

extreme wind events typically associated with major storms, tornadic activity, and microbursts are the greatest risk to the Company's transmission and distribution system; and the proposed Resiliency Measures that will be implemented to mitigate the impact of extreme wind events. I next explain how the Company's approach in developing the 2026-2028 T&D SRP differs from the approach used by the Company for the 2025-2027 T&D SRP that was filed in Commission Docket No. 56548. Last, I explain the Company's systematic approach to implementing the other Resiliency Measures in the 2026-2028 T&D SRP, including vegetation management- and wildfire mitigation-related Resiliency Measures.

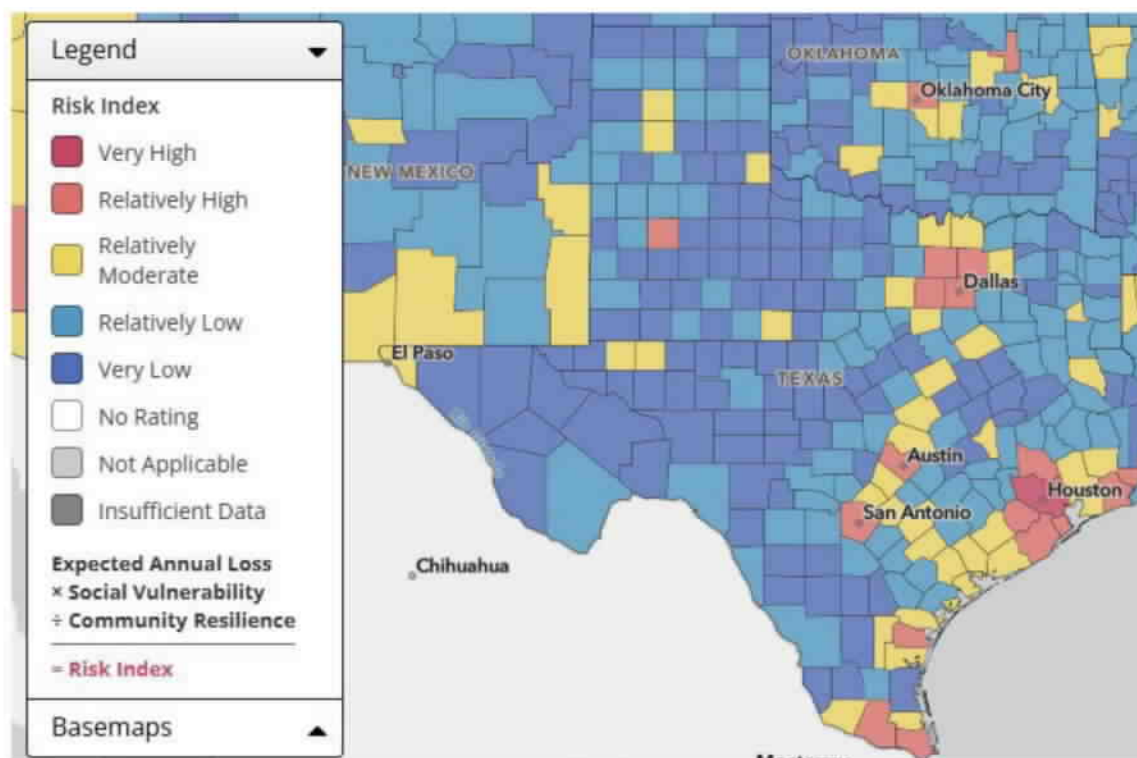
III. GREATER HOUSTON AREA: HIGHEST CLIMATE AND WEATHER-RELATED RISK IN THE COUNTRY

Q. WHAT ARE THE CLIMATE AND WEATHER-RELATED RISKS FACED BY THE GREATER HOUSTON AREA?

A. The Greater Houston area's location near the Gulf Coast subjects it to the following climate and weather-related risks: (1) extreme wind events (i.e., hurricanes, tropical storms, severe storms, tornadoes, derechos, microbursts); (2) flooding and extreme water events; and (3) extreme temperatures (i.e., droughts, freezes). As depicted in Figure EE-3 below, FEMA categorizes the Greater Houston area as being in the "very high" risk category for all hazards.²

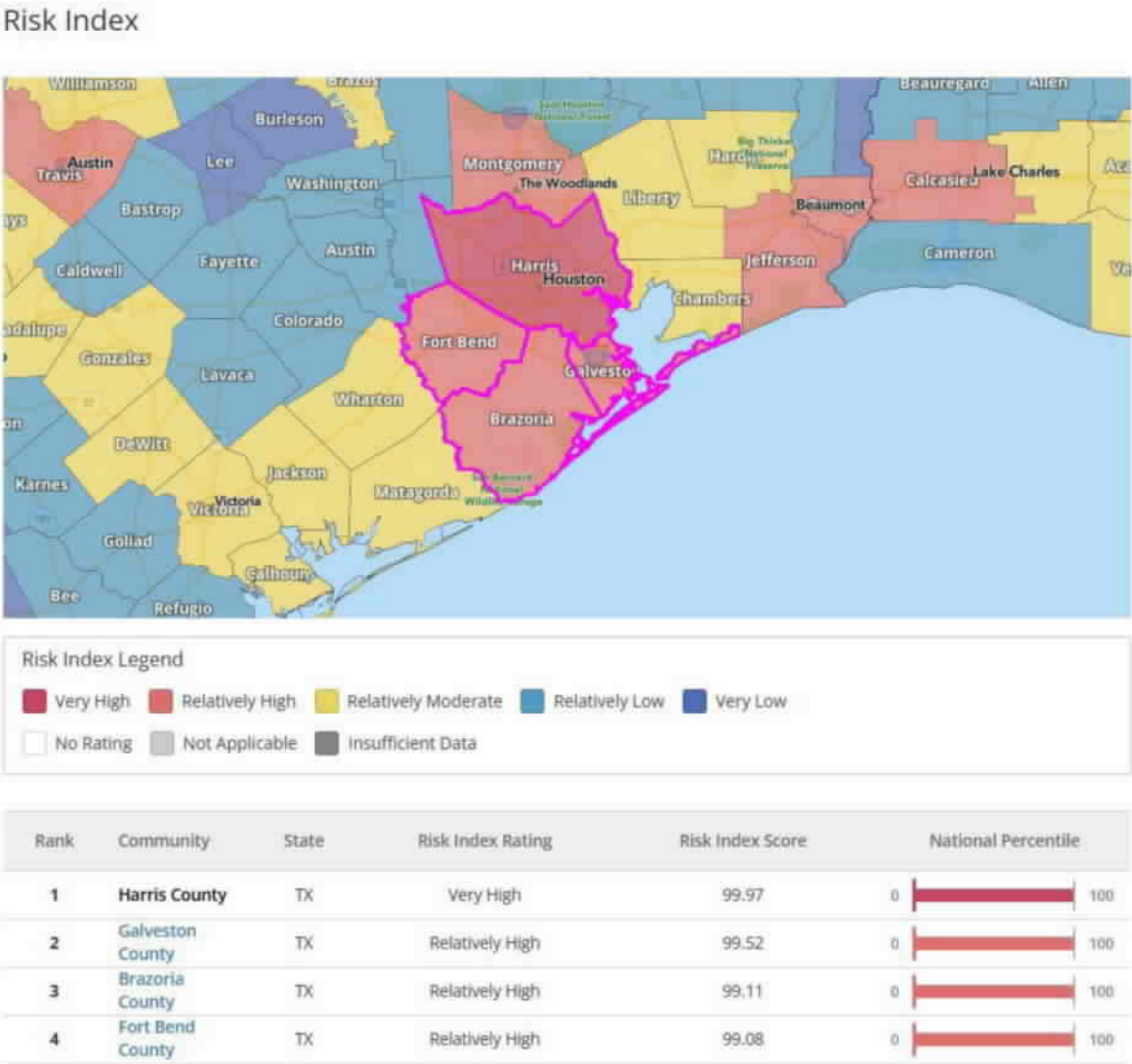
² FEMA's risk index map is available online at: <https://hazards.fema.gov/nri/map>.

Figure EE-3
FEMA Hazard Risk Map (Texas)



Additionally, as depicted in Figure EE-4 below, Harris County, Galveston County, Brazoria, and Fort Bend County, which comprise a large portion of the Greater Houston Area, have FEMA risk scores that put them in the 99.97, 99.52, 99.11, and 99.08 percentiles, respectively, in the country.

