Date Filed: August 14, 2026

Witness: Christopher Leigh
Request from: Office of Education, Outreach, and Enforcement

Question:

(INFORMATION TECHNOLOGY REVIEWS) Does the Company regularly perform security evaluations or have an independent evaluation of its technological infrastructure systems? Please provide all related Company policies and procedures regarding cybersecurity protections and cybersecurity evaluations of the Company's technology systems.

Response:

The Company regularly performs IT security evaluations, with support from security assessment professionals. The work is facilitated by the Eversource Energy Internal Audit Department.

Internal Audit Approach
The Eversource Energy Internal Audit Department is responsible for several important functions within the management structure, including but not limited to the following functions:

- Establishing controls and risk management activities and assuring that those processes are designed adequately and operating effectively.
- Implementing processes to assure that resources are acquired economically, used efficiently and protected adequately.
- Implementing processes to assure that business programs, plans and objectives are achieved.
- Implementing processes to assure that quality and continuous improvement are fostered within the organization.

The development of the annual Audit Plan is among the most critical functions that Internal Audit performs. A thorough and effective planning process helps to ensure that Internal Audit is able to assemble a meaningful and challenging plan, designed to provide Company management with timely and useful feedback on Company operations and the control environment. Audits related to technological infrastructure systems and IT security are considered during the development of the annual audit plan.

The audit process varies, depending on the specific audit scope, in order to evaluate the technology system chosen for audit.

The following confidential attachments provide the Eversource Energy IT Security Policies.

- EOE-002, Attachment 1 CONFIDENTIAL – **Security Management** – Defines the governance structure for information security, including the establishment of a robust security infrastructure and the delivery of ongoing security training and awareness programs to all personnel.

- EOE-002, Attachment 2 CONFIDENTIAL – **Risk Management** – Outlines processes for information ownership, classification, and periodic risk assessments. Establishes security baselines and safeguards for both hard copy and electronic media, including emerging considerations for Artificial Intelligence (AI) security.

- EOE-002, Attachment 3 CONFIDENTIAL – **Personnel Security** – Implements controls for pre-employment screening, separation of duties, and ongoing personnel oversight. Includes measures for secure handling of transfers, resignations, and terminations to prevent unauthorized access.

- EOE-002, Attachment 4 CONFIDENTIAL – **Physical Security** – Protects facilities and information systems through physical access controls, environmental safeguards, and secure facility management.

- EOE-002, Attachment 5 CONFIDENTIAL – **Operations Management** – Establishes operational controls to prevent, detect, and respond to malicious code, ensure reliable backup and recovery, maintain software support, and manage configuration changes securely.

- EOE-002, Attachment 6 CONFIDENTIAL – **Security Monitoring and Response** – Defines continuous monitoring activities, incident detection, and coordinated response procedures to mitigate threats and minimize impact.

- EOE-002, Attachment 7 CONFIDENTIAL – **Communications Management** – Establishes Encryption, Exchange of Information, Email, Internet and Other Electronic Communications, Voice / Fax / Video Communications, Meetings and Conversations

- EOE-002, Attachment 8 CONFIDENTIAL – **Access Control** – User Enrollment and Authorization, Account Identification, Authentication, Privileged and Special Account Access, Remote Access, Wireless Access

- EOE-002, Attachment 9 CONFIDENTIAL – **Network Security** – Network Access, Network Security Control Devices

- EOE-002, Attachment 10 CONFIDENTIAL – **Third Party Services** – Third Party Services

- EOE-002, Attachment 11 CONFIDENTIAL – **Application Management** – Application Development Process, System Business Requirements

- EOE-002, Attachment 12 CONFIDENTIAL – **Business Continuity** – Business Continuity Management Program, Recovery / Business Continuity Plan Testing, Recovery Sites, Disaster Recovery Runbooks

- EOE-002, Attachment 13 CONFIDENTIAL – **IT Management** – IT Management Infrastructure, Change Management

- EOE-002, Attachment 14 CONFIDENTIAL – **IT Incident Management** – IT Event Management, IT Incident Management

Note: Policy 13 is a placeholder for a future policy to be determined.