnergy Corp.'s ("FirstEnergy" or the "Company") regulated distribution and transmission operating companies serve 6 million customers across the Midwest and Mid-Atlantic regions, with a combined system spanning more than 269,900 miles of distribution lines, 24,000 miles of transmission lines, two regional transmission operation centers, and 3,599 megawatts of generation.

In Pennsylvania specifically, FirstEnergy Pennsylvania (FE PA), which is comprised of the rate districts for Metropolitan Edison, Pennsylvania Electric, Pennsylvania Power, and West Penn Power, serves approximately 2.1 million customers in 56 of the 67 counties throughout the Commonwealth of Pennsylvania.

FirstEnergy is dedicated to providing customers with safe, reliable, and responsive service. Cybersecurity is a critical component of that.

Cybersecurity is not simply a technology issue for electric utilities. It is a consumer protection imperative. Our customers depend on safe, reliable, and affordable electricity for nearly every aspect of daily life, from heating and cooling homes to powering medical devices, communications networks, businesses, schools, and other critical public services. As the electric grid becomes more interconnected and digitally enabled, cyber threats have the potential to impact the reliability and resilience of the electric service consumers depend on.

Threats to the Electric Grid

Today's electric grid is more digitally managed than at any point in its history. That connectivity allows utilities to move power more efficiently, respond more quickly to outages, and coordinate across service territories and regions. However, it also means cyber risks are no longer isolated to a single company or geographic area. With an interconnected grid, the effects of a cyber incident can extend well beyond its point of

origin while having cascading impacts, reinforcing the need for strong cyber security practices and close industry coordination.

U.S. electric companies face the threat of sophisticated cyber-attacks from the governments and militaries of foreign adversaries, as well as a barrage of attacks from less-sophisticated actors—who are increasingly enhancing their capabilities with the use of new and emerging technology to enable attacks, including artificial intelligence ("AI").

Criminal groups may use ransomware and extortion to disrupt operations or steal sensitive information for profit, while government-backed groups or individuals may seek intelligence, long-term access, or the ability to cause disruption during a future conflict. Attackers increasingly exploit stolen passwords, internet-connected equipment, and weaknesses in third-party products, so their activity resembles normal computer use and is harder to detect. The growing use of cloud services, remote access, automated controls, and consumer-connected devices delivers significant operational and customer benefits. At the same time, it expands the threat landscape and increases the number of potential pathways that utilities must continuously monitor and secure to protect critical infrastructure.

Utilities cannot wait for a crisis to begin. They must continuously identify and eliminate hidden vulnerabilities, strengthen their ability to recover from disruption, share threat intelligence, and ensure they can maintain critical operations through a sustained cyber-attack.

How FirstEnergy Protects the Grid

FirstEnergy safeguards the electric grid through a mature risk-based cybersecurity program built around six core functions: governing risk, identifying critical systems, protecting those systems, detecting suspicious activity, responding to incidents, and recovering operations. The program is aligned with the National Institute of Standards and Technology Cybersecurity ("NIST") framework and is continually enhanced through independent assessments, rigorous testing, industry benchmarking, regulatory requirements, and ongoing analysis of the evolving threat landscape. FirstEnergy does not treat cybersecurity as a separate function. It is an integrated part of the Company's broader efforts to ensure the resilience, reliability, and security of the critical infrastructure our customers depend on every day.

A foundational principle of FirstEnergy's cyber security program is defense in depth. Rather than relying on any single security measure, the Company employs multiple layers of administrative, technical, and physical safeguards to prevent, detect, and mitigate threats.

This layered approach helps ensure that the failure of one control does not automatically expose a critical system. Corporate information technology and operational technology, the specialized systems used to monitor and control the grid, are managed separately according to their different functions and risks, with network separation, controlled access, secure configurations, system monitoring, and protections tailored to the criticality of the equipment involved. Cybersecurity personnel also take part in the design and review of new systems and grid-modernization initiatives, so that security is built in from the start rather than added after deployment.