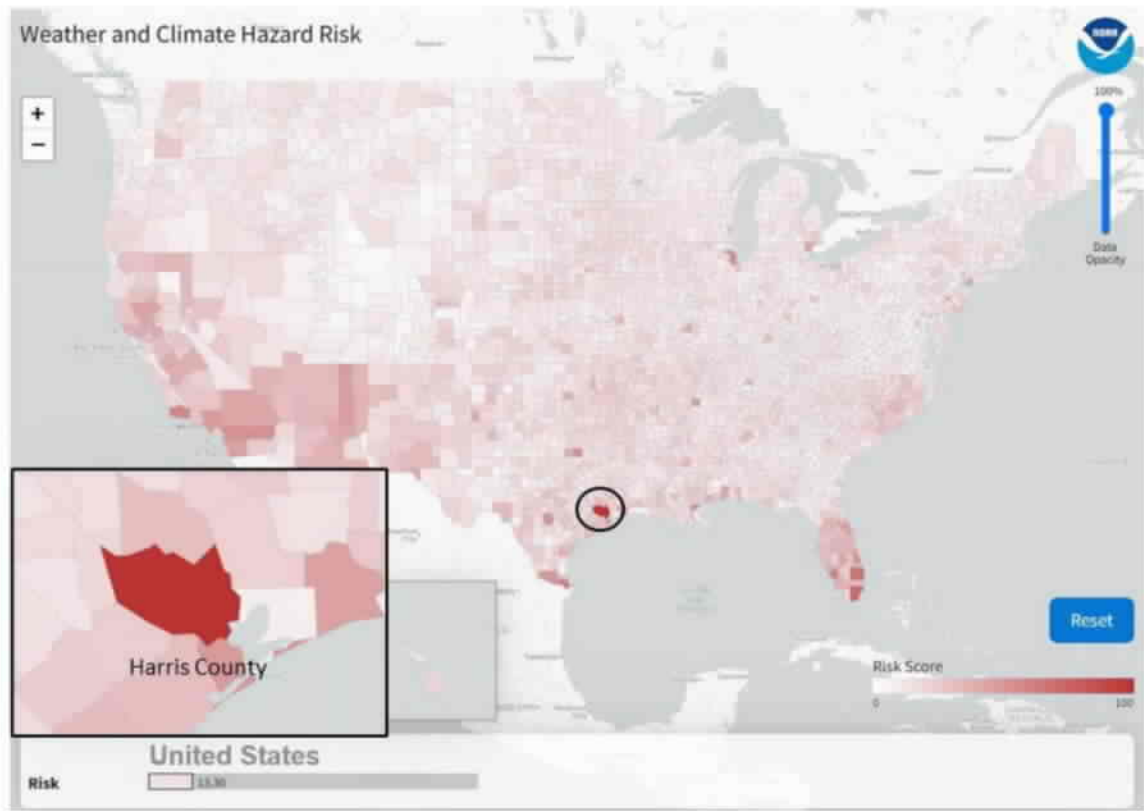
1 **Figure EE-4**
2 **FEMA Hazard Risk Map (Harris, Galveston, Brazoria, and Fort Bend Counties)**



3
4 NOAA further confirms that the Greater Houston Area has the highest weather and
5 climate hazard risk in the country. According to NOAA, Harris County has a risk
6 score of 100.00. The county with the second highest risk score is Miami-Dade
7 County, with a risk score of 71.53. Harris County's risk score is far greater than
8 the risk scores of Dallas County (53.94), Tarrant County (39.64), Bexar County

(50.56), Travis County (28.97), and the state of Texas (17.29) as a whole. In Figure EE-5 below, NOAA's risk map, illustrates Harris County's high risk relative to other counties throughout the country.³

Figure EE-5
NOAA Risk Map (United States)











Q. WHICH SPECIFIC CLIMATE AND WEATHER-RELATED RISKS CONTRIBUTE TO HARRIS COUNTY'S RISK SCORE OF 100.00?

A. The following Figure EE-6 from NOAA summarizes the risk scores for Harris County for specific climate and weather-related risks.

³ The NOAA's weather and climate risk map is available online at: <https://www.ncei.noaa.gov/access/billions/risk>.

Figure EE-6
NOAA Weather and Climate Risk Scores (Harris County, Texas, United States)

Risk and Vulnerability

Data Type	Harris County	Texas	U.S.
Weather and Climate Risk			
 Drought Risk	20.36	14.32	11.61
 Flooding Risk	100.00	12.97	9.13
 Freeze Risk	12.05	13.09	15.72
 Severe Storm Risk	94.56	20.58	16.99
 Tropical Cyclone Risk	100.00	6.41	4.36
 Wildfire Risk	11.81	11.28	6.30
 Winter Storm Risk	65.33	15.99	13.71
 Weather and Climate Combined Risk	100.00	17.29	13.30

Q. AS IT RELATES TO RESILIENCY, WHAT IS THE SIGNIFICANCE OF THE GREATER HOUSTON AREA HAVING THE HIGHEST CLIMATE AND WEATHER-RELATED RISK IN THE COUNTRY?

A. The Greater Houston Area having the highest climate and weather-related risk in the country is significant for two reasons. First, the Greater Houston Area having the highest climate and weather-related risk in the country justifies and underscores the necessity of the Company making substantial investments that enhance the resiliency of the Company's transmission and distribution system, consistent with the Company's prior resiliency-related investments and consistent with industry

best practice.⁴ The Company's 2026-2028 T&D SRP and the corresponding \$5.754 billion in resiliency-related investments is a continuation of the Company's commitment to making substantial investments that enhance the resiliency of the Company's transmission and distribution system and is warranted given the highest climate and weather-related risk level assigned by both FEMA and NOAA.

Second, the Greater Houston Area having the highest climate and weather-related risk in the country justifies and underscores the necessity of the Company implementing multiple types of hardening, modernization, flood mitigation, information technology, cybersecurity, physical security, wildfire mitigation, and vegetation management Resiliency Measures to enhance the resiliency of its transmission and distribution system. The diversity of the thirty-nine Resiliency Measures in the Company's 2026-2028 T&D SRP reflects the multi-faceted approach needed to mitigate the impact of the multiple types of climate and weather-related risk faced by the Greater Houston area.

IV. RISK-BASED ANALYSIS USED TO DEVELOP THE 2026-2028 T&D SRP

Q. HOW DID THE COMPANY DEVELOP ITS 2026-2028 T&D SRP?

A. In developing its 2026-2028 T&D SRP, the Company sought to enable the most effective mitigation at the least resilient locations of the Company's transmission and distribution system by:

- Decreasing asset failure risk by prioritizing less accessible locations, based on criticality and total customers;

⁴ Please refer to the Direct Testimonies of Deryl Tumlinson and David Mercado for examples of prior resiliency-related investments made by the Company, and the Direct Testimony of Eugene Shlatz for a discussion on industry best practice.

- 1 ▪ Increasing use of automation for a self-healing grid (i.e., IGSDs); and
- 2 ▪ Reducing restoration times by decreasing the number and extent of asset
- 3 failures, total customers affected, and time needed for repair.

4 The Company used a scenario-based framework in which the Company
5 conducted: (1) post-event analyses of Resiliency Events that have occurred in the
6 Greater Houston area and have caused power outages; (2) benchmarking against
7 industry best practices; and (3) scenario-based modeling.

8 **Q. WHAT IS A RESILIENCY EVENT?**

9 A. A Resiliency Event is a high impact, low frequency event such as “extreme weather
10 conditions, wildfires, cybersecurity threats, or physical security threats that poses a
11 material risk to the safe and reliable operation”⁵ of the Company’s transmission and
12 distribution system. For the Company, and as would be expected given the
13 proximity of the Greater Houston area to the Gulf Coast, past Resiliency Events
14 that have affected the Company’s transmission and distribution system are
15 primarily extreme weather-related events (e.g., extreme wind events associated
16 with storms).

17 **Q. WHY DID THE COMPANY ANALYZE PAST RESILIENCY EVENTS**
18 **THAT OCCURRED IN THE GREATER HOUSTON AREA?**

19 A. Analyzing past Resiliency Events that have occurred in the Greater Houston area
20 informs and assists the Company in:

⁵ Subsection (b)(3), T&D SRP Rule.

- Forecasting the types of Resiliency Events that may occur in the future in the Greater Houston area;
- Identifying the portions of the Greater Houston area and the Company's transmission and distribution system that may be impacted by similar types of Resiliency Events that occur in the future; and
- Identifying which portions of the Greater Houston area and the Company's transmission and distribution system that are susceptible to outages caused by extreme wind, vegetation, flooding, extreme temperature, and wildfire.

The Company used its analyses of past Resiliency Events to determine the Resiliency Measures to include in the Company's 2026-2028 T&D SRP, to determine the specific locations in the Greater Houston area and the Company's transmission and distribution system to implement Resiliency Measures, and to develop and enhance tools to forecast the impact of future weather-related Resiliency Events.

