Senator Hardy,

Thank you for taking the time to hear from me this afternoon. Please find below a written copy of my remarks on H.291 on behalf of Green Mountain Power (GMP) and Vermont Gas Systems (VGS).

We have reviewed Draft 1.2 of H.291 dated April 27, 2023, and appreciate several of the proposed changes, specifically the provision clarifying that the Council would retain its authority to review best practices but would not have the authority to approve cybersecurity standards for critical infrastructure. We believe this change meets the proposed Council's statewide coordination objective without risking involvement with existing federal and state cybersecurity regulations.

GMP and VGS are both fully regulated by the Public Utility Commission and are subject to various cybersecurity standards already in place. While both companies are firmly committed to cybersecurity and welcome oversight from state regulators, we do not believe that another layer of oversight in the form of a Cybersecurity Advisory Council that approves cybersecurity standards for critical infrastructure is necessary or appropriate. Oversight of cybersecurity standards for both companies is already handled through federal, industry, and regional transmission operator standards, with Public Utility Commission (PUC) oversight at the state level in accordance with a series of orders and memorandums of understanding.

As critical infrastructure, all utilities coordinate with the federal Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA), which provides frequent updates about energy-related threats. Electric utilities also are subject to North American Electric Reliability Corp (NERC) critical infrastructure standards, while gas utilities such as VGS follow the Transportation Safety Administration (TSA) Pipeline Security Guidelines, and collaborate with industry peers, including other utilities, gas utilities, and the American Gas Association, to share information about cybersecurity and threats.

GMP, along with VELCO, VEIC and other Vermont distribution utilities, are also subject to a 2019 Public Utility Commission order, including a statement of principles relative to cybersecurity. The 2019 order requires each utility to maintain a cybersecurity program, tailored to that utility's specific needs and infrastructure. Utilities are required to notify the Commissioner of Public Service of any cybersecurity attack that results in the release of confidential customer information, a compromise of grid reliability, or required reporting to another entity. The order also requires the Department of Public Service is required to convene an annual meeting with the utilities to discuss significant developments relating to cybersecurity programs, including implementation of any new or proposed state or federal cybersecurity standards. The utilities have also signed on to an MOU that outlines how this information is shared among parties, since aspects are highly sensitive.

One point of clarity that we would draw the committee's attention to is the Council membership, specifically the seat reserved for "*a representative from a State electrical public utility, appointed by the Commissioner of Public Service*". We would respectfully submit that this clause should read "*a representative from a Vermont distribution or transmission utility, appointed by the Commissioner of Public Service*."

Thank you again for the opportunity to speak to the committee. Please do not hesitate to reach out if you have any questions.

Best,

Dylan Zwicky