Protection also requires continuous visibility. FirstEnergy maintains security monitoring capabilities for both its business and operational environments, supported by specialized personnel who review alerts, investigate unusual behavior, incorporate threat intelligence, and look proactively for signs that an attacker may be present. Separate monitoring approaches are used where appropriate for information technology and real-time operational systems, recognizing that the technologies, operating requirements, and potential consequences are different. The Company continues to observe a sustained increase in malicious cyber activity originating from foreign threat actors targeting critical infrastructure and customer-facing services. Over the past year, tracked threat actor activity increased 12% and monitored malware families increased 8%, while defensive measures blocked an average of 41,000 automated malicious connection attempts per month against our public-facing website. To address this evolving threat landscape, new detection and prevention rules are continuously developed while FirstEnergy conducts proactive threat hunting activities every day to identify and disrupt potential threats before they impact operations. The Company continues to improve these capabilities through detection engineering, automation, network visibility, threat hunting, and testing intended to identify weaknesses before an adversary can exploit them.

FirstEnergy also works to reduce the opportunities available to an attacker. The Company maintains processes for identifying vulnerabilities, evaluating their potential effect in the context of the affected system, prioritizing remediation, managing security patches, controlling user access, and reviewing changes to important systems. Because utilities depend on a broad network of equipment manufacturers, software providers, service companies, and contractors, the cybersecurity program also evaluates third-party and supply chain risks throughout the lifecycle of those relationships. FirstEnergy has experienced a 27.5% year-over-year increase from 2025 to 2026 in the number of security-related software vulnerabilities that were addressed and remediated in our environment. A key driver is AI, which is accelerating the discovery of exploitable software defects while also shortening the between discovery and attack. The Company is employing AI measures as well as other processes to keep pace with the tempo of these vulnerabilities. These

measures are intended to address not only weaknesses within FirstEnergy's direct control, but also risks that may enter through trusted products, services, or business partners.

No responsible organization can guarantee that every cyberattack will be prevented. For that reason, preparedness, response, and resilience are as important as prevention. FirstEnergy maintains a comprehensive cybersecurity incident response plan for identifying, classifying, containing, investigating, reporting, and recovering from significant events, including incidents affecting critical grid systems, third-party compromises, and supply-chain events. Cybersecurity Incident Response is a cross-functional effort that brings together experts from across FirstEnergy's cybersecurity, operations, legal, compliance, communications, and other business units as the circumstances require. FirstEnergy regularly conducts exercises to strengthen coordination and decision-making before an actual crisis occurs. Robust recovery capabilities, including tested backup and restoration processes, are designed to support the continuity of critical operations and the safe timely restoration of services following a disruptive event.

In order to ensure that people remain an essential part of this defense, FirstEnergy provides recurring cybersecurity awareness and role-based training, conducts phishing simulations and exercises, and reinforces that protecting the grid is a shared responsibility among employees and contractors who have access to Company systems. At the same time, FirstEnergy's dedicated cybersecurity professionals provide specialized expertise in incident response, threat intelligence, vulnerability management, secure architecture, operational technology, compliance, and security engineering. This combination of a well-informed workforce and specialized defenders strengthens the Company's ability to be proactive and identify threats earlier, reduce risk, and respond more effectively to emerging incidents.

Finally, FirstEnergy's cybersecurity program operates within a substantial framework of mandatory reliability and security obligations. The Company implements applicable North American Electric Reliability Corporation Critical Infrastructure Protection requirements governing electronic access, system security, incident response, configuration management, protection of sensitive grid information, supply-chain risk, and network monitoring. Compliance is supported by documented controls, internal assessments, vulnerability testing, audits, and a commitment to continuous improvement. Yet, compliance represents only a baseline level of assurance. FirstEnergy's goal is to build upon that foundation through risk-informed practices that continuously adapt to evolving technologies, emerging threats, and operational realities.