Q. WHICH PAST WEATHER-RELATED RESILIENCY EVENTS IN THE GREATER HOUSTON AREA DID THE COMPANY ANALYZE?

A. Figure EE-7 below summarizes the past Resiliency Events analyzed by the Company:

Figure EE-7
1980-2024 Resiliency Events Analyzed

1980s (10 Years)	1990s (10 Years)	2000s (10 Years)	2010s (10 Years)	2020-2024 (5 Years)
August 1983: Hurricane Alicia	December 1991: Severe thunderstorms	June 2001: Tropical Storm Allison	August 2011: Wildfires	February 2021: Winter Storm Uri
October 1984:	March 1992:	October 2002:	May 2015:	

Direct Testimony of Eric D. Easton
CenterPoint Energy Houston Electric, LLC
2026-2028 T&D SRP

1980s (10 Years)	1990s (10 Years)	2000s (10 Years)	2010s (10 Years)	2020-2024 (5 Years)
Severe storms, flooding	Severe storms, flooding	Severe storms, tornadoes, flooding	Severe storms, tornadoes, straight-line winds, flooding	September 2021: Hurricane Nicholas
May 1989: Severe storms, tornadoes, flooding	November 1992: Severe thunderstorms, tornadoes	September 2005: Hurricane Rita	October 2015: Severe storms, tornadoes, straight-line winds, flooding	February 2023: Tornado
June 1989: Tropical Storm Allison	October 1994: Severe thunderstorms, flooding	November 2006: Extreme wildfire threat	April 2016: Severe storms, flooding	June 2023: Microburst
	August 1998: Tropical Storm Charley	August 2007: Tropical Storm Erin	August 2017: Hurricane Harvey	May 2024: Derecho
	September 1998: Hurricane George	September 2008: Hurricane Ike	August 2017: Hurricane Harvey	July 2024: Hurricane Beryl
	October 1998: Flooding		September 2019: Tropical Storm Imelda	December 2024: Severe storms, tornadoes

1

2 **Q. DID THE COMPANY ANALYZE WEATHER-RELATED RESILIENCY**
3 **EVENTS THAT OCCURRED OUTSIDE OF THE GREATER HOUSTON**
4 **AREA?**

5 A: Yes, the Company reviewed resiliency events outside the Greater Houston area for
6 event types similar and unlike those historically occurring in the Company's service
7 area. Hurricane events from other states were reviewed, as well as less frequent
8 events including wildfires and ice storms occurring in various locations.

9

10 **Q. WHAT DID THE COMPANY CONCLUDE FROM ITS ANALYSES OF**
11 **THESE PAST RESILIENCY EVENTS?**

12 A. These analyses assisted in several ways, such as: validating effective mitigations
13 being considered by the company, understanding the potential consequences of less

1 likely event types, increased awareness of how changing weather patterns create
2 regional shifts in plausible event types, data points for model development and
3 confirmation of event type priorities. The Company, in collaboration with its
4 third-party resources, completed benchmarking of mitigation actions to determine
5 those predicted to provide the most customer value; the resiliency event review
6 complemented this effort by reviewing after action reports from historical events.
7 Similarly, these same reviews helped gain insights from events which were
8 exceedingly rare, such as the wildfires which occurred on island of Maui in August
9 2023 and the freeze event in Austin during February of the same year. The events
10 and after-action reviews offer empirical data points which serve as inputs for
11 damage prediction modeling and resiliency project identification. Ultimately, the
12 Company concluded that the past events that posed the highest resiliency-related
13 risk to the Greater Houston area and the Company's transmission and distribution
14 system were:

- 15 ▪ Extreme wind events associated with hurricanes, tropical storms, major storms,
16 tornadoes, and microbursts;
- 17 ▪ Flooding and other extreme water events that may result from hurricanes,
18 tropical storms, and major storms; and
- 19 ▪ Extreme freeze and drought events.

20 This conclusion is supported by Guidehouse's independent, third-party risk
21 assessment.

1 **Q. DOES THE COMPANY ANTICIPATE THAT SIMILAR EXTREME WIND**
 2 **EVENTS, FLOODING AND OTHER EXTREME WATER EVENTS, AND**
 3 **EXTREME FREEZE AND DROUGHT EVENTS WILL OCCUR IN THE**
 4 **GREATER HOUSTON AREA IN THE FUTURE AND THUS IMPACT THE**
 5 **COMPANY’S TRANSMISSION AND DISTRIBUTION SYSTEM?**

6 A. Yes. Based on Guidehouse’s independent, third-party risk assessment, the
 7 frequency and magnitude of extreme wind events, flooding and other extreme water
 8 events, and extreme freeze and drought events in the Greater Houston area are
 9 forecasted to increase over time. For example, maximum wind speeds in the twelve
 10 (12) counties in which the Company provides service are forecasted to increase
 11 between 2020 and 2050.

12 **Q. HOW DID THE COMPANY INCORPORATE ITS CONCLUSION OF**
 13 **PAST RESILIENCY EVENTS INTO THE 2026-2028 T&D SRP?**

14 A. Recognizing that extreme wind events, flooding and other extreme water events,
 15 extreme freeze events, and extreme drought events pose the highest
 16 resiliency-related risk and are forecasted to occur with greater frequency and
 17 magnitude, the Company included twenty-five (25) hardening, modernization,
 18 undergrounding, flood mitigation, wildfire mitigation, and vegetation management
 19 Resiliency Measures in the 2026-2028 T&D SRP to mitigate the impact of such
 20 events. Of the approximately \$5.754 billion that the Company will invest as part
 21 of its 2026-2028 T&D SRP, approximately \$5.405 billion of the \$5.754 billion will
 22 be invested for these twenty-five (25) Resiliency Measures. Additionally, of the
 23 \$5.405 billion that will be invested for these twenty-five (25) Resiliency Measures,

approximately \$4.013 billion of the \$5.404 billion will be invested in Resiliency Measures intended to mitigate the impact of extreme wind events. However, the Company's execution strategy requires flexibility to pivot within each Resiliency Measure, and from one Resiliency Measure to another as constraints are encountered so that program scope and activities pursued within each Resiliency Measure may be adjusted based on the needs of the Company's transmission and distribution system, as determined by the Company's analyses of the resiliency-related investment decisions. The need for flexibility is consistent with the Commission's SRP Rule, which acknowledges that each electric utility's transmission and distribution system has different system characteristics, is subject to different Resiliency Events and risks, and therefore should be given flexibility in developing the manner in which is appropriate to approach those risks.⁶ With that need for flexibility in mind, Figure EE-8 below breaks down how the Company anticipates investing \$5.405 billion in Resiliency Measures intended to mitigate the impact of extreme wind events, flooding and other extreme water events, extreme freeze events, and extreme heat events.

Figure EE-8

Estimated Costs for Extreme Wind, Flooding and Extreme Water, Extreme Freeze, and Extreme Drought-Related Resiliency Measures (in millions)

Resiliency Measure	T&D SRP Rule Category	Estimated Capital Costs 2026-2028	Estimated O&M Costs 2026-2028	Estimated Total Costs 2026-2028	Estimated 3-Year CMI Savings
Extreme Wind					
Distribution Circuit Resiliency (RM-1)	Hardening	\$513.4	None	\$513.4	263.0
Strategic Undergrounding	Undergrounding	\$860.0	None	\$860.0	81.1

⁶ Subsection (a)(1), T&D SRP Rule.

Resiliency Measure	T&D SRP Rule Category	Estimated Capital Costs 2026-2028	Estimated O&M Costs 2026-2028	Estimated Total Costs 2026-2028	Estimated 3-Year CMI Savings
(RM-2)					
IGSD Installation (RM-3)	Modernization	\$107.3	\$0.5	\$107.8	97.0
Distribution Pole Replacement and Bracing (RM-4)	Hardening	\$251.6	None	\$251.6	121.0
Vegetation Management (RM-5)	Vegetation Management	None	\$146.1	\$146.1	137.0
Transmission System Hardening (RM-6)	Hardening	\$1,467.3	\$0.8	\$1,468.0	223.8
69 kV Conversions (RM-7)	Hardening	\$369.3	None	\$369.3	65.5
S90 Tower Replacements (RM-8)	Hardening	\$118.4	None	\$118.4	59.5
Coastal Resiliency Projects (RM-9)	Hardening	\$177.4	\$0.8	\$178.1	7.8
Extreme Wind Total		\$3,864.6	\$148.1	\$4,012.7	1,055.7
Extreme Water					
Substation Flood Control (RM-10)	Flood Mitigation	\$43.8	None	\$43.8	3.9
Control Center Flood Control (RM-11)	Flood Mitigation	\$7.0	None	\$7.0	2.5
MUCAMS (RM-12)	Modernization	\$10.8	None	\$10.8	0.6
Mobile Substations (RM-13)	Modernization	\$30.0	None	\$30.0	3.9
Extreme Water Total		\$91.5	None	\$91.5	11.0
Extreme Temperature (Freeze)					
Anti-Galloping Technologies (RM-14)	Hardening	\$14.0	\$1.0	\$15.0	5.3
Load Shed IGSD (RM-15)	Modernization	\$4.5	\$0.1	\$4.6	N/A*
Microgrid Pilot Program (PP-1)	Modernization	\$35.0	\$1.5	\$36.5	N/A*
Extreme Temperature (Freeze)		\$53.5	\$2.6	\$56.1	5.3
Extreme Temperature (Heat)					
Distribution Capacity Enhancement/Substation (RM-16)	Modernization	\$579.6	None	\$579.6	138.1
MUG Reconductor (RM-17)	Modernization	\$245.0	None	\$245.0	13.6
URD Cable Modernization (RM-18)	Modernization	\$128.4	None	128.4	13.0
Contamination Mitigation (RM-19)	Modernization	\$144.0	\$6.0	\$150.0	15.7
Substation Fire Barriers (RM-20)	Hardening	\$9.0	None	\$9.0	1.5
Digital Substation (RM-21)	Modernization	\$31.8	None	\$29.4	1.2

Resiliency Measure	T&D SRP Rule Category	Estimated Capital Costs 2026-2028	Estimated O&M Costs 2026-2028	Estimated Total Costs 2026-2028	Estimated 3-Year CMI Savings
Wildfire Advanced Analytics (RM-22)	Wildfire	None	\$0.9	\$0.9	N/A*
Wildfire Strategic Undergrounding (RM-23)	Wildfire Undergrounding	\$50.0	None	\$50.0	N/A*
Wildfire Vegetation Management (RM-24)	Wildfire	None	\$30.0	\$30.0	N/A*
Wildfire IGSD (RM-25)	Wildfire	\$19.4	\$0.1	\$19.5	N/A*
Extreme Temperature (Heat)		\$1,207.2	\$37.2	\$1,244.4	183.1
Weather Event Total		\$5,216.8	\$187.9	\$5,404.7	1,255.1
Note: Please see Section 5 of Exhibit ELS-2 for a qualitative benefit analysis of this Resiliency Measure.					

