Date Filed: October 22, 2026

Witness: Christopher Leigh and Sean P. Noonan
Request from: ALLCO

Question:

(Storage and hosting of confidential information and CEII.) State whether the Company's confidential information, customer information, and CEII are stored or processed in any third-party cloud or hosted environment (including, without limitation, Microsoft 365, Microsoft Azure, Amazon Web Services, Google Cloud, Salesforce, ServiceNow, Oracle, SAP, PowerPlan, or any e-discovery or document-hosting platform), identifying each environment, the vendor, the country of hosting, and whether the vendor's terms permit it to use, retain, or train on Company data; and state whether any such environment includes AI Tool features (such as Microsoft 365 Copilot or Azure OpenAI) that are enabled for Company users, and if so which.

Response:

Eversource maintains an enterprise data governance and information protection framework designed to govern Company information based on its sensitivity, business need, regulatory obligations, and authorized use. The Company uses a four-tier information classification model consisting of Public Information, Internal Use, Confidential, and Highly Restricted. Confidential information includes confidential and proprietary business information, while more sensitive information, such as Critical Energy Infrastructure Information (CEII), is subject to heightened protection requirements.

Information stored within governed Microsoft 365 environments is subject to information-protection controls that include sensitivity classification, encryption where applicable, Data Loss Prevention (DLP), access and sharing controls, retention/lifecycle requirements, and monitoring. Eversource is continuing to expand these governance and protection capabilities across structured and unstructured information environments.

Microsoft 365 Copilot and Copilot Chat are enabled for approved Company users within the Microsoft enterprise environment. Eversource has implemented controls intended to restrict Copilot processing of sensitive information. Current controls include DLP rules that prevent Copilot processing when defined sensitive information types are detected and separately block content classified as Confidential or Highly Restricted. Company guidance also restricts the use of sensitive or restricted information in Copilot prompts or supporting documents.

Eversource's broader AI governance model includes controlled enablement, security and governance review, data classification and DLP controls, monitoring, and defined accountability

for AI-related data protection. Unapproved external AI tools are restricted, and AI capabilities are subject to governance and security review prior to broader enablement.

Vendor-specific contractual provisions, hosting locations, data-retention rights, and terms governing whether a vendor may use Company data to train or improve its models are governed through the applicable contractual and third-party review processes and should be addressed, where required, by the appropriate Legal, Procurement, or technology service owner.