Chief Cybersecurity Risk Officer
55 Farmington Avenue
Hartford, Connecticut 06015
October 12, 2017

Honorable Dannel P. Malloy, Governor, State of Connecticut
Co-Chairs, Vice Chairs and Ranking Member, Committee on Energy and Technology
Honorable Elin Swanson Katz, Consumer Counsel

Honorable Connecticut Officials:

Connecticut has concluded its first set of annual cybersecurity reviews with the state's electric, natural gas and water utility companies. The review process achieved its objectives of realizing a cooperative, candid, productive and insightful sharing of pertinent information regarding Connecticut's critical infrastructure cybersecurity defense.

The positive results support the Public Utility Regulatory Authority's decision to negotiate an agreed cybersecurity review and assessment rather than to mandate such a process through the traditional docket process.

The ground rules of the agreed review process provide that the proceedings and information shared are to remain confidential to protect each company's cybersecurity defenses, and that any information made public will be by explicit consent of each company. The attached 2017 Annual Review Report has been approved by the four State of Connecticut participants: Arthur House and Steven Capozzi representing PURA, and Brenda Bergeron and Brett Paradis representing respectively the Division of Emergency Management and Homeland Security (DEMHS) and the Connecticut Intelligence Center (CTIC), and by the four participating companies (Aquarion, Avangrid, Connecticut Water and Eversource).

The following are some of the key points in the 2017 Annual Review Report:

- Senior company executives led the company presentations, and all included professional cybersecurity officers with direct operational responsibility.

- All companies shared the same starting point: that Connecticut utilities face ongoing, changing and serious cybersecurity probes and need to maintain constant vigilance with skilled personnel and up-to-date defense systems.

- All four companies chose to conduct the reviews using the Cybersecurity Capabilities Maturity Model ("C2M2").

- All four companies have deployed an array of internal company defenses, retained external specialists, trade association insights and assets and other means to detect and thwart efforts to penetrate and compromise cybersecurity defenses.

- All four companies have healthy corporate cultures addressing cybersecurity hygiene, all have currently adequate operational defense systems and all are investing in ways to strengthen cybersecurity going forward.

- The Connecticut officials concurred that all four companies have made marked, positive improvements in their cybersecurity cultures since completion of PURA's Critical Infrastructure Cybersecurity Strategy in 2014 and the 2016 PURA Cybersecurity Action Plan.

- The review identified two main areas requiring ongoing vigilance and continued improvement to counter constantly evolving threat environments. The first is attention to spear phishing forms of malware and techniques of insinuating damaging intrusions into systems. The second is managing third-party services.

A noted positive benefit of the annual reviews was that inclusion of a DEMHS officer and a CTIC representative was increased company understanding of local and state resources, especially intelligence, law enforcement and emergency management, to support cybersecurity in Connecticut.

There was consensus that emergencies potentially involving cyber attacks on critical infrastructure would present scenarios and demands Connecticut has not experienced, requiring planning and cooperation beyond existing norms.

The attached report includes seven specific actions that support conclusion that Connecticut utilities are actively working to strengthen deterrence and to prepare for post-incident recovery.

Both the Connecticut officials and the participating companies agreed that as the threats facing cybersecurity continue to evolve, so, too, must creative and energetic efforts to stay ahead of the threats. The companies all offered to participate in state emergency activities designed to manage and alleviate the consequences of a cyber incident.

Realizing that achievement of cybersecurity is an ongoing process and challenge and not a state or finished accomplishment, the participants all look forward to continued vigilance and the important work of serving and protecting the people of Connecticut from the potentially dangerous consequences of cyber compromise.

Sincerely,

Arthur H. House

Arthur H. House
Chief Cybersecurity Risk Officer, State of Connecticut

Copies:

Chair Katie Dykes, Public Utilities Regulatory Authority
Commissioner Melody A. Currey, Department of Administrative Services
Commissioner Dora B. Schriro, Department of Emergency Services and Public Protection
Chief Information Officer Mark Raymond