1

2 **Q. IN ADDITION TO ANALYZING PAST RESILIENCY EVENTS, WAS A**
3 **BENCHMARKING STUDY PERFORMED?**

4 A. Yes. As part of Guidehouse's independent, third-party analysis of the Company's
5 2026-2028 T&D SRP, a benchmarking study was performed. The purpose of the
6 benchmarking study was to determine if the Resiliency Measures in the Company's
7 2026-2028 T&D SRP are consistent with the resiliency-related investments made
8 by comparable electric utilities. The benchmarking study concluded that the
9 Resiliency Measures in the Company's 2026-2028 T&D SRP are consistent with
10 and align with industry best practices on resiliency-related investments.⁷ Notably,
11 the top two weather events that the benchmarked electric utilities addressed in their
12 resiliency-related investments are extreme windstorms (i.e., extreme wind events)
13 and extreme temperatures (i.e., extreme freeze and heat events). Additionally, the
14 top two categories of resiliency-related investments made by the benchmarked

⁷ Refer to Appendix A and B of Guidehouse's report for additional detail on Guidehouse's benchmarking studies.

1 electric utilities are distribution pole replacements and circuit rebuilds (i.e.,
2 hardening) and automation (i.e., modernization).

3 **Q. HOW DID THE COMPANY USE THE RESULTS OF THE**
4 **BENCHMARKING STUDY IN DEVELOPING ITS 2026-2028 T&D SRP?**

5 A. The results of the benchmarking study further confirmed that the Company was
6 correct in identifying the types of Resiliency Events that posed risks to the
7 Company's transmission and distribution system and further confirmed the
8 appropriateness of the Resiliency Measures included in the Company's 2026-2028
9 T&D SRP.

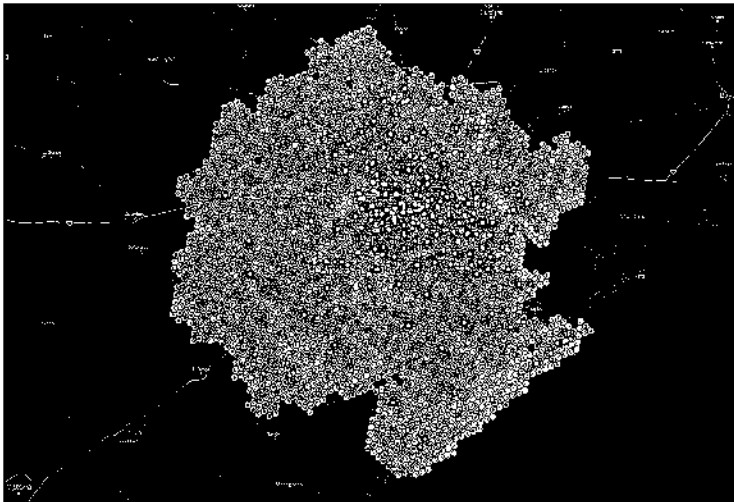
10 **Q. DID THE COMPANY CONDUCT SCENARIO-BASED MODELING TO**
11 **ASSIST IN THE DEVELOPMENT OF ITS 2026-2028 T&D SRP?**

12 A. Yes. The Company developed a robust internal model to identify regions in the
13 Greater Houston area or portions on the Company's transmission and distribution
14 system that are more susceptible to specific Resiliency Events and thus are potential
15 implementation locations for specific Resiliency Measures. The Company
16 conducted a granular analysis of future weather and climate impacts on the counties
17 in which the Company provides service. The level of granularity entailed dividing
18 the Company's service area into approximately 3,000 polygons that each represent
19 a contiguous 2-mile geographic area. The Company then layered on LiDAR data
20 on these polygons to conduct damage modeling, which was used to inform the
21 Company on potential locations for implementation of Resiliency Measures.

22 For example, the Company identified portions of its distribution system that
23 would benefit from the installation of IGSDs. Figure EE-9 below depicts portions

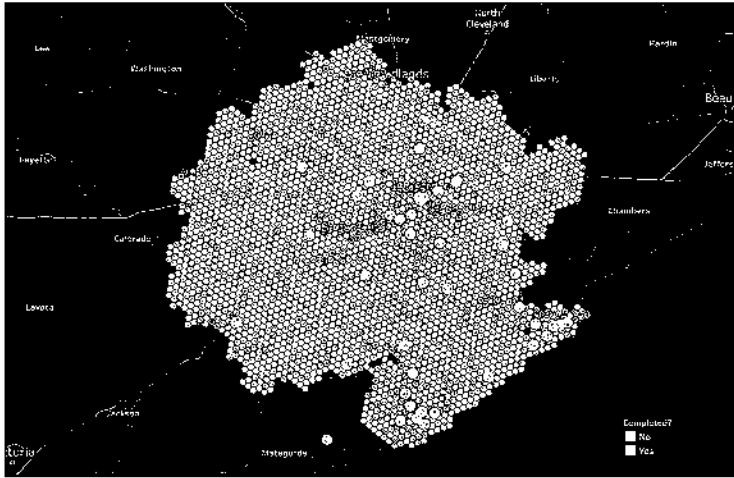
- 1 of the Company's distribution system that have been identified as potential
- 2 locations for IGSD installation.

Figure EE-9
Potential Locations for IGSD Installation



Similarly, the Company identified specific substations that are more susceptible to be impacted by a flooding or extreme water event and thus would benefit from the Substation Flood Control Resiliency Measure, which proposes to elevate substation equipment. Figure EE-10 below depicts the Company's substations that have already been elevated or are candidates to be elevated.

Figure EE-10
Locations for Elevated Substations



1 **Q. IN ADDITION TO IDENTIFYING REGIONS IN THE GREATER**
2 **HOUSTON AREA AND PORTIONS OF THE COMPANY'S**
3 **TRANSMISSION AND DISTRIBUTION SYSTEM THAT ARE MORE**
4 **SUSCEPTIBLE TO RESILIENCY EVENTS, DID THE COMPANY**
5 **CONDUCT OTHER SCENARIO-BASED MODELING?**

6 A. Yes. Using the same polygons and aerial imagery data, the Company modeled each
7 of the twelve (12) counties in which the Company provides service to identify
8 regions in each county that may receive damage due to a weather-related Resiliency
9 Event and the corresponding outage durations. For example, figure EE-11 below
10 depicts the regions in Harris County that may receive damage due to a
11 weather-related Resiliency Event and the corresponding outage durations for
12 customers in Harris County.

Figure EE-11
Harris County Damage Predictions and Outage Durations



Q. PLEASE EXPLAIN WHY THE COLORATION IN THE DAMAGE PREDICTION POLYGONS DOES NOT ALIGN WITH THE COLORATION IN THE OUTAGE DURATION POLYGONS.

A. Outage durations can differ from the damage prediction based on a number of factors. One example is localized events such as tornados which disrupt predicted behavior. This example occurred during the modeling of Hurricane Beryl where a tornado caused a divergence in the model prediction and actual outcomes. A second cause of misalignment in the polygon-based predictions is event specific crew deployment. Event specific crew allocations can be impacted by factors such

1 as road closures or coordination with emergency management agencies and critical
2 infrastructure locations such as hospitals, fire, or police.

