

House Consumer Protection, Technology & Utilities Committee

09/01/2026, 9:30 a.m., Room 515, Irvis Office Building

Pennsylvania Legislative Services

The committee held an informational hearing on utility cybersecurity.

[Rep. Pat Gallagher](#) (D-Philadelphia) opened by framing cybersecurity of critical utility infrastructure as an urgent, day-to-day reality. He noted that public utilities rely on highly interconnected digital networks and operational technology that undergird electricity, gas and water services, creating vulnerabilities. He said ransomware groups, criminal syndicates and state-sponsored actors are probing systems not merely to steal customer data but to manipulate, disrupt or disable control systems that provide critical utilities.

[Rep. Craig Williams](#) (R-Delaware) marveled at the contrast in power between computers during his time stationed at the Pentagon and today. He said failures in incidents often involved people and security equipment rather than computers alone. He stressed supply-chain risks and human vulnerabilities such as phishing as primary enablers of intrusions into utility systems. He framed the issue as regulatory and statutory.

Stephen DeFrank, chairman, Public Utility Commission (PUC), described the interconnected nature of critical infrastructure systems in the modern era. “Safeguarding these assets against sophisticated cyber threats becomes fundamental to both utility reliability and public safety,” he said. He spoke about the Office of Cybersecurity Compliance and Oversight (OCCO) and its role in providing technical advisory and incident response. He said PUC approved a comprehensive notice of proposed rulemaking (NOPR) on June 18, 2026, that transitions from self-certification to an objective, verifiable framework grounded in National Institute of Standards and Technology (NIST) standards. He emphasized reviewing cost allocation when cybersecurity is a shared corporate service and expressed willingness to collaborate with the legislature.

Jeremy Young, CEO, Federal Resources Corporation (FRC), said Pennsylvania should move from measuring cybersecurity spending and compliance activity to measuring cybersecurity outcomes. He described a threat environment accelerated by automation and artificial intelligence (AI), outlining the scale and asymmetry of risk across thousands of employees, devices, applications, identities, suppliers and systems. He argued that cybersecurity must be a continuous risk-management discipline rather than an episodic compliance exercise. He cited federal frameworks as foundations and recommended several focus areas, including maintaining inventories, continuous monitoring of critical controls, connecting spending to demonstrable risk reduction with evidence; treating third-party and supply-chain risk as utility risk and properly preparing for risks posed by AI. He urged starting with a pilot of willing utilities to set outcome measures, monitor controls, test effectiveness, set remediation timelines and measure risk reduction while allowing flexibility in technical solutions.

Rep. Gallagher asked whether current rate structures allow necessary capital investment in cybersecurity upgrades without undue ratepayer burden. DeFrank responded that determinations are made in the rate-case process and that OCCO reviews expenses to ensure prudence, balancing risk reduction against rate impacts and distinguishing baseline safeguards from extraordinary spending during rate cases.

Rep. Williams asked whether PUC has the authority it needs or whether the General Assembly should provide additional power. DeFrank said he believes the commission has the authority it needs under existing Title 66 authority. Rep. Williams noted NOPR's move away from self-certification and observed that legislatures find it difficult to write prescriptive standards that age quickly, suggesting tying state regulation to NIST standards while acknowledging standards evolve.

[Minority Chair Carl Walker Metzgar](#) (R-Somerset) asked whether once-a-year cybersecurity checkups are sufficient. Young answered that annual checks are insufficient, reiterated continuous monitoring and measurement of risk. Chair Metzgar sought guidance on defending investments to ratepayers amid rising rates. Young said regulators should require evidence that investments produced measurable risk reduction to justify expenditures to ratepayers, while emphasizing training and outcome-based accountability.

Sumit Nair, vice president and CIO, Essential Utilities, said Essential Utilities has not experienced a cybersecurity incident that disrupted operations, interrupted service or caused a material financial impact. He cautioned that threats persist and are constantly increasing. He described Essential Utilities' program aligned to the NIST cybersecurity framework, covering IT and OT. He said his company treats cybersecurity spending as a normal, prudent part of operating safe and reliable utility systems-analogous to investing in pipes or treatment plants. He stated the company has not recognized a material loss or cyber-related impact on customer rates. He emphasized cybersecurity is a continuous discipline requiring adaptation and collaboration with the PUC, peers and federal partners.

Craig Fahnestock, senior director of government relations, Pennsylvania Municipal Authorities Association (PMAA), said PMAA represents nearly 700 municipal authorities serving roughly 6 million Pennsylvanians and more than 500 associate members who provide expertise including IT and cybersecurity support. He said cybersecurity now implicates water supply, public health, environmental protection and public safety. He described municipal authorities as independent public entities governed locally and funded by user fees, which creates resource variability. He warned OT attacks can interfere with physical operations, treatment or distribution and stressed readiness for manual operation when Supervisory Control and Data Acquisition (SCADA) is unavailable. He suggested that any new commonwealth requirements be risk-based, scalable and coordinated with existing frameworks. He said success should be measured by reduced risk and improved response.