Additionally, FirstEnergy participates in several industry and public-private partnerships to share information and best practices. Engagement with the Electricity Information Sharing

and Analysis Center, the Edison Electric Institute, the North American Transmission Forum, and many others to increase both the Company's reliability and security posture. The Company's approach helps strengthen the security, reliability, and resilience of the electric system on which Pennsylvania homes, businesses, and critical services depend.

Future Concerns

Energy security will increasingly depend on decisions made at the intersection of technology, electricity, and cybersecurity.

Utilities, and all companies and organizations, must approach AI not only as an opportunity, but also as a source of operational, cybersecurity, privacy, and governance risk. To realize AI's benefits while protecting critical infrastructure and public interest, organizations should maintain meaningful human oversight and incorporate security, privacy, and resilience into each use from the outset. AI offers significant benefits for cybersecurity and utility operations by helping utilities analyze large amounts of information, identify unusual activity more quickly, automate routine tasks, and help skilled professionals respond to threats with greater speed and precision. At the same time, AI can be leveraged by malicious actors to create more convincing fraud, automate attacks, discover vulnerabilities, target employees, customers, and critical systems at greater scale. The rapid deployment of AI technologies also presents governance and compliance challenges, such as protecting sensitive data, reliance on third-party vendors and cloud services, supply-chain dependencies, accountability, and the need to verify that automated decisions are accurate and appropriate.

Accordingly, realizing AI's promise will require a risk-based governance framework that promotes innovation while maintaining robust cybersecurity safeguards, protecting privacy, strengthening resilience, and ensuring public trust keeps pace with technological advancements. As AI evolves, so too must all these considerations.

Cybersecurity must be recognized as a core investment in reliability and resilience, not as a discretionary cost. Building and maintaining secure systems require sustained investment in technology, skilled personnel, monitoring, preparedness, and infrastructure modernization. These investments help reduce the risk of cyber incidents whose impacts can be far more costly, particularly when they disrupt electric service, threaten public safety, impede economic activity, and compromise sensitive information. Legal, policy, and regulatory frameworks should therefore support prudent and adaptable risk-based cybersecurity investments, encourage cooperation and information sharing, and evaluate affordability over the full life of the systems on which reliable electric service depends.

Testimony from PJM Interconnection, L.L.C.

Testimony of Steven McElwee, Vice President & Chief Security Officer, PJM Interconnection, L.L.C., Before the Pennsylvania House Consumer Protection, Technology & Utilities Committee Informational Hearing: "Utility Cybersecurity, Consumer Protection and Cost Recovery"

Sept. 1, 2026

For Public Use

Contents

Executive Summary

PJM appreciates the opportunity to share perspectives on how to ensure Pennsylvania ratepayers receive secure, reliable utility services without bearing unreasonable financial burdens. The Committee's focus on utility cybersecurity mandates is timely and critical at a time when technological advances have changed the threat landscape.

Since 1927, PJM Interconnection has provided power reliably and cost-effectively by sharing electricity across state lines. Working with local utilities, PJM operates the grid across 13 states and the District of Columbia, from New Jersey to North Carolina and west to Illinois, helping ensure reliable electric service 24/7. PJM's regional planning process assesses the need for transmission upgrades to ensure reliability, increase efficiency and advance public policy goals. PJM's large geographic footprint allows it to pool resources across its region to serve customers each day. This approach mitigates generator outage risk, enhances reliability and reduces transmission and operating reserves needed during emergencies and other operational challenges.

Cybersecurity is a reliability issue. Cyber incidents can disrupt utility operations, reduce situational awareness and damage critical equipment, quickly becoming reliability events. Cybersecurity investments help identify and address vulnerabilities before they can be exploited, directly benefiting ratepayers by supporting the safe, reliable operation of substations and transmission lines.