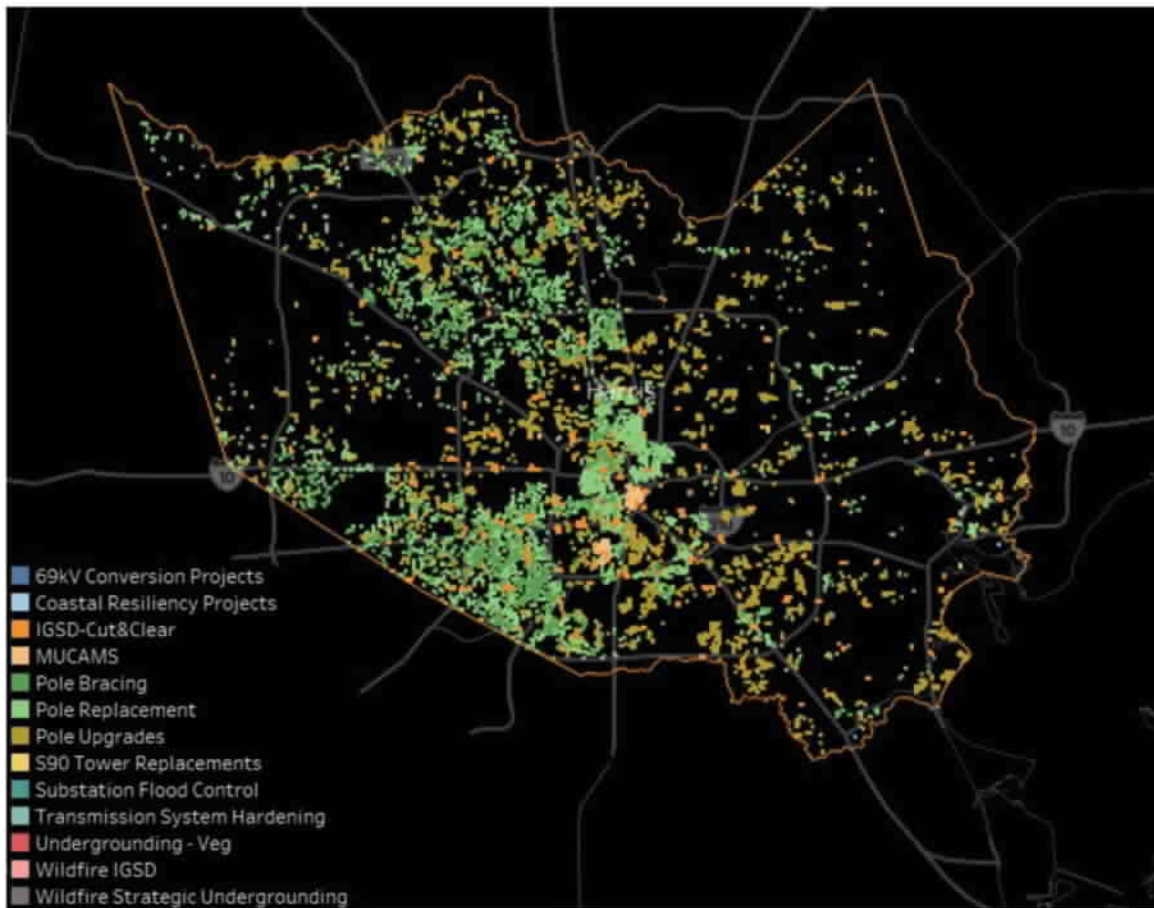
3 **Q. HOW DID THE COMPANY USE THE DAMAGE PREDICTION AND**
4 **OUTAGE DURATION INFORMATION IT ANALYZED FOR EACH OF**
5 **THE TWELVE COUNTIES?**

6 A. The Company used this information to identify specific areas and distribution
7 circuits that: (1) have a higher probability of longer-duration outages; (2) serve
8 critical infrastructure like hospitals, water treatment plants, and first responder
9 facilities; and (3) serve priority locations, as determined by a county's office of
10 emergency management. The identification of specific areas and distribution
11 circuits will inform and assist the Company in determining potential locations to
12 implement Resiliency Measures in the county and informs the Company for
13 purposes of restoration.

14 Using the Harris County damage prediction and outage duration as an
15 example, the Company has identified, on a preliminary basis, potential locations in
16 Harris County to implement Resiliency Measures.⁸ Figure EE-12 below depicts
17 the potential locations in Harris County where a Resiliency Measure may be
18 implemented.

⁸ The number and locations for Resiliency Measures that will actually be implemented in Harris County may differ.

Figure EE-12
Harris County Resiliency Measures Map



Q. HOW DOES THE COMPANY'S APPROACH IN DEVELOPING ITS 2026-2028 T&D SRP DIFFER FROM THE COMPANY'S APPROACH IN DEVELOPING ITS 2025-2027 T&D SRP FILED IN COMMISSION DOCKET NO. 56548?

A. In developing the 2025-2027 T&D SRP that was filed in Commission Docket No. 56548, the Company's analysis of future weather and climate impacts was done at the county level, and the Company relied more on historical trends. Now, the Company's analysis of future weather and climate impacts is done at the polygon

1 and asset level, and the Company relied on both historical trends and
2 forward-looking modeling. The deployment of additional analytical capabilities
3 developed by the Company since the withdrawal of its 2025-2027 T&D SRP in
4 Docket No. 56548 has provided the Company the opportunity to utilize a more
5 granular and risk-based approach in developing the 2026-2028 T&D SRP. This
6 allowed the Company to develop a plan based on specific project locations.

7 **V. AI AND ADVANCES IN TECHNOLOGY**

8 **Q. WHAT ARE THE KINDS OF TECHNOLOGY THAT THE COMPANY IS**
9 **IMPLEMENTING TO IMPROVE RESILIENCY IN ITS SERVICE AREA?**

10 A. The Company has developed and continues to enhance a digital version of its
11 transmission and distribution system (known as “Digital Twin”), including
12 equipment, poles, conductors, and other assets to assess and determine risks and
13 other factors that would affect the resiliency of the Company’s transmission and
14 distribution system. The Digital Twin leverages asset data, operational data,
15 location data (LiDAR) and other inputs to simulate the performance of the
16 Company’s transmission and distribution system under various operating
17 conditions, which in turn allows the Company to assess and determine the optimal
18 mitigations for each Resiliency Event type.

19 **Q. WHAT TECHNOLOGY IS THE COMPANY USING TO ASSIST ITS**
20 **VEGETATION MANAGEMENT EFFORTS?**

21 A. The Company is leveraging LiDAR technology to capture vegetation data,
22 including vegetation located outside of the Company’s ROW or easement to
23 determine vegetation encroachment and tree fall-in risk that could result in outages

1 or damages to distribution and transmission facilities. This encroachment and tree
2 fall-in risk data will assist the Company in determining and prioritizing areas for
3 accelerated vegetation management efforts.

4 **Q. WILL THE COMPANY USE LIDAR TECHNOLOGY IN DETERMINING**
5 **WHERE TO CONDUCT VEGETATION MANAGEMENT AS PART OF**
6 **ITS 2026-2028 T&D SRP?**

7 A. Yes.

8 **Q. DID THE COMPANY CONSIDER OTHER TECHNOLOGIES AND**
9 **VENDORS TO ASSIST IN DEVELOPING THE DIGITAL TWIN?**

10 A. Yes. The Company considered several technologies and vendors to capture and
11 analyze vegetation and asset data to support the development of the Digital Twin.
12 Satellite imagery technology was evaluated, but it did not provide the resolution
13 and accuracy needed for the advanced analytics and simulations. The Company
14 evaluated other LiDAR-based solutions, but it did not have the capability to process
15 and classify the LiDAR data system wide quickly or automatically and provide
16 meaningful results to make timely decisions. Most of the vendors considered by the
17 Company provided services that focused on a specific use case such as vegetation
18 management, instead of a holistic solution that can leverage high-quality LiDAR
19 data for multiple use cases and models. Investing in higher quality data can unlock
20 more future use cases and business value to enhance resiliency and reliability.

1 **Q. PLEASE DESCRIBE THE COMPANY’S COLLABORATION WITH**
2 **NEARA.**

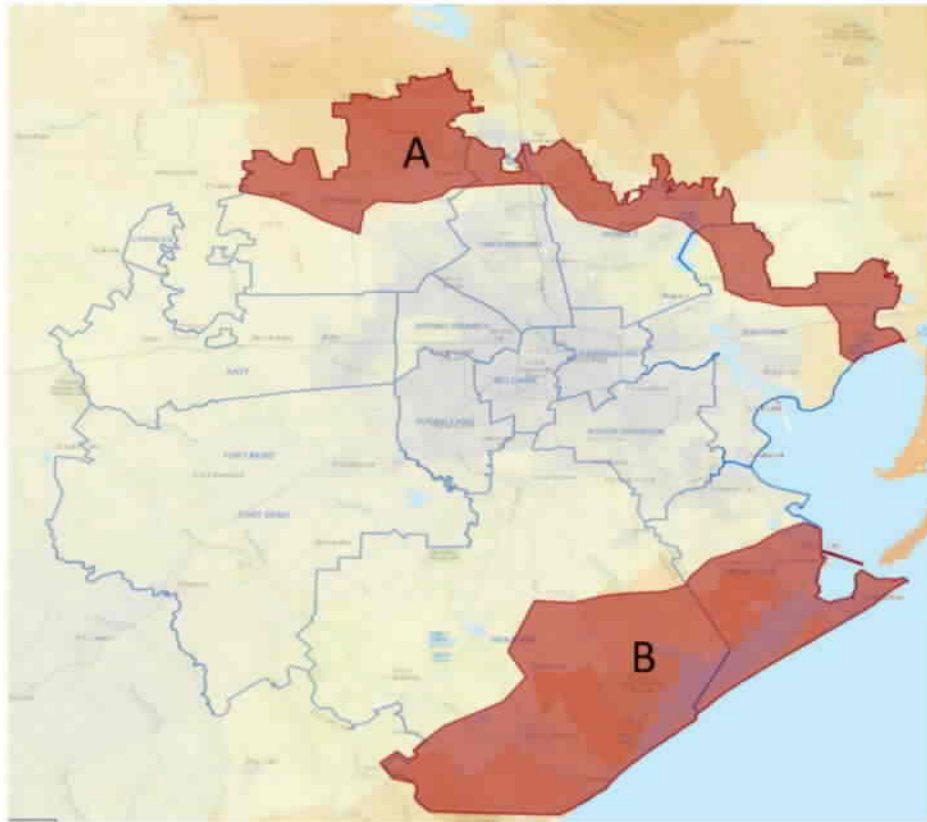
3 A. Neara is a vendor that offers an AI-powered platform for LiDAR based simulations
4 and analytics. The Company will utilize Neara’s AI-powered platforms to quantify
5 various external risk factors that affect the Company’s transmission and distribution
6 system to determine areas where resiliency improvements are needed, such as
7 accelerated vegetation management, upgrades, replacements, undergrounding, and
8 other risk-mitigation projects.

