Date Filed: August 11, 2026

Witness: Christopher Leigh
Request from: Office of Consumer Counsel

Question:

(Cybersecurity) Please provide details on the Company's cybersecurity monitoring center, including staffing levels, organization chart, background of staff and their experience in cybersecurity, documented strategies to structure the monitoring center's work, and guidelines for responding to alerts originating from the automated monitoring system.

Response:

The Eversource cybersecurity monitoring center is a three-tiered model consisting of a combination of 11 contractors and 8 Eversource employees. Level One consists of 8 contractors who provide the 24/7 monitoring of Eversource's initial detection capabilities. Level One monitors for alerts and performs initial triage and outreach. They follow a set of standard operating procedures ("SOPs") to either resolve or escalate events and incidents. Events can include malware detection, improbable travel, failed logins, locked accounts, and a number of other detections.

Level Two consists of 2 contractors and 3 Eversource employees. Level two provides advance monitoring in restricted tools sets, initial escalation support, and investigation capabilities. Level Two operates Eversource's email and data loss prevention defenses and cyber threat intelligence program. In addition, they receive alerts and notifications from other IT or OT teams.

Level Three consists of 3 Eversource employees who provide more advanced event and incident response capabilities including threat hunting, computer forensics, and network defense. Level Three also develops detection rules and workflows that provide the alerts for Levels One and Two. Other teams contribute technical expertise and support as needed based upon the challenge and technology.

Levels Two and Three provide 24/7 support to Level One through an after-hours on-call system. In addition, the contractor provider has its own manager. The overall security monitoring center is led by an Eversource supervisor and manager.

The contractors are trained and certified through the vendor's in-house training program and pipeline. The Eversource employees come from a variety of experience to include military and legal backgrounds. Each Eversource employee member is required to participate in a minimum of 40 hours of training per year to develop and maintain cybersecurity skills. This includes

participation in cyber exercises, certification courses, and vendor provided tool specific training. Collectively, the team has professional certifications in incident response, network monitoring and detections, network forensics, computer forensics, penetration testing, malware analysis/reverse engineering, operational technology security and incident response, and cybersecurity management with more than 75 years of shared cybersecurity experience.

Standard Operating Practices are developed collaboratively between the contractor providers and the Eversource team. Lessons learned are incorporated into the documentation over time. In addition, both teams work together to refine and tune detections and alerts to reduce noise and improve the accuracy of the alerts. In the event of a major incident, Eversource has an Incident Response Plan ("IRP") that defines the composition of the initial response team, responsibilities, authorities, and communications requirement. Other plans and documents such as personal data breach plans and disaster recovery plans support the IRP.

Please refer to OCC-131, Attachment 1 CONFIDENTIAL, for an organizational chart of the Company's Cybersecurity staff.