The threat landscape has changed. Recent international conflict has demonstrated that critical infrastructure is a prime target of nation-state threat actors. At the same time, rapid advances in artificial intelligence (AI) have increased the automation of cyberattacks, enabling nation-states and criminal actors to develop exploits, infiltrate organizations and disrupt operations in minutes. As a result, utilities must continually adapt and advance cybersecurity capabilities to address evolving threats.

Current grid conditions increase the importance of cyber resilience. As electricity demand grows and generation resources become scarcer, the power grid has less flexibility to absorb the impacts of disruptive events. In addition, the growth of large computational loads has changed grid operating conditions, creating challenges, including over-voltage, over-frequency and oscillating conditions.

Consumer protection and cybersecurity are not competing goals. Ratepayers benefit from proactive measures to prevent, detect, respond to and recover from cyberattacks. These actions include routine cyber-hygiene activities that keep adversaries from exploiting systems as well as larger initiatives to strengthen organizations' abilities to address threats and vulnerabilities.

Cybersecurity for utilities has evolved into a set of practices and frameworks that establish a standard of due care. Frameworks such as the NIST Cybersecurity Framework (CSF) provide a foundation for organizations to implement security controls and establish target maturity levels. In addition to the NIST CSF, many electric utilities comply with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, which establish cybersecurity requirements for systems critical to grid operations. NERC CIP standards apply to entities that perform essential reliability functions on the bulk electric system. Together, these frameworks and standards help reduce cybersecurity risk, support reliable grid operations and protect consumers against service disruptions.

In addition to frameworks and standards, organizations must make strategic investments in emerging cybersecurity technologies to adapt to a rapidly changing, AI-enabled threat landscape. These investments in cybersecurity are guided by risk assessments and are unique to each utility's technology environment, business model and threat profile. These risk assessments continue to show that critical grid infrastructure is a target for various threats across

the spectrum. By reducing cybersecurity risk, these investments help protect consumers from service disruptions by preventing future adverse impacts of cyberattacks.

Cybersecurity investments are analogous to utility vegetation management programs. Routine vegetation management prevents power outages by trimming trees that could interfere with transmission lines. These activities support reliable electric service much as patch management, user access management, routine security management and compliance activities support grid operations. Unlike many physical threats, cyber threats often develop over time. Threat actors may gain access to systems and remain undetected before disrupting operations. Routine cybersecurity activities help identify and close these pathways before they can be exploited, much as vegetation management removes conditions that could lead to future outages. Like vegetation management, these cyber hygiene activities are ongoing operational functions that should be treated as routine operating expenses.

Larger vegetation management initiatives include activities such as expanding rights-of-way, storm hardening and wildfire prevention. These larger-scale activities are analogous to strategic cybersecurity investments, including advanced security architectures, threat-hunting programs, security operations centers, AI-enabled detection systems and recovery capabilities. Like enhanced vegetation management, these investments also directly support electric service and position utilities' ability to defend against the rapidly evolving threat landscape.

Ineffective vegetation management can result in customer outages, safety risks and equipment damage. When those outcomes stem from ineffective programs, ratepayers should not bear the resulting recovery costs. Similarly, ratepayers should not be asked to finance poor cybersecurity management or deferred compliance activities.

Pennsylvania consumers depend on a reliable bulk electric system, and prudent, risk-based cybersecurity investments are now as essential to reliability as substations, transmission lines and control rooms.

As the Committee considers policies that hold utilities accountable while protecting consumer interests, several principles warrant consideration:

- Operational and strategic cybersecurity investment helps prevent disruptions and reduce the impacts of cyberattacks, directly benefiting consumers.
- A disruptive cyberattack can impose greater costs on utilities and consumers than preventative measures by utilities that reduce cybersecurity risk.
- AI is changing the risk equation by simplifying sophisticated exploits at a time when the grid is operating on thin reserve margins.
- Policymakers should evaluate cybersecurity through a risk-management lens and recognize that adversaries will look for the weakest link across critical infrastructure sectors.
- A prudent policy framework should drive accountability for cybersecurity investment and risk management before an incident occurs.
- Consistent standards and principles will be more cost-effective than a disparate set of requirements.
- Policymakers should consider how to shield consumers from the costs of responding to events resulting from ineffective cybersecurity programs, noncompliance or negligence.