9 **VI. WILDFIRE MITIGATION**

10 **Q. DOES THE GREATER HOUSTON AREA HAVE WILDFIRE RISK?**

11 A. Yes. The Greater Houston area has some wildfire risk, particularly in the northern
12 portion towards Montgomery County and in the southern portion towards Brazoria
13 County, as shown on Figure EE-13. In 2011, there were notable wildfires in parts
14 of Texas, with one wildfire within the Company’s service area (Riley Road
15 wildfire). In 2023, the Company saw heightened wildfire risks in parts of its service
16 territory after we experienced prolonged periods of drought and high heat. In late
17 June of 2024, a wildfire occurred within the Company’s territory in Brazoria
18 County.

Figure EE-13
Wildfire Risk Map



Q. WHY ARE AREAS A & B CONSIDERED TO HAVE WILDFIRE RISK?

A. The Company identified areas A&B as HFRAs after analyzing historical fire information, as well as data from the following sources.

- Texas A&M Texas Wildfire Risk Explorer ("Risk Explorer") – The Risk Explorer is found on TxWRAP. It is the primary mechanism for the Texas A&M Forest Service to deploy wildfire risk information and create awareness about wildfire issues across the state. Risk Explorer analyzes layers of data related to wildfire

1 threat, wildland urban interface, surface fuels, historic wildfire ignitions, fire
2 behavior, and much more.⁹

3 • U.S. Forest Service KBDI – KBDI is an index used to determine forest fire
4 potential.¹⁰ It assesses the risk of fire by representing the net effect of
5 evapotranspiration and precipitation in producing cumulative moisture deficiency
6 in deep duff and upper soil layers.

7 • USDA Forest Service WHP – WHP is an index that quantifies the relative potential
8 for high-intensity wildfire that may be difficult to manage, used as a measure to
9 help prioritize where fuel treatments may be needed. WHP identifies areas with a
10 higher probability of experiencing torching, crowning, and other forms of extreme
11 fire behavior under conducive weather conditions.¹¹

12 **Q. DOES THE COMPANY HAVE A PROCESS FOR MANAGING WILDFIRE**
13 **RISK?**

14 A. Yes. Annex D (Wildfire) to the Company's EOP filed on March 15, 2024 in Docket
15 No. 53385 details the Company's processes for the mitigation of wildfire risk,
16 monitoring of drought conditions, and response to elevated wildfire risk, including
17 PSPS.

18 **Q. DOES THE COMPANY'S 2026-2028 T&D SRP HAVE WILDFIRE**
19 **MITIGATION MEASURES?**

20 A. Yes. The wildfire mitigation Resiliency Measures relate to monitoring, IGSD
21 installation, vegetation management, and inspection.

⁹ Texas Wildfire Risk Explorer

¹⁰ Keetch-Byram Drought Index more information: [TWC | Keetch-Byram Drought Index \(KBDI\) \(tamu.edu\)](https://www.tamu.edu/twri/)

¹¹ [Wildfire Hazard Potential | US Forest Service Research and Development](https://www.fs.fed.us/research/development/wildfire_hazard_potential/)

1 **Q. HOW WILL THE COMPANY MONITOR WILDFIRE RISK?**

2 A. During 2025, the Company will install cameras at high fire risk areas to monitor
3 wildfire risk. These cameras will allow for improved detection of wildfires and
4 alerting of teams to validate and dispatch accordingly. The Company's monitoring
5 of wildfire risk will be supplemented with the use of AI and predictive analytics
6 services provided by Technosylva, a leader in wildfire science and technology.

7 **Q. WHAT OTHER STRATEGIES WILL THE COMPANY IMPLEMENT TO**
8 **MONITOR AND MITIGATE THE IMPACT OF WILDFIRES IN ITS**
9 **SERVICE AREA?**

10 A. In addition to the installation of monitoring cameras, the Company will implement
11 other strategies to mitigate the risk and impact of a wildfire. The Company will
12 install IGSDs at select locations on distribution circuits to allow for limiting the
13 number of impacted customers by sectionalizing at risk circuit sections in the event
14 the Company institutes a public safety power shutoff. Wildfire related IGSDs are
15 developed in a selection process separate from IGSDs deployed for load shed due
16 to the differences in primary use cases. Load shed IGSD locations are selected based
17 on their proximity to critical loads and the ability to maintain service to critical load
18 while reducing load on the remainder of the feeder. Additionally, the Company will
19 re-configure the relay settings on select distribution circuits where digital relays are
20 installed and underground certain portions of overhead distribution circuits to
21 reduce the risk of the Company's equipment acting as an ignition source. The
22 Company will perform greater clearing of vegetation and increase the size of the

1 ROW within high wildfire risk areas. Finally, the Company will conduct additional
2 inspections in high wildfire risk areas.

3 In addition to these operational strategies, the Company will utilize
4 advanced analytics to monitor and forecast potential fire risks to warn customers
5 and the general public and, in the event of a wildfire attributable to the Company's
6 equipment, leverage the analytics with our real-time risk analysis to determine most
7 likely paths where the wildfire may spread.

8 **VII. CONCLUSION**

9 **Q. IS IMPLEMENTATION OF THE RESILIENCY MEASURES IN THE**
10 **COMPANY'S 2026-2028 T&D SRP IN THE PUBLIC INTEREST?**

11 A. Yes. The Company's 2026-2028 T&D SRP mitigates the impact of the Resiliency
12 Events that pose the highest risk to the Greater Houston area and the Company's
13 transmission and distribution system – i.e., extreme wind events, flooding and
14 extreme water events, and extreme freeze and drought events – and is anticipated
15 to save 1,255 CML.

16 **Q. SHOULD THE COMMISSION APPROVE THE COMPANY'S 2026-2028**
17 **T&D SRP?**

18 A. Yes.

19 **Q. DOES THIS CONCLUDE YOUR DIRECT TESTIMONY?**

20 A. Yes.

STATE OF Texas §
COUNTY OF Harris §

AFFIDAVIT OF ERIC D. EASTON

BEFORE ME, the undersigned authority, on this day personally appeared ERIC D. EASTON who having been placed under oath by me did depose as follows:

1. "My name is ERIC D. EASTON. I am of sound mind and capable of making this affidavit. The facts stated herein are true and correct based upon my personal knowledge.
2. I have prepared the foregoing Direct Testimony and the information contained in this document is true and correct to the best of my knowledge."

Further affiant sayeth not.


ERIC D. EASTON

SUBSCRIBED AND SWORN TO BEFORE ME on this 8th day of January,
2025.


Notary Public in and for the State of Texas

My commission expires: 3/16/2025

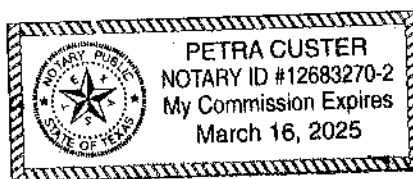


Exhibit EE-1: Glossary of Acronyms

2026-2028 T&D SRP or SRP	The Company's 2026-2028 Transmission and Distribution System Resiliency Plan
AI	Artificial intelligence
Company	CenterPoint Energy Houston Electric, LLC
Commission	Public Utility Commission of Texas
EOP	Emergency Operations Plan
FEMA	Federal Emergency Management Agency
IGSD	Intelligent grid switching device
Guidehouse	Guidehouse Inc.
HFRA	High-Fire Risk Areas
KBDI	Keetch-Byram Drought Index
LiDAR	Light detection and ranging
NOAA	National Oceanic and Atmospheric Administration
PSPS	Public Safety Power Shutoff
Resiliency Event	An event involving extreme weather conditions, wildfires, cybersecurity threats, or physical security threats that poses a material risk to the safe and reliable operation of the Company's transmission and distribution systems
Resiliency Measure	A measure designed to prevent, withstand, mitigate, or more promptly recover from the risks posed to the Company's transmission and distribution system by a Resiliency Event
Risk Explorer	The Texas A&M Wildfire Risk Explorer
ROW	Right of Way
Technosylva	Technosylva Inc.
TxWRAP	Texas Wildfire Risk Assessment Portal
USDA	United States Department of Agriculture
WHP	Wildfire Hazard Potential

This page was
intentionally left
blank.

