Date Filed: August 11, 2026

Witness: Christopher Leigh and Jared A. Lawrence
Request from: Office of Consumer Counsel

Question:

(Cybersecurity) The cybersecurity section of Exhibit CLP-AMI-2 on pages 34-35 considers only cybersecurity issues related to customer data and privacy. Please provide information on if and how the company plans for and addresses cybersecurity threats outside of the individual data collection and data privacy space, including but not limited to operational security and assessment of third party companies.

Response:

The Eversource Cyber Security Plan (provided in this proceeding as OCC-128, Attachment 1 CONFIDENTIAL), Section 6 Situational Awareness and Section 7 Information Sharing and Communications discuss our overall program for addressing cyber-security threats. Eversource works closely with various government agencies to share threat information. This information is part of our situational awareness for how threat actors target critical infrastructure. Then detection alerts are created and monitored, and, if needed, action taken.

Eversource participates in various government information sharing programs where network traffic is provided to DOE and DHS programs for analysis. This provides the agencies with national situational awareness, when combined with other utility data. Their analysis also can result in specific threat information being provided back to Eversource for review. No customer information is ever provided to these agencies.

Eversource reviews third party controls through the Due Diligence Questionnaire ("DDQ"). Eversource also uses a third-party service to monitor the security posture of our critical vendors and if their posture score drops or notice of an incident is made public, then we assess the risk to Eversource and will take appropriate action. However, the response to an event at a third-party site is the responsibility of the third party.