In today's threat environment, cybersecurity is a reliability investment. Can Pennsylvania consumers afford the consequences of underinvestment in the cybersecurity systems that support reliable electric service?

I. Cybersecurity Is a Reliability Issue

Electric utilities rely on technology and digitalization to optimize their services and operate efficiently. This reliance on technology, while beneficial, also increases the likelihood and consequences of cyberattacks. Both operational technology (OT) systems and back-office systems are at risk, since they affect how utilities deliver services to their customers. Back-office systems are often an adversary's initial target since they are more accessible and can be the steppingstone to gain access to the OT systems. As a result, cybersecurity practices that address both OT and back-office systems are essential to prevent disruptions that may affect consumers and may lead to power outages.

A cyber compromise that is not sufficiently contained in time may result in damage to transmission lines and substations. This outcome may occur if an adversary can force the operation of equipment beyond its voltage and thermal limits. It may also result in oscillations on the power grid, which creates the potential to cascade to other equipment and result in widespread outages.

In addition, a cyber compromise may render systems untrustworthy and may impair situational awareness. This awareness is vital when operating the electric grid, since power is generated and consumed in real time. Situational awareness enables generation and transmission dispatchers to make decisions that both enable the reliable operation of the grid and enable them to make the most cost-effective energy dispatch decisions.

In the Northeast Blackout of 2003, a combination of gaps in situational awareness and trees intersecting with power lines resulted in the most severe cascading outage in United States history. While the nexus of this event was not a malicious actor, the consequences of the gaps in situational awareness are evident in the impact to consumers in the Northeast (Final Report on the August 14, 2003, Blackout in the United States and Canada [PDF]). A capable cyber adversary can cause utilities to lose visibility to the information they need to operate the grid reliably and cost-effectively.

The reality of this risk is clear in the 2015 and 2016 Russian cyberattacks against Ukrainian electricity utilities. The Russian adversaries were able to remotely operate breakers, erase data from OT systems, disrupt power to customers and require the utilities to manually close breakers at substations (Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience [PDF]).

II. The Threat Landscape Has Changed

Recent international conflicts have demonstrated that nation-states will target critical infrastructure that civilians depend upon. Russia's war against Ukraine set a precedent for nation-states, and as a result, U.S. critical infrastructure must be considered a prime target for exploitation by capable nation-state actors, like Russia, China and Iran. Against this backdrop, cybersecurity for electric utilities is essential to protect the nation, our states and our consumers from disruptions.

While these nation-states have demonstrated both their intent and capability to conduct cyber operations against critical infrastructure, advances in AI have made these capabilities more accessible and effective for threat actors previously considered less sophisticated. In July 2026, AI-enabled cyberattacks were conducted by China against Taiwan government agencies and at least seven energy companies (Taiwan Says It Was Hit by "Abnormal" AI-Assisted Cyber-Attack). AI-enabled attacks can be more potent than human-generated attacks, in that the AI agents can discover vulnerabilities humans cannot find, develop exploits in minutes and chain together lower severity vulnerabilities to successfully compromise organizations.

As a result, electric utilities need to adopt newer approaches to discover and prioritize vulnerabilities. Cyber threats do not always occur in real time. Threat actors often gain access to systems, establish persistence and remain undetected while identifying opportunities to disrupt operations. Traditional patch cycles are insufficient to address vulnerabilities, since adversaries can develop exploits and compromise organizations in minutes. Utilities therefore must invest in cybersecurity operations and maintenance, including patch management, access management and continuous monitoring, and strategic investment in technologies that can help defend against AI-enabled threats.

