107 Selden Street, Berlin, CT 06037
P.O. Box 270, Hartford, CT 06141-0270

Lauren H. Bidra
Senior Counsel

(860) 665-5429
Lauren.Bidra@eversource.com

October 22, 2026

Jeffrey R. Gaudiosi, Esq.
Executive Secretary
Public Utilities Regulatory Authority
10 Franklin Square
New Britain, CT 06051

Re: Docket No. 26-10-11, Petition of William Tong, Attorney General for the State of Connecticut, and Claire E. Coleman, Consumer Counsel, for a Review of Artificial Intelligence Utilization, Data Security, and Cybersecurity in the Operations of Public Utilities

Response to Joint Petition

Dear Mr. Gaudiosi:

The Connecticut Light and Power Company d/b/a Eversource Energy and Yankee Gas Services Company d/b/a Eversource Energy (together, the "Company" or "Eversource") respectfully respond to the Joint Petition of William Tong, Attorney General for the State of Connecticut, and Claire E. Coleman, Consumer Counsel, for a *Review of Artificial Intelligence Utilization, Data Security, and Cybersecurity in the Operations of Public Utilities*, submitted to the Public Utilities Regulatory Authority ("PURA") on October 13, 2026 ("Joint Petition").

This response provides the Company's perspective on the factors that should be considered in the event that PURA decides to undertake the inquiry requested by the Joint Petition. In short, Eversource emphasizes the need to establish measured and deliberate processes to review utility cybersecurity and artificial intelligence ("AI") practices with appropriate safeguards for maintaining the confidentiality of highly sensitive information. The Company supports the concept of a transparent and collaborative evaluation of the use of AI to ensure there is a secure and aligned process for all stakeholders working on important matters for Connecticut customers. A deliberative process would also help to ensure that evolving technology is used safely and for the benefit of the Company's customers.

- **Cybersecurity Practices**: Ensuring a high level of cybersecurity and protection of customer information is a paramount objective of the Company. The Company takes its obligations in this regard very seriously and is taking appropriate measures to guard against cyber threats, further harden information systems relied on throughout the organization and ensure continuing vigilance.

The Company encourages PURA to return to, and utilize, its well-worn path in reviewing sensitive information related to technology and cybersecurity so that earnest dialogue may be exchanged during non-public meetings outside of a public record. PURA established such a framework and collaborative process in Docket No. 14-05-12, PURA Cybersecurity Compliance Standards and Oversight Procedures, in order to strengthen the cybersecurity practices of public service companies. As described below, that framework and collaborative process can be leveraged to continue to safely review utility cybersecurity and AI practices.

- **Use of AI**: In addition to reviewing the utilities' utilization of AI with the same thoughtful process in which it has previously reviewed utility cybersecurity programs, PURA should consider establishing standards for the responsible use of AI by all parties, intervenors, and consultants in PURA dockets, given the inherent risks in supplying utility data to unapproved AI tools and confirming that confidential data is not used as inputs to generative AI tools.

- **Data Security Practices**: The Company can demonstrate its compliance with other regulators to PURA, as appropriate; however, the Company clarifies that there is an established statutory process for data security in the Connecticut Data Privacy Act, Conn. Gen. Stat. § 36a-701b, under which utilities have reporting obligations to the Connecticut Attorney General for prescribed data breach events.

1. Cybersecurity Practices

The Company routinely participates in applicable regulatory proceedings related to cybersecurity practices and partners with appropriate law enforcement to exchange cybersecurity intelligence. The Company employs robust security controls, technologies, and training strategies to defend against cyberattacks. The Company welcomes opportunities to collaborate with peer utilities and stakeholders on its cybersecurity program in an appropriate manner with safeguards to protect highly sensitive information.

PURA established a framework and collaborative process in Docket No. 14-05-12, PURA Cybersecurity Compliance Standards and Oversight Procedures, to strengthen the cybersecurity practices of public service companies.[1] That established process of over a decade relies on cybersecurity review meetings with utility, cybersecurity, and emergency response subject matter experts. PURA could consider reinitiating this process to review the cybersecurity practices of utilities. Cyberattacks are now a regular occurrence across industries, including the energy sector.[2]

[1] See Cybersecurity and Connecticut Public Utility Companies

[2] As the Joint Petition recognizes, "[t]he number of cyber attacks per week per energy organization has been steadily increasing this decade." Joint Petition at 3 (citing Eduardo Garcia, *Energy firms face AI-enhanced cyber attacks in connectivity*, REUTERS (Sept. 1, 2026)).

In that regard, PURA has previously recognized that confidential cybersecurity information requires appropriate procedural treatment. PURA's established utility cybersecurity review framework does not put confidential cybersecurity information in PURA's Cybersecurity Reports or even in the administrative record on a confidential basis. In fact, the process informs PURA but avoids PURA retaining any sensitive cybersecurity records. As PURA set forth in its "*Connecticut Public Utilities Cybersecurity Action Plan*," dated April 6, 2016:

> Drawing on the technical sessions, PURA proposed the following initial guidelines for the annual cybersecurity review meetings, which include protection against disclosure of sensitive information:
>
> 1. Utilities will hold private, closed-door meetings with the designated PURA and Division of Emergency Management and Homeland Security ["DEMHS"] representatives. No other companies will be present, and there will be no government participation other than PURA and DEMHS unless agreed in advance by the host utility.
>
> 2. Meetings will be at the utility's office or another mutually agreed place;
>
> 3. Meeting participants shall be bound by a non-disclosure agreement ["NDA"] not to release or otherwise reveal information shared or divulged through the cybersecurity review;
>
> 4. PURA and the other government participants will not retain records, in hardcopy, electronic or other format. Neither PURA nor the government participants will take custody of confidential information;
>
> 5. Each utility will maintain a cybersecurity risk register, which will be reviewed during the annual meeting; and
>
> 6. Each utility will document and track actions requested by PURA and DEMHS to enable follow-up and review at subsequent meetings.