Rep. Gallagher inquired about barriers preventing smaller water authorities from reporting near-miss cyber incidents, and whether the commonwealth can incentivize a culture of transparent information sharing. Fahnestock said PMAA members take cybersecurity seriously and are conducting risk assessments but face concrete operational barriers, including a lack of dedicated IT staff, reliance on third-party vendors and limited access to proper technology in rural areas.

Rep. Williams said many are surprised water systems are routinely targeted and recounted recent multi-state and international incidents and asked what municipal systems want from legislators, specifically whether the PUC's approaches are on target and how state regulation should coordinate with U.S. Environmental Protection Agency (EPA) and the Department of Environmental Protection (DEP). Fahnestock replied that members follow EPA and DEP requirements and requested that commonwealth regulation be coordinated with those entities. He reiterated the need for funding and technical assistance, described PMAA's training and user-group activities and said there is no one-size-fits-all approach for authorities.

[Rep. Napoleon Nelson](#) (D-Philadelphia) asked whether utilities face new liability scrutiny, whether insurers are changing underwriting and whether cyber risk is being scrutinized by carriers. Nair said Essential maintains cyber insurance, scrutinizing applicants and ensuring safe practices.

Brian Harrell, CSO, FirstEnergy, said FirstEnergy serves about 2.1 million customers across 56 counties and described cybersecurity as a consumer-protection and reliability issue. He said the grid's digital interconnections create opportunities for nation-state actors and criminal organizations, warned that AI makes threats more dynamic and emphasized the potential for cascading impacts from incidents affecting one organization. He described FirstEnergy's program around six core functions-governing risk, identifying critical systems, protecting those systems, detecting suspicious activity, responding to incidents and recovery operations-aligned with NIST. He provided a metric that FirstEnergy's defenses block "10s of 1000s of automated malicious connection attempts against public-facing services each month" to illustrate the volume of malicious activity. He urged policymakers to view cybersecurity as a core investment in reliability while valuing information sharing.

Steven McElwee, CSO, Pennsylvania-New Jersey-Maryland Interconnection (PJM), said PJM treats cybersecurity as a reliability issue because incidents can reduce situational awareness and damage equipment. He said recent international conflicts show nation-state actors are targeting infrastructure, warned AI lowers the bar for attack automation and described grid conditions. He argued cybersecurity investments identify vulnerabilities before exploitation and benefit ratepayers and urged risk-based investments and accountability so consumers are not forced to pay for consequences of ineffective programs. He recommended policy that drives accountability for investment and risk management before incidents occur.

Rep. Gallagher asked whether protocols exist to ensure the electrical grid remains resilient enough to support other critical sectors if a localized cyber-attack compromises communications or water systems. Harrell referenced his work creating a North American Electric Reliability Corporation (NERC) grid security exercise, noting exercises have evolved to address interdependencies among telecommunications, water and other sectors. He said lessons from exercises drive updated response and recovery plans.

Rep. Williams asked what worries Harrell the most and what the General Assembly can do to help. Harrell said the sector has addressed much low-hanging cyber hygiene but that third-party supply-chain and vendor risk is his primary concern, urging that security be emphasized early in procurement rather than added later as a barrier. Rep. Williams asked whether the PUC's proposed rulemaking addresses third-party supply chain problems. Harrell said he had not yet reviewed the PUC proposal but would do so and reiterated the need for procurement-level security considerations.

[Rep. Jim Haddock](#) (R-Luzerne) asked how Pennsylvania ranks relative to other states and whether the PUC has the required tools. McElwee said he could not rank states but described Pennsylvania's alignment with NIST and regulation as positive. He said PJM primarily works with asset owners to ensure resiliency and added that state rulemaking helps utilities not subject to federal regulation.

Rep. Nelson asked whether federal action is sufficient and how states should work alongside federal efforts. McElwee said the electricity sector has substantial federal support and that state rulemaking can fill gaps for utilities that are not federally regulated. He said electricity and natural gas are federally regulated but he was unsure of the status of other sectors and reiterated state rulemaking can help. Harrell added that education government agencies would increase protection for the grid.

Qian Zhou, director of cybersecurity, Philadelphia Gas Works (PGW), could not deliver testimony due to technical issues.

Rep. Gallagher asked whether Essential's disaster recovery plan includes a "cyber blackout scenario" requiring extended manual analog operations of gas distribution. Nair said the company conducts annual cyber tabletop exercises, annual fall disaster-recovery tests to validate systems' restoration, nearly real-time information-system restoration capability and annual manual failover testing for gas operations.

Rep. Williams said the threat to utilities is persistent and that AI accelerates and intensifies the threat environment. He urged the General Assembly to continue conversation about rules and funding to address ongoing attacks.

Rep. Gallagher thanked the panelists for their expertise and stressed the importance of utilizing cybersecurity to protect Pennsylvania's critical utilities.