



## **Filing Receipt**

**Filing Date - 2025-04-10 02:44:20 PM**

**Control Number - 57579**

**Item Number - 169**

**SOAH DOCKET NO. 473-25-11558  
PUC DOCKET NO. 57579**

<b>APPLICATION OF CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC FOR APPROVAL OF ITS 2026-2028 TRANSMISSION AND DISTRIBUTION SYSTEM RESILIENCY PLAN</b>	<b>§ § § § §</b>	<b>BEFORE THE STATE OFFICE  OF  ADMINISTRATIVE HEARINGS</b>
---	----------------------------------	---

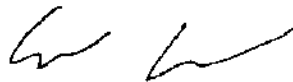
**OFFICE OF PUBLIC UTILITY COUNSEL’S  
ERRATA TO THE DIRECT TESTIMONY OF RONALD KEEN**

The Office of Public Utility Counsel (“OPUC”) submits this Errata to the Direct Testimony of Ronald Keen that was filed on April 8, 2025. This Errata makes the change below to Mr. Keen’s Direct Testimony.

1. Page 14, Footnote 20: Adds context to CenterPoint’s Responses to OPUC’s Third RFI.
2. Page 15, lines 17-19: Notes a potential threat vector related to detailed security information.
3. Page 17, lines 12-13: Context added for a lack of detailed responses to certain questions.

Date: April 10, 2025

Respectfully submitted,  
Benjamin Barkley  
Chief Executive and Public Counsel  
State Bar No. 24092083



---

Connor Drysdale  
Assistant Public Counsel  
State Bar No. 24143982  
Sharbel A. Sfeir  
Assistant Public Counsel  
State Bar No. 24071204  
Justin Swearingen  
Senior Assistant Public Counsel  
State Bar No. 24096794  
Chris Ekoh  
Deputy Public Counsel  
State Bar No. 06507015

1701 N. Congress Avenue, Suite 9-180  
P.O. Box 12397  
Austin, Texas 78711-2397  
512-936-7500 (Telephone)  
512-936-7525 (Facsimile)  
connor.drysdale@opuc.texas.gov (Service)  
sharbel.sfeir@opuc.texas.gov (Service)  
justin.swearingen@opuc.texas.gov (Service)  
chris.ekoh@opuc.texas.gov (Service)  
opuc\_eservice@opuc.texas.gov (Service)

**ATTORNEYS FOR THE  
OFFICE OF PUBLIC UTILITY COUNSEL**

**CERTIFICATE OF SERVICE**

SOAH DOCKET NO. 473-25-11558

PUC DOCKET NO. 57579

I hereby certify that a copy of the foregoing document was served on all parties of record in this proceeding on this 10<sup>th</sup> day of April 2025 by facsimile, electronic mail, and/or first class, U.S. mail.



---

Connor Drysdale

**SOAH DOCKET NO. 473-25-11558  
PUC DOCKET NO. 57579**

<b>APPLICATION OF CENTERPOINT</b>	<b>§</b>	<b>BEFORE THE STATE OFFICE</b>
<b>ENERGY HOUSTON ELECTRIC, LLC</b>	<b>§</b>	
<b>FOR APPROVAL OF ITS 2026-2028</b>	<b>§</b>	<b>OF</b>
<b>TRANSMISSION AND DISTRIBUTION</b>	<b>§</b>	
<b>SYSTEM RESILIENCY PLAN</b>	<b>§</b>	<b>ADMINISTRATIVE HEARINGS</b>

**DIRECT TESTIMONY**

**OF**

**RONALD KEEN**

**ON BEHALF OF THE**

**OFFICE OF PUBLIC UTILITY COUNSEL**

**APRIL 8, 2025  
(REVISED APRIL 10, 2025)**

1 taking into account the historical aggressiveness of adversaries, the resilience plan must be  
 2 as forward looking as possible without being unrealistic in the assessment of the threat.

3 CenterPoint's Response to OPUC'S Third Request for Information ("RFI")  
 4 Request No. OPUC-RFI03-03 evidences the following:

5 **QUESTION:**

6 Admit or deny, if "resiliency" is defined as the ability "to prevent,  
 7 withstand, mitigate, or promptly recover from the risks posed" and  
 8 the company examines all risks which can potentially impact the  
 9 company's business and operations, then the company should  
 10 develop a Rumsfeld Matrix to determine all risks within each  
 11 quadrant. If deny, please explain.

