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.