EXHIBIT 7

THE DIRECT TESTIMONY OF
COMPANY WITNESS
MR. RONALD W. BAHR

This page was
intentionally left
blank.

DOCKET NO. 57579

**APPLICATION OF CENTERPOINT
ENERGY HOUSTON ELECTRIC, LLC
FOR APPROVAL OF ITS 2026-2028
TRANSMISSION AND DISTRIBUTION
SYSTEM RESILIENCY PLAN**

§
§
§
§
§
§
§

**PUBLIC UTILITY
COMMISSION OF TEXAS**

DIRECT TESTIMONY OF

RONALD W. BAHR

ON BEHALF OF

CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC

JANUARY 2025

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	ES-1
I. INTRODUCTION.....	1
II. OVERVIEW OF TESTIMONY	3
III. OVERVIEW OF IT AND COMMUNICATIONS	4
A. IT SERVICES	6
B. OPERATIONAL TECHNOLOGY SERVICES.....	7
IV. DEVELOPMENT OF THE COMPANY’S SRP	8
V. IT AND COMMUNICATIONS RESILIENCY MEASURES	12
VI. CONCLUSION	14

TABLE OF EXHIBITS

<u>Exhibits</u>	<u>Description</u>
Exhibit RB-1	Glossary of Acronyms

TABLE OF FIGURES

Figure RB-1 - Technology-Related Resiliency Measures Estimated Costs and CMI (in millions)	2
Figure RB-2 - Operations Witnesses and Corresponding Testimony Subjects	3
Figure RB-3 - Resiliency Events Impacting Technology 2020 - 2024.....	11
Figure RB-4 - Technology-Related Resiliency Measures Estimated Costs and CMI (in millions)	13

EXECUTIVE SUMMARY

The Company's 2026-2028 T&D SRP aims to strengthen the Company's transmission and distribution system to maintain reliable service for its customers during Resiliency Events. The SRP contains thirty-nine (39) Resiliency Measures. As the Vice President of the Office of the Chief Information Officer, I am responsible for four (4) standalone Information Technology ("IT") Resiliency Measures that are related to IT and communications.

In addition to four technology-related Resiliency Measures, I co-sponsor and speak to the operational technology aspects of the five (5) IT to Support Operations Resiliency Measures (as described in the Company's SRP) sponsored by Mr. Pryor, Mr. Easton and Mr. Mercado: IGSD Installation and Loadshed IGSD (Pryor), Wildfire IGSD and Advanced Aerial Imagery Platform/Digital Twin (Easton) and Substation Flood Control (Mercado). Collectively, I refer to the five IT to Support Operations Resiliency Measures and the four IT Resiliency Measures as the "IT and Communications Resiliency Measures". These IT and Communications Resiliency Measures modernize the Company's IT, communications infrastructure and operations infrastructure, thus enabling Company personnel to better respond to Resiliency Events, which are typically extreme weather (i.e., wind-related) events, that occur in the Greater Houston area and affect the Company's transmission and distribution system. As summarized in the table below, the four IT Resiliency Measures will cumulatively cost approximately \$88.2 million in capital costs and \$1.3 million in incremental O&M expense from 2026-2028 (the cost of the five operations resiliency measures is discussed in the testimony of each Resiliency Measure's sponsor).

Figure RB-1

**Technology-Related Resiliency Measures Estimated Costs and CMI
(in millions)**

Resiliency Measure	Resiliency Event to be Mitigated	T&D SRP Rule Category	Estimated Capital Costs 2026-2028 (millions)	Estimated O&M Costs 2026-2028 (millions)	Estimated Total Costs 2026-2028 (millions)	Estimated CMI Savings (millions)
Spectrum Acquisition (RM-28)	All	Information Technology	\$42.0	None	\$42.0	N/A*
Data Center Modernization (RM-29)	All	Information Technology	\$12.7	\$1.3	\$13.9	N/A*
Voice & Mobile Data Radio System (RM-36)	All	Information Technology	\$20.9	None	\$20.9	N/A*
Backhaul Microwave Communication (RM-37)	All	Information Technology	\$12.7	None	\$12.7	N/A*
Total			\$88.2	\$1.3	\$89.5	
*Note: Please see Section 5 of Exhibit ELS-2 for a qualitative benefit analysis of this Resiliency Measure						

I. INTRODUCTION

Q. PLEASE STATE YOUR NAME AND CURRENT POSITION.

A. My name is Ronald W. Bahr, and I am employed by CNP as Vice President, Office of the Chief Information Officer.

Q. PLEASE SUMMARIZE YOUR EDUCATIONAL AND WORK EXPERIENCE.

A. I earned my Bachelor of Science degree in Accounting from Eastern Illinois University and a Master of Business Administration degree from Bowling Green State University. I have over 40 years of energy industry experience and have held IT leadership roles for over 22 years, for both non-regulated and regulated companies. In 2017, I joined CNP as Vice President of IT for CNP's natural gas marketing subsidiary. My role as Vice President included oversight of all technology functions. In 2020, I accepted a position as Vice President of IT for all CNP subsidiaries, including the Company. During my time with CNP, I have led and overseen major enterprise-wide IT projects for CNP and its subsidiaries including: the Energy Trading Risk Management System, Network Modernization Project, Customer Enterprise Integration Project, and currently the Agile Platform Operating model.

Q. DO YOU HOLD ANY PROFESSIONAL LICENSES OR CERTIFICATES?

A. I hold the following certifications: Certified Financial Management and Certified Management Accountant, both sponsored by the Institute of Management Accountants. I also hold a Professional in Human Resources certification through the Society of Human Resources.

1 **Q. WHAT ARE YOUR CURRENT RESPONSIBILITIES AT CNP?**

2 A. As Vice President, Office of the Chief Information Officer, I am a senior leader in
3 the IT organization and responsible for strategy, financial management, project
4 management, and vendor management. Additionally, my responsibilities include
5 agile operations, service delivery, IT asset management, regulatory support and
6 technology governance. I also lead the development and execution of IT strategies
7 and work with CNP business leaders across the CNP enterprise to support the
8 execution and achievement of their objectives through IT.

9 The IT organization has approximately 510 employees that are responsible
10 for overseeing and managing IT for CNP and its utility subsidiaries like the
11 Company. Additionally, the IT organization includes approximately 845 external
12 contractors that provide cybersecurity-related services to CNP or the Company.

13 **Q. ON WHOSE BEHALF ARE YOU TESTIFYING IN THIS PROCEEDING?**

14 A. I am testifying on behalf of the Company.

15 **Q. HAVE YOU TESTIFIED PREVIOUSLY?**

16 A. Yes. I have provided testimony to the Indiana Utility Regulatory Commission in
17 Cause No. 45990 as well as to the Public Utility Commission of Texas in Docket
18 No. 56211 as well as Docket No 56548, the Company's prior System Resiliency
19 Plan, which this SRP replaces.

20 **Q. WHAT EXHIBITS HAVE YOU INCLUDED WITH YOUR TESTIMONY?**

21 A. I have included the one exhibit listed in the Table of Contents as part of my
22 testimony.

Q. DO YOU CO-SPONSOR THE COMPANY'S 2026-2028 T&D SRP?

A. Yes, I co-sponsor the Company's 2026-2028 T&D SRP, which is included as an attachment to the Company's application as Exhibit 1. I also co-sponsor the technology aspects of the IGSD Installation, Loadshed IGSD, Wildfire IGSD, Advanced Aerial Imagery Platform/Digital Twin, and Substation Flood Control Resiliency Measures with Mr. Pryor, Mr. Mercado and Mr. Easton. I sponsor the Spectrum Acquisition, Data Center Modernization, Backhaul Microwave Communication, and Voice & Mobile Data Radio System. Mr. Christopher Ford sponsors the three additional cybersecurity Resiliency Measures related to technology.

Q. WAS YOUR TESTIMONY PREPARED BY YOU OR UNDER YOUR DIRECTION AND CONTROL?

A. Yes.

II. OVERVIEW OF TESTIMONY

Q. WHAT IS THE PURPOSE OF YOUR TESTIMONY AND HOW IS IT ORGANIZED?

A. There are six operations witnesses – Mr. Deryl Tumlinson, Mr. David Mercado, Mr. Randy Pryor, Mr. Eric Easton, Mr. Christopher Ford, and me – addressing the following subjects.

Figure RB-2

Operations Witnesses and Corresponding Testimony Subjects

Witness	Subject of Testimony
Mr. Deryl Tumlinson	Overhead Distribution System

Witness	Subject of Testimony
Mr. David Mercado	Transmission System and Substations
Mr. Randy Pryor	Strategic Undergrounding and Vegetation Management
Mr. Eric Easton	Damage Prediction, Use of Advanced Analytics, and Wildfire Mitigation
Mr. Ronald Bahr	Information Technology
Mr. Christopher Ford	Cybersecurity Operations

1

2 My testimony provides a general overview of the IT and communications
3 infrastructure needed and used by electric utilities, like the Company, to conduct
4 the day-to-day activities necessary to provide safe and reliable electric delivery
5 service to its customers. With this context in mind, my testimony describes the
6 importance and functionality of the IT and Communications Resiliency Measures
7 in the Company's 2026-2028 T&D SRP and why the Company considers these
8 measures to be appropriate for inclusion in the SRP.