12 **ANSWER:**

13  
 14 The company does not use a Rumsfeld Matrix for this purpose;  
 15 however, the company does maintain a risk register which is used  
 16 by Cybersecurity to identify and rate the severity of risks to the  
 17 company's assets.<sup>20</sup>

18 **Q. ARE YOU SAYING A RUMSFELD MATRIX IS NECESSARY TO DETERMINE**  
 19 **THREATS AND VULNERABILITIES FRO RESILIENCE PLANS?**

20 **A.** No. A Rumsfeld Matrix is simply an effective tool that requires the plan developer to  
 21 research and understand both past threats and vulnerabilities potentially at a forensic level  
 22 as well as the current threat environment. Doing so allows the developer to understand the  
 23 adversary(s) and the trends used in past as well as current attacks. It gives the developer a  
 24 sense of the methodologies used and how those methodologies are evolving or, in some  
 25 cases, being disposed of in favor of new methodologies. It also potentially reveals

---

<sup>20</sup> CenterPoint Energy Houston Electric, LLC's Responses to Office of Public Utility Counsel Third Set of RFIs, Response to OPUC 3-3 (Mar. 26, 2025). ("CenterPoint's Response to OPUC's 3<sup>rd</sup> RFI"). [On March 13, 2025, OPUC and the Company discussed security concerns as to detailed responses and agreed to modifying the RFIs.]

“unknown knowns” or “unknown unknowns” – things the adversary knows about the company and its vulnerabilities and operations the company isn’t aware of.<sup>21</sup>

**Q. WHAT IS A THREAT VECTOR?**

A. A threat vector (or attack vector) is a method or mechanisms an adversary uses to gain illegal, unauthorized access to computer systems and networks.<sup>22</sup> Threat vectors can be classified as active or passive – understanding threat vectors develops an awareness of the entry points into computer components, systems, and networks (boundary protection). Armed with this information, vulnerabilities within the company’s business and operations systems and components of those systems can be remediated and gaps closed. Interpreting and understanding the magnitude of a threat vector also allows an appreciation of the scale of the attack surface – the company then can use that knowledge to eliminate or minimize the vector.

Taking a proactive approach to understanding threat vectors enables the employment of effective measures to significantly reduce risk – most cyberattacks take the path of least resistance and target known vectors that are often overlooked, especially those unknown to the company.

One such vector is access to detailed information about a company’s security and threat response procedures, which is why an agreement was reached for CenterPoint to provide general statements to certain RFI responses.

---

<sup>21</sup> See The Uncertainty Project – Rumsfeld Matrix at <https://www.theuncertaintyproject.org/tools/rumsfeld-matrix>. (Last Visited Apr. 7, 2025).

<sup>22</sup> See SailPoint -What is a threat vector? Examples in cybersecurity (May 14, 2023) at <https://www.sailpoint.com/identity-library/threat-vector>. (Last Visited Apr. 7, 2025).

1 response except in overall generalized terms, it is difficult to assess whether all threats have  
2 been identified or the proper measures applied to defeat those threats, whether identified  
3 or not.

4 **Q. CAN CENTERPOINT ARGUE THAT THE REQUIREMENTS OF THE**  
5 **SRP RULE HAVE BEEN FULFILLED IF CENTERPOINT BELIEVES THEIR**  
6 **TEAM HAS ADEQUATELY ADDRESSED ALL THREATS IN THE REGISTER?**

7 A. If CenterPoint were funding this initiative from their own resources without requiring  
8 additional funding from the ratepayer, I would agree. But, because the ratepayer is funding  
9 these initiatives and it is the ratepayer who ultimately pays the cost if the adversary, in  
10 some way, disrupts or shuts down CenterPoint operations, it is the ratepayer who must be  
11 assured that the Company has done everything possible to ensure its SRP is not just  
12 adequate, but also forward looking. Because the Company, due to security concerns that  
13 were shared with OPUC, will not share the details of the planning methodologies used  
14 (except in broad brush terms) or data considered in developing the measures (especially  
15 data dealing with prior attacks, including forensic and trend analysis data) to protect against  
16 cybersecurity incidents, the doubt in the comprehensiveness is sufficient to cause concern.

17 **Q. HAS CENTERPOINT PROVIDED ANY INFORMATION OR RESPONSE THAT**  
18 **LEADS YOU TO BELIEVE THE COMPANY MAY NOT HAVE CONSIDERED**  
19 **ALL THREAT VECTORS?**

20 A. In its Response to OPUC'S Third RFI Request No. OPUC-RFI03-02, CenterPoint stated,  
21 "The company examines all known risks which might reasonably be expected to impact