STATE OF CONNECTICUT
PUBLIC UTILITIES REGULATORY AUTHORITY

JOINT PETITION OF WILLIAM TONG ATTORNEY GENERAL FOR THE STATE OF CONNECTICUT, AND CLAIRE E. COLEMAN, CONSUMER COUNSEL FOR A REVIEW OF ARTIFICAL INTELLIGENCE UTILIZATION, DATA SECURITY, AND CYBERSECURITY IN THE OPERATIONS OF PUBLIC UTILITIES	:	DOCKET NO. 26-10-11
	:	OCTOBER 23, 2026

RESPONSE OF CONNECTICUT NATURAL GAS CORPORATION, THE SOUTHERN CONNECTICUT GAS COMPANY, AND THE UNITED ILLUMINATING COMPANY TO THE JOINT PETITION OF THE ATTORNEY GENERAL AND CONSUMER COUNSEL

Connecticut Natural Gas Corporation ("CNG"), The Southern Connecticut Gas Company ("SCG"), and The United Illuminating Company ("UI") (collectively, the "Companies") submit this response to the Public Utilities Regulatory Authority ("PURA"), to address the Petition filed on October 13, 2026 (the "Petition") by William Tong, Attorney General for the State of Connecticut and Claire E. Coleman, Consumer Counsel (collectively, the "Petitioners"). The Companies respectfully request that PURA rule that the Petitioners' request for a multi-docketed proceeding to investigate the use of artificial intelligence in the operations of Connecticut's electric, gas, and water utilities is moot because it is duplicative of PURA's established cybersecurity review processes and is unsupported by any showing that those processes are deficient.

The Companies further request that PURA deny the Petitioners' request to investigate public service companies' compliance with Conn. Gen. Stat. § 36a-701b, as enforcement of this statute is the exclusive responsibility of the Attorney General, and related questions have already been decided by PURA. In the event that PURA grants the Petition in any part, the Companies

request that PURA open a single, narrowly scoped proceeding, and that the scope include, and discovery extend to, how PURA and any other PURA appearing docket participants, including the Petitioners, use artificial intelligence and protect the cybersecurity and data security of utility and customer information in their possession.

I. The Petition is Duplicative of the Existing Cybersecurity Review Meeting and Practices

The Companies first recommend that PURA rule that the Petitioners' request ***is moot*** because it seeks an investigation that is largely duplicative of PURA's existing review processes. Those processes were developed through years of significant effort, involving collaboration between PURA, the utilities, the Office of Consumer Counsel, the Attorney General's Office, and other stakeholders. They further do not expose the utilities to potentially revealing highly confidential business, proprietary and grid infrastructure information in a public forum.

The Petitioners, who themselves participated in developing that framework, either overlook these efforts or seek to impermissibly relitigate them without cause. PURA's review processes establish a coherent framework and provide the public service companies with critical guarantees related to confidentiality, which are essential when the subject matter is the very security architecture that bad actors seek to exploit. An adversarial, multi-docketed proceeding would place those protections at risk, and could create a public roadmap of utility vulnerabilities by exposing critically sensitive information to bad actors. While the Companies appreciate that the use of artificial intelligence presents a novel topic for consideration, PURA deliberately designed its review processes to evolve with the dynamic cybersecurity landscape,[1] and artificial intelligence is precisely the type of emerging issue those processes were built to absorb. Rather than opening the multi-docketed proceeding contemplated by the Petitioners, PURA should use

[1] See, Docket No. 14-05-12, *PURA Cybersecurity Compliance Standards and Oversight Procedures*, Connecticut Public Utilities Cybersecurity Action Plan, April 6, 2016, at 25.

the tools already available to it. An abbreviated history of PURA's Cybersecurity Oversight Program and its annual cybersecurity review meetings is discussed below.

On February 19, 2013, the Connecticut Department of Energy and Environmental Protection ("DEEP") issued its Comprehensive Energy Strategy for Connecticut, in which it recommended that PURA conduct a review of Connecticut's electricity, natural gas, and major water companies to assess the adequacy of their capabilities to deter interruption of service. See, 2013 Comprehensive Energy Strategy for Connecticut, at 111. On April 14, 2014, in response to DEEP's charge, PURA issued a strategic plan entitled Cybersecurity and Connecticut's Public Utilities, wherein it outlined 12 questions for consideration, including the role of regulators. See, Cybersecurity and Connecticut's Public Utilities, at 25 – 28. These questions were fully explored in Docket No. 14-05-12, *PURA Cybersecurity Compliance Standards and Oversight Procedures*, with the participation of the public service companies, the Office of Consumer Counsel, the Attorney General's Office, and other stakeholders. Following a series of six technical meetings PURA ultimately developed its Cybersecurity Action Plan. See, Docket No. 14-05-12, Connecticut Public Utilities Cybersecurity Action Plan, dated April 6, 2016. See also, Technical Meetings dated January 15, 2015, February 4, 2015, March 5, 2015, March 18, 2015, June 16, 2015, and July 23, 2016. A critical component of PURA's Cybersecurity Action Plan is the Cybersecurity Oversight Program and its ongoing annual cybersecurity review meeting. Id., at 21 – 25. PURA hosted seven annual cybersecurity review meetings before determining that the process should be transferred to the biennial review of emergency plans. See, Docket No. 14-05-12, 2024 Connecticut Public Utility Annual Cybersecurity Report, at 6. See also, Docket No. 24-02-03, *PURA Review and Report on Connecticut Public Service Company Emergency Response Plans*, Final Legislative Report, at 14 – 15.

The Petitioners have not offered any evidence to suggest either that the existing review process is inadequate or that PURA would otherwise be better served by initiating a new adversarial proceeding. The Petition identifies no incident, deficiency, or harm attributable to any Connecticut utility's use of artificial intelligence. To the contrary, a review of the most recent annual reports shows that PURA has consistently lauded the results accomplished through its collaborative process. See, Docket No. 14-05-12, Annual Cyber Security Reports, dated December 20, 2024 at 2; dated March 31, 2023 at 1; and dated January 7, 2022 at 1. Although the Petitioners' request sets out a broad scope of inquiry, many of the topics identified by the Petitioners overlap with those already addressed in the Cybersecurity Oversight Program. See, Petition, at 5 (identifying eight discrete topics for consideration); see also, Docket No. 14-05-02, Connecticut Public Utilities Cybersecurity Action Plan, at 21 – 34 (identifying six foundational topics and a further 14 subtopics within the cybersecurity topic); 2021 Connecticut Public Utilities Annual Cybersecurity Report (identifying the three primary topics discussed); 2022 Connecticut Public Utilities Annual Cybersecurity Report (identifying three primary topics discussed and a further 10 subtopics), and the 2024 Connecticut Public Utilities Annual Cybersecurity Report (identifying three primary topics discussed and a further 10 subtopics). Finally, nothing within the reports suggests that additional scrutiny of the Companies is necessary. While the ever-evolving cybersecurity threat environment is a recurring theme in these reports, so too is the conclusion that the Companies meet their obligations to public safety and reliable service. Id. Absent any showing of a gap in the existing framework, there is no basis to divert PURA, utility, and stakeholder resources, ultimately funded by ratepayers, to a redundant investigation.

In light of the foregoing, PURA should rule that the Petitioners' request to open an investigatory proceeding is moot. As a practical matter, the Petitioners' request is largely

duplicative of the existing review processes. Because the Petitioners do not even address the existing review processes, they offer no justification for such a significant redundancy, and none exists. While the Companies acknowledge that the annual cybersecurity review meetings did not take place in conjunction with the most recent biennial review of emergency response plans,[2] the Companies understand that PURA's Reliability, Security and Resilience division has scheduled the cybersecurity review meeting during the month of November. The Companies do not object to PURA including a review of artificial intelligence within that meeting or otherwise deferring the topic to the next biennial review of emergency response plans. That approach would address any legitimate interest underlying the Petition while preserving the confidentiality protections and collaborative structure that have served the State well. As a procedural matter, the Petitioners' request raises significant concerns. As discussed above, the existing review process is the product of significant effort, involving collaboration between the State, utilities, and other stakeholders. Opening a new proceeding would necessarily require many of the same questions to be litigated again, risking inconsistent outcomes and regulatory uncertainty. Should PURA nonetheless determine that some further inquiry is warranted, it should open a single, limited proceeding confined to artificial intelligence, conducted under robust protective orders, rather than the open-ended, multi-docketed investigation the Petitioners propose. For these reasons, the Companies recommend that PURA deny the Petitioners' request as moot.

II. The Attorney General Has Exclusive Jurisdiction Over Breach of Security Reporting

The Petitioners have also requested that PURA investigate "whether the utilities follow what is required by Conn. Gen. Stat. § 36a-701b in reporting breaches[.]" See, Petition, at 5. The Companies respectfully request that PURA deny this portion of the Petitioners' request as it lacks

[2] See, Docket No. 26-02-03, *2026 Review of Emergency Response Plans*, Final Legislative Report, dated August 31, 2026.

jurisdiction. Conn. Gen. Stat. § 36a-701b(j) plainly states that the Attorney General alone is responsible for enforcing compliance with the statute's reporting requirements. The Attorney General cannot transfer an enforcement function to PURA that the General Assembly vested exclusively in his office, and a parallel PURA inquiry would risk conflicting determinations under the same statute. PURA may deny this portion of the Petitioners' request as a matter of simple subject matter jurisdiction.

The Petitioners also ask PURA to investigate "whether the utilities go beyond what is required by Connecticut's statute in reporting breaches, and whether the utility conducts a review after each data breach or cybersecurity breach to evaluate its policies and practices." See, Petition, at 5 – 6. For CNG and SCG, these questions have already been asked and answered in Docket No. 25-04-23. The Office of Consumer Counsel was a very active participant in that docket: filing the initial petition; issuing more than 50 interrogatories; preparing a report of its own investigation; submitting a brief; and providing written exceptions to the proposed final decision. The outcome of that docket was PURA's finding that CNG and SCG had "acted reasonably to (1) implement its cybersecurity program, (2) respond to the incident, and (3) notify other state agencies and customers." See, Docket No. 25-04-23, Final Decision, dated March 25, 2026, at 1. As that finding is barely more than six months old, collateral estoppel prevents the Petitioners' efforts to relitigate it anew.

In light of the foregoing, PURA should deny this portion of the Petitioners' request, as PURA either lacks the subject matter jurisdiction to investigate the issue or is precluded from doing so by virtue of collateral estoppel. At a minimum, any proceeding PURA may open should expressly exclude these previously decided and jurisdictionally foreclosed issues.

III. Any Investigation Should Necessarily Include PURA and All Docket Participants

In the event that PURA grants the Petitioners' request in any part, the scope of the proceeding must necessarily include PURA and all docket participants, including the Petitioners, and all parties should be subject to discovery on their use of artificial intelligence, their cybersecurity measures, and their data security measures. Utility and customer information does not reside solely with the Companies. Through rate cases, compliance filings, interrogatory responses, and technical meetings, PURA, the Office of Consumer Counsel, the Attorney General's Office, and other participants routinely receive, store, analyze, and transmit sensitive utility operational data and customer information, including information designated confidential or critical energy infrastructure information.

The risks the Petitioners identify do not stop at the utilities' firewall. If artificial intelligence tools are used to review, summarize, or analyze utility filings, the same questions the Petitioners pose to the utilities apply with equal force to those tools: what data is input, whether it is retained or used to train third-party models, who can access it, how it is secured, and how breaches are detected and reported. A vulnerability in any participant's systems could compromise the very information the Petitioners seek to protect, regardless of how well the Companies safeguard their own systems. An investigation that examines only one link in the chain would provide an incomplete and potentially misleading picture of the actual risk to customers.

These concerns are not hypothetical. The information the Companies provide in regulatory proceedings frequently includes confidential business information and grid information, such as system topology, substation and pipeline configurations, asset condition data, load and capacity data, network architecture, incident response procedures, and vendor relationships, much of which

is designated confidential or critical energy infrastructure information. If the Petitioners or other participants input that information into artificial intelligence tools, particularly publicly available or third-party hosted tools, the information may leave the protected regulatory environment entirely. Depending on the tool and its terms of service, inputs may be retained by the provider, reviewed by the provider's personnel, used to train or refine models, stored in jurisdictions outside the United States, or exposed through a breach of the provider's systems. Artificial intelligence tools may also aggregate discrete pieces of information that are individually innocuous into a comprehensive picture of grid vulnerabilities, and certain tools have been shown to be susceptible to prompt injection, data leakage, and the inadvertent disclosure of prior inputs to other users. Once such information is disclosed in this manner, it cannot be retrieved, and no protective order can undo the harm. In the hands of a bad actor, aggregated confidential grid information could be used to identify points of failure and plan attacks on the electric and gas systems on which Connecticut residents depend for their safety, health, and economic well-being. For these reasons, the Petitioners' own use of artificial intelligence on utility information poses a serious risk to the security of Connecticut's critical infrastructure and must be examined in any proceeding PURA may open.

Reciprocal discovery is also a matter of basic fairness and sound regulatory policy. The Petitioners ask PURA to scrutinize the Companies' policies and practices on the premise that the handling of sensitive information by artificial intelligence and the security of that information are matters of public concern. That premise applies equally to the government entities that request, receive, and rely on that information. Subjecting only the utilities to discovery would create an asymmetric record, deprive PURA of the information necessary to develop consistent standards, and undermine confidence that confidential filings are protected throughout the regulatory process.

Moreover, the Companies' willingness to continue providing sensitive information in future proceedings depends on assurance that recipients maintain safeguards at least as rigorous as those the Petitioners would demand of the utilities.

Accordingly, should PURA open a proceeding, the Companies request that PURA (1) limit the proceeding to a single docket focused on artificial intelligence; (2) direct that PURA, the Petitioners, and every other participant respond to discovery regarding their use of artificial intelligence, their cybersecurity measures, and their data security measures as applied to utility and customer information; and (3) adopt protective orders ensuring that security-sensitive information produced by any party is not publicly disclosed.

IV. Conclusion

The Companies respectfully request that PURA rule that the Petitioners' request for a multi-docketed investigatory proceeding is moot and deny the Petitioners' request to investigate the Companies' compliance with Conn. Gen. Stat. § 36a-701b as it lacks the jurisdiction to do so. In the alternative, should PURA grant the Petition in any part, the Companies respectfully request that PURA open a single, narrowly scoped proceeding, conducted under appropriate protective orders, that excludes matters within the Attorney General's exclusive jurisdiction and matters previously decided, and that includes PURA's own use of artificial intelligence, cybersecurity measures, and data security measures, as well as those of all docket participants, including the Petitioners, with all parties subject to discovery, so that any review is comprehensive and consistently applied to all parties that handle utility and customer information.

Respectfully submitted,

CONNECTICUT NATURAL GAS COPORATION,
THE SOUTHERN CONNECTICUT GAS COMPANY, and
THE UNITED ILLUMINATING COMPANY

By: *Alex E. Soter*

Alex E. Soter
Counsel
UIL Holdings Corporation
180 Marsh Hill Road
Orange, CT 06477
Phone: 203-836-4603
Fax: 203-499-2414
E-mail: alex.soter@avangrid.com

CERTIFICATION

This is to certify that on this day, the foregoing document was filed with the Public Utilities Regulatory Authority, and copies of the foregoing document were served upon each person designated on the Authority's official service list in this proceeding in accordance with R.C.S.A. § 16-1-15.

By: *Alex E. Soter*
Alex E. Soter
Counsel