III. Grid Conditions Increase the Importance of Cyber Resilience

The power grid in the PJM footprint has seen a sharp rise in demand, largely because of large computational loads. At the same time, generation resources have been retiring, and new generation has not been built to keep up with the rising demand. On most days of the year, there is sufficient electricity for all customers, but on extremely hot and cold days, scarcity of generation results in razor thin margins and often requires PJM to call upon Demand Response (DR) resources to curtail their electricity use to ensure that consumers are not impacted. These extreme temperature days occur regularly and put strain on the operation of the grid.

With less margin on the system, a cyberattack when all resources are needed may result in catastrophic impacts. A cyberattack against any utility in Pennsylvania on a day when grid conditions are pushed to their extreme may cause generation units, transmission lines or transmission substations to trip offline. This may result in controlled load shed, or even worse, cascading outages.

In addition to scarcity conditions, operating the power grid with large computational loads has introduced new challenges. For example, on July 22, 2026, a transmission line trip resulted in one data center to transfer to backup generation. This sudden loss of load on the grid caused unstable grid conditions that caused other data centers to transfer to backup generation. In total, PJM saw 3,800 MW of load rapidly drop from the grid, resulting in over-voltage and over-frequency conditions (Dominion Load Transfer Event [PDF]). As NERC and utilities deal with how to safely operate the grid with large computational load, this volatility puts more strain on the reliable operation of the grid. While the initial view of the cause of this event was automatic relay protection, this same vulnerability, maliciously triggered, is also a new risk for utilities. Under these conditions, a simultaneous cyber compromise may result in widespread outages and equipment damage.

IV. Consumer Protection and Cybersecurity Are Not Competing Goals

Cybersecurity benefits ratepayers by helping to prevent outages, preventing damage to equipment and ensuring utilities can operate with the information needed to provide electricity cost-effectively.

To compare cybersecurity to other utility practices, utilities have historically invested in vegetation management because regulators, utilities and consumers share a common understanding that preventing outages is less costly than responding to them. Although vegetation management activities often occur out of public view, they are widely recognized as essential to maintaining safe and reliable electric service. The benefits are frequently measured not by visible outcomes, but by disruptions that never occur.

Cybersecurity increasingly occupies a similar role in utility operations. As electric systems become more interconnected and digitally enabled, cybersecurity is essential to maintain reliable service. Activities such as patch management, identity and access management, system monitoring, employee training and regulatory compliance reduce the likelihood that malicious actors can disrupt utility operations. Like routine vegetation management, these activities represent ongoing operational responsibilities that help utilities maintain the reliability customers expect.

While routine vegetation management provides an important analogy for foundational cybersecurity activities, the current threat environment increasingly requires investments that resemble broader resiliency and infrastructure-hardening initiatives. Utilities have long pursued strategic investments, such as expanded rights-of-way, storm hardening programs, flood protection measures and wildfire mitigation efforts, when conditions indicate that historical operating practices are no longer sufficient. These investments are undertaken because the nature of the threat has changed. In those circumstances, utilities are expected to prepare for emerging risks rather than rely exclusively on traditional maintenance activities.

The cybersecurity environment is undergoing a similar transformation. Nation-state actors target critical infrastructure. Criminal ransomware organizations have become sophisticated. AI is making it possible for malicious actors to automate reconnaissance, generate convincing phishing campaigns, accelerate vulnerability discovery and increase the speed and scale of attacks. As a result, many of the cybersecurity capabilities needed to protect modern utility operations extend beyond routine security maintenance. Investments in security operations centers, advanced monitoring and analytics, threat hunting programs, OT security architecture, incident response capabilities and cyber recovery systems are designed to improve the resilience of critical infrastructure in the same way that physical hardening projects improve resilience against severe weather and other physical threats. These investments should be viewed as reliability investments rather than discretionary technology expenditures.

The cost of prudent cybersecurity investment must be considered alongside the potential economic costs associated with service interruptions, restoration activities, emergency response and broader impacts to customers and communities. Utilities should have a reasonable opportunity to recover costs associated with prudent cybersecurity investments that materially improve reliability and resilience. Such investments should be subject to appropriate regulatory oversight, supported by clear business justification and aligned with the risks facing the utility and the electric system.

Customers are less willing to bear costs resulting from negligence, deferred maintenance or poor operational decisions. The same distinction should guide cybersecurity policy. Utilities should maintain strong cybersecurity programs as part of their responsibility to operate critical infrastructure. They should be held accountable for compliance failures, unreasonable delays in addressing known vulnerabilities or deficiencies resulting from poor management practices.

A balanced approach advances both cybersecurity and consumer protection objectives simultaneously. It ensures that ratepayers are not asked to subsidize poor performance while also recognizing that protecting the electric grid against evolving threats requires continued investment.

V. PJM's Role in Cyber Investment

PJM's role in cybersecurity investment outside of PJM is limited. PJM does not make or direct cybersecurity investment decisions on the distribution system; those decisions appropriately reside with individual electric utilities and their state utility regulator, i.e., the Pennsylvania PUC. PJM likewise does not mandate cybersecurity investments on the bulk electric system. Rather, cybersecurity requirements for the bulk electric system are established through mandatory Critical Infrastructure Protection (CIP) standards approved by the Federal Energy Regulatory Commission (FERC) and developed and enforced by NERC, supplemented by applicable NIST standards and practices.

PJM is itself subject to these requirements and maintains cybersecurity measures as part of its overall operating budget. With respect to recovery of cybersecurity-related costs on the bulk system, the applicable regulatory

framework is established by FERC, with cost recovery reflected through the rates and market revenues applicable to regulated entities, including competitive generators where appropriate. Thus, while PJM has an important responsibility to maintain the cybersecurity of its own operations and systems, it does not determine or direct the broader cybersecurity investment decisions of utilities or other market participants.

PJM uses the NIST CSF to define a foundation of security practices. CSF includes 106 specific actionable technical and management outcomes that ensure we address foundational cybersecurity activities. These outcomes fall into high-level categories of Govern, Identify, Protect, Detect, Respond and Recover. PJM annually assesses areas of improvement needed to advance our maturity in these outcomes and executes action plans to close gaps and further enhance our security posture. These practices work together to secure the systems and data we need to operate the grid.

In addition, PJM adheres to NERC CIP standards. These standards define specific requirements for utilities with a goal of the safe and reliable operation of the bulk electric system. Not all systems are in scope of NERC CIP, but only those systems that, if compromised or rendered inoperable, could affect the power grid.

In addition to standards and frameworks for cybersecurity, PJM conducts an annual cyber risk assessment and aligns it with enterprise risk. The result of the risk assessment helps identify the highest priority security investments that may not be covered by our adherence to existing frameworks. This is especially important considering the rapidly changing technology and threat landscape. PJM directs investment into tools and technologies that are necessary to reduce the time needed to detect and respond to threats and vulnerabilities. While these investments are often longer-term and strategic, they help protect the systems needed to operate the grid reliably.

Over many years, the cycle of evaluating adherence to standards and frameworks and investing in technologies that address cyber risk has resulted in a portfolio of cybersecurity tools and technologies that help to protect PJM against cyber threats. But past investment is not sufficient to address the escalation of threats as adversaries develop new methods to attack at machine speed. Ongoing investment in cybersecurity, using risk-informed prioritization, is essential.

Separating cybersecurity practices that do not benefit ratepayers is difficult because cybersecurity has become an integrated collection of practices that work together to manage risks to the bulk electric system and the systems that support reliable grid operations.

A more effective policy approach may be to protect ratepayers from the costs associated with underinvestment in cybersecurity that leads to cyber incidents and noncompliance. Holding utilities accountable for negligence and ineffective cybersecurity management can help ensure that cybersecurity investments are prudent, risk-based and focused on reducing threats to reliable electric service while protecting consumer interests.

VI. Principles for Policymakers

As the Committee considers policies that hold utilities accountable while protecting consumer interests, several principles warrant consideration:

- Operational and strategic cybersecurity investment helps prevent disruptions and reduce the impacts of cyberattacks, directly benefiting consumers.
- A disruptive cyberattack can impose greater costs on utilities and consumers than preventative measures by utilities that reduce cybersecurity risk.

- AI is changing the risk equation by simplifying sophisticated exploits at a time when the grid is operating on thin reserve margins.
- Policymakers should evaluate cybersecurity through a risk-management lens and recognize that adversaries will look for the weakest link across critical infrastructure sectors.
- A prudent policy framework should drive accountability for cybersecurity investment and risk management before an incident occurs.
- Consistent standards and principles will be more cost-effective than a disparate set of requirements.
- Policymakers should consider how to shield consumers from the costs of responding to events resulting from ineffective cybersecurity programs, noncompliance or negligence.

TESTIMONY OF QIAN (JACKIE) ZHOU

DIRECTOR, CYBER SECURITY – PHILADELPHIA GAS WORKS (PGW)

BEFORE THE HOUSE COMMITTEE ON CONSUMER PROTECTION, TECHNOLOGY, AND UTILITIES

ON

TUESDAY, SEPTEMBER 1, 2026

Good morning, Chairman Burgos, Chairman Metzgar, and members of the Committee, my name is Jackie Zhou, and I am the Director of Cyber Security for the Philadelphia Gas Works (PGW) in Philadelphia, Pennsylvania. PGW is the nation's largest municipally owned natural gas utility in the country serving 500,000 ratepayers. For the last 190 years, PGW has innovated to ensure safe, reliable, and affordable service. PGW does not make a profit, we have no shareholders and do not pay a dividend or a rate of return. Thank you for the opportunity to speak with you today about how PGW protects the natural gas systems our customers depend on every day.

Since 2021, PGW's cybersecurity program has been subject to federal oversight, and each year we have met 100 percent of the requirements evaluated during the inspection. We stay informed about evolving threats through coordination with government and industry partners such as the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI) and the American Gas Association (AGA). The utility industry has seen a growing trend of cyberattacks shifting from traditional Information Technology (IT) environments to Operational Technology (OT) Systems. To counter this threat, PGW's OT Systems remain off Internet. Gas operators must work onsite, and no vendor has remote access to our systems. This year we have

upgraded our systems. Not only were both hardware and software updated, but we also took the opportunity to improve network security and upgrade security solutions.

Because our systems help deliver an essential service, we understand that a cyberattack on a company like ours isn't just an IT problem — it's a public safety issue. That's why we've made significant investments not only in technology, but in the people who operate and defend those systems on a daily basis. One example: several years ago, we built a training program to help employees recognize and avoid phishing attempts, which remains one of the most common ways attackers try to gain access to a company's systems. Employees who need extra help receive hands-on coaching from our security team. Since we started this program, the number of employees needing that additional coaching has dropped by more than 90 percent, and our overall vulnerability to these attempts has been cut in half.

We also don't wait for a real emergency to test our readiness. Every year, our team including our senior leadership, runs through realistic exercises simulating a cyberattack, so that if something ever happens, our response is practiced, not improvised, and we can continue serving our customers safely and reliably. Every year we stress test both cyber and physical security of our critical infrastructure facilities. We engage external experts to execute simulated breaches of our cyber and physical defenses.

PGW doesn't view cybersecurity as a box to check once a year; we view it as a standing obligation to the communities we serve. PGW is committed to staying ahead of this threat, and we welcome this committee's continued attention to this issue.

This concludes my testimony and I welcome your questions at this time. Thank you.