Docket No. 14-05-12, PURA Correspondence entitled "*Connecticut Public Utilities Cybersecurity Action Plan*," dated Apr. 6, 2016, at 24-25.

Thus, PURA has already recognized the substantial risks in publicly disclosing highly sensitive cybersecurity information into the public domain, and for these reasons, has previously erred on the use of confidential meetings without obtaining possession of confidential records in order to help protect the security and integrity of the electric and natural gas systems that serve our Connecticut customers. No one wants such sensitive information to unintentionally fall into the hands of one or more cybercriminals who will misuse that information to harm our systems and customers. For these reasons, the Company recommends that PURA employ the same sound and established process for reviewing the utilities' cybersecurity and AI practices.

2. The Use of AI

Utility Use of AI

The Company's AI strategy emphasizes cybersecurity, data privacy, oversight, and responsible application of emerging technologies. AI initiatives are evaluated through established corporate governance processes, including appropriate business and technical review. While exploring the potential safe use of AI as a productivity tool, ensuring a high level of cybersecurity and protection of customer information remains a principal objective for the Company. All technology at the Company, including AI, must be used responsibly, ethically, and professionally in a manner consistent with the Company's values, ethical standards, risk tolerance, and industry-specific obligations.

In the event that PURA elects to move forward with the Joint Petition, PURA should review utilities' use of AI in the same way it has reviewed utility cybersecurity programs—*i.e.*, with appropriate stakeholders in private, closed-door meetings; with the use of NDAs; and through a process whereby government entities do not take custody of confidential AI information—so that highly sensitive information about technology is not publicly available to cybercriminals who may manipulate the information to attack the State's utilities.

For instance, the Joint Petition requests that "each of the companies should be required to report ***all use of AI systems*** in their operations including but not limited to the functional objective of the system, the level of human oversight, and the policies, procedures, and protocols that govern the use of AI systems within their organizations." Joint Petition at 5 (emphasis added). It is essential that an appropriate process for confidentially be established, as PURA developed in Docket No. 14-05-12, because a catalog of the Company's use of AI would provide hackers information that could be used to target those systems and specifically design attacks targeting AI use cases.

Process for Stakeholder Use of AI in PURA Proceedings

Separate from the utilities' AI practices, PURA should utilize the administrative uncontested docket process to evaluate and set standards for the way in which parties, intervenors, and their consultants may use AI in PURA dockets. As guiding principles, fairness, transparency, accountability, and security must be prioritized. All stakeholders have a shared responsibility to ensure that sensitive utility data—such as data about important infrastructure projects, Critical Energy/Electric Infrastructure Information, and any information about potential infrastructure vulnerabilities—does not fall into the hands of bad actors who may weaponize the information to launch cyberattacks.

If PURA elects to move forward with the Joint Petition, PURA should examine appropriate protocols for the use of Large Language Models ("LLMs") given the inherent risks in supplying Company data into unapproved AI tools. Also, PURA should establish a process for notification to utilities when their discovery information is supplied into AI tools by parties, intervenors, and

their consultants. As a floor, all state agencies and their consultants must follow the State of Connecticut Policy AI-01 AI Responsible Use Framework.[3]

3. Data Security Practices

The Company complies with the data breach law in Connecticut, which is the Connecticut Data Privacy Act, Conn. Gen. Stat. § 36a-701b ("CTDPA"), enforced by the Connecticut Attorney General.[4] The Joint Petition recommends that PURA's investigation should include:

> [A]n inquiry into data security and cybersecurity protections and breaches, both stemming from AI and outside of AI. This inquiry should include which entities and customer groups are informed about data breaches, whether the utilities follow what is required by Conn. Gen. Stat. § 36a-701b in reporting breaches, 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.

Joint Petition at 5.

In fact, there is a specific statutory scheme for data breaches in Connecticut that does not include PURA review or enforcement. The CTDPA is under Title 36(a) of the Connecticut General Statutes related to "The Banking Law of Connecticut," not Title 16 related to "Public Service Companies." Accordingly, Connecticut utilities comply with the CTDPA as a "person" who "maintains computerized data" that includes the personal information of Connecticut residents, not as public service companies. See, Conn. Gen. Stat. § 36a-701b(b)(1). Whether the utilities should "***go beyond*** what is required by Connecticut's statute in reporting breaches" in Title 36a is a legislative matter. Joint Petition at 5 (emphasis added).[5]

4. Conclusion

Eversource appreciates the opportunity to respond to the Joint Petition and, should PURA elect to move forward with the Joint Petition, urges PURA to proceed in a deliberate manner that adequately protects highly sensitive information related to cybersecurity and technology.

---

[3] Policy AI-01 expressly prohibits the submission of confidential or privileged information to LLMs, such as ChatGPT, Bard, Bing, and Chat, and generative AI. Policy AI-01 also provides many other guidelines and prohibitions around the use of AI by state agencies.

[4] The Connecticut Data Privacy Act

[5] Connecticut law is well established that administrative agencies such as PURA are tribunals of limited jurisdiction and their jurisdiction is dependent entirely upon the statutes vesting them with power; administrative agencies cannot confer jurisdiction on themselves. See Tele Tech of Conn. Corp. v. Dep't of Pub. Util. Control, 270 Conn. 778, 789 (2004) (internal citations & quotes omitted).

Respectfully submitted,

Lauren H. Bidra

Vincent P. Pace
Assistant General Counsel
Lauren H. Bidra
Senior Counsel
On Behalf of The Connecticut Light and Power Company d/b/a Eversource Energy and
Yankee Gas Services Company d/b/a Eversource Energy