9

III. OVERVIEW OF IT AND COMMUNICATIONS

10 **Q. PLEASE DESCRIBE THE ROLE OF IT AND COMMUNICATIONS IN**
11 **THE OPERATIONS OF A UTILITY.**

12 A. IT and communications are critical to operate an electric utility safely, reliably and
13 efficiently. Increasingly, as the grid becomes smarter, technology and
14 communication systems enable the Company to respond quickly to both safety risks
15 and ever-evolving threats. Through various software applications, employees can
16 access information about facility locations, including the locations of electric
17 transmission and distribution lines, substations, electric poles, and other critical

1 data, that allow the Company respond quickly and efficiently during both normal
2 and emergency situations. IT systems include software (e.g., operating systems,
3 applications, programs, databases), computer networks, and hardware (e.g.,
4 computers, servers, network devices) that are integral to providing critical data to
5 both field personnel workers performing construction and maintenance, and
6 workers performing back-office support functions, such as accounting.
7 Additionally, technology systems utilities use must be securely connected to people
8 and businesses outside the utility, allowing the Company to accomplish essential
9 tasks such as receiving and remitting payments, ordering supplies, and providing
10 customers with necessary information and updates.

11 **Q. PLEASE GENERALLY DESCRIBE THE TECHNOLOGY**
12 **INFRASTRUCTURE NEEDED FOR THE COMPANY TO PROVIDE SAFE**
13 **AND RELIABLE SERVICE TO THE COMPANY'S CUSTOMERS.**

14 A. At a general level, the Company needs technology infrastructure (i.e., equipment
15 and software) that enables the Company to:

- 16 ■ securely monitor, operate, and control the Company's transmission system and
17 substations in real-time;
- 18 ■ securely communicate and coordinate with ERCOT regarding operation of the
19 Company's transmission system in real-time;
- 20 ■ securely monitor, operate, and control the Company's distribution system in
21 real-time;
- 22 ■ efficiently manage and dispatch personnel for maintenance, repairs, and outage
23 restoration;

- 1 ▪ efficiently communicate with all field personnel, including third-party
- 2 contractors, and customers;
- 3 ▪ process ERCOT retail market transactions and securely communicate retail
- 4 market data to ERCOT and REPs; and
- 5 ▪ provide necessary back-office services, including back-office services in
- 6 support of the tasks listed above.

7 **Q. PLEASE GENERALLY DESCRIBE THE RELATIONSHIP BETWEEN IT,**
8 **OPERATIONAL TECHNOLOGY, AND CYBERSECURITY.**

9 A. IT is a broad term that refers to any equipment or systems used in the storing,
10 controlling, retrieving, or transmitting of information. CenterPoint Houston uses
11 Operational Technology (“OT”) to refer to IT that manages the assets used to
12 directly operate or facilitate the operation of an electric utility’s transmission and
13 distribution system and equipment. Cybersecurity manages and protects against
14 cyber risks that impact both IT and OT. For a more detailed discussion of CNP’s
15 cybersecurity concerns and practices, see the testimony of Company witness Mr.
16 Chris Ford. The Company’s SRP (and the remainder of my testimony) use the term
17 IT to categorize IT functions that do not involve OT unless otherwise noted.

18 **A. IT SERVICES**

19 **Q. IN THE CONTEXT OF THE IT RESILIENCY MEASURES DESCRIBED**
20 **IN YOUR TESTIMONY, WHAT IS IT?**

21 A. IT is information technology including, but not limited to activities, standards,
22 policies, procedures, practices, hardware or software, services, and supporting
23 infrastructure systems to support metering, billing, customer service, work

1 management, data analysis, and interrelated enterprise systems that manage, store,
2 retrieve, deliver, or protect information or associated IT assets for both on-premise
3 and cloud-based platforms to manage, monitor, protect, or control information and
4 associated technology assets to operate, or to facilitate the operation of, an electric
5 utility's transmission and distribution system. This includes programmable systems
6 or devices that interact with the physical environment (or manage devices that
7 interact with the physical environment through secure communications networks)
8 to detect or cause a direct change through the monitoring and/or control of devices,
9 processes, and events. Such systems may include industrial control systems,
10 building management systems, fire control systems, and physical access control
11 mechanisms all of which have a critical role in ensuring reliable and consistent
12 Company functions.

13 **B. OPERATIONAL TECHNOLOGY SERVICES**

14 **Q. IN THE CONTEXT OF THE IT AND COMMUNICATIONS RESILIENCY**
15 **MEASURES DESCRIBED IN YOUR TESTIMONY, WHAT IS OT?**

16 **A.** OT is a type of IT that includes programmable systems or devices that interact with
17 the physical environment (or manage devices that interact with the physical
18 environment through secure communications networks). These systems or devices
19 detect or cause a direct change the through monitoring or control of devices,
20 processes, and events including industrial control systems, building management
21 systems, fire control systems, and physical access control mechanisms.

IV. DEVELOPMENT OF THE COMPANY'S SRP

Q. WHAT IS RESILIENCY?

A. For purposes of this proceeding, the Resiliency Rule¹ defines resiliency. Based on the definitions of "Resiliency Event" and "Resiliency Measure," resiliency is the ability "to prevent, withstand, mitigate, or promptly recover from the risks posed" by events "involving extreme weather conditions, wildfires, cybersecurity threats, or physical security threats that pose[] a material risk to the safe and reliable operation" of the Company's transmission and distribution system.² Colloquially speaking, resiliency is the ability of a transmission and distribution system to "take a punch."

Q. IN THE CONTEXT OF TECHNOLOGY, WHAT IS RESILIENCY?

A. In the context of technology, resiliency refers to the ability of a system or organization to withstand and recover from unexpected events, such as cyberattacks, weather events, natural disasters, or system failures. Resilient technology is therefore critical in maintaining uninterrupted services for customers and providing service to customers during normal operations, peak times, or during a resiliency event.

Q. HAS THE COMPANY PREVIOUSLY INVESTED IN AND IMPLEMENTED TECHNOLOGY RESILIENCY PROJECTS?

A. Yes. The Company has extensive experience investing in and implementing resiliency projects. We are constantly needing to invest in more resilient infrastructure, communications equipment, network solutions, applications, and

¹ 16 Texas Administrative Code ("TAC") § 25.62.

² *Id.*

1 other technology necessary to operate and provide transmission and distribution
2 service to our customers as well as respond to and recover quickly from resiliency
3 events. This is not something new, we have been doing “resiliency” for a long time.
4 For example, we have moved critical applications to the cloud, installed 539 miles
5 of fiber, and implemented new cybersecurity solutions to address changing threats
6 and stay in front of evolving vulnerabilities.

7 **Q. WILL THE COMPANY CONTINUE TO INVEST IN TECHNOLOGY-**
8 **RELATED RESILIENCY PROJECTS EVEN IN THE ABSENCE OF H.B.**
9 **2555, WHICH ENABLED TRANSMISSION AND DISTRIBUTION**
10 **UTILITIES TO FILE AND SEEK COMMISSION APPROVAL OF A SRP?**

11 A. Yes. The technological landscape is constantly changing in response to
12 technological advancement in equipment and software (and as both equipment and
13 software reach the end of their useful lives). Additionally, the technology landscape
14 must change in response to evolving physical security and cybersecurity risks.
15 Anticipating and repelling these attacks before they gain access and can control the
16 Company’s assets will require continuous deployment of technology solutions to
17 be able to provide and improve service to our customers. Thus, the Company will
18 need to continue investing in and implementing technology resiliency projects.

19 **Q. WHAT IS A RESILIENCY EVENT?**

20 A. The definition of “Resiliency Event” used in the Company’s SRP is substantively
21 identical to the definition used by the Commission: “an event involving extreme
22 weather conditions, wildfires, cybersecurity threats, or physical security threats that

1 poses a material risk to the safe and reliable operation of [the Company's]
2 transmission and distribution systems.”³

3 **Q. IN THE CONTEXT OF TECHNOLOGY, WHAT IS A RESILIENCY**
4 **EVENT?**

5 A. In the context of technology, a resiliency event refers to a challenging event that
6 can compromise the technology stack (i.e., a combination of technologies used to
7 develop and run an application) of an organization. Such events can include
8 cyberattacks, natural disasters, or other risks to the technology environment. If one
9 such attack were successful, it could compromise communications between CNP
10 and its other operating entities, technicians in the field, and its customers, as well
11 as endanger the Company's ability to provide, detect and monitor service delivery
12 to its customers.

13 **Q. WHAT ARE THE TYPES OF RESILIENCY EVENTS THAT ELECTRIC**
14 **UTILITIES TYPICALLY EXPERIENCE THAT CAN AFFECT**
15 **TECHNOLOGY?**

16 A. Weather events that include extreme wind, water, temperatures, or fire,
17 construction impacting network fiber cables, vendor outages, and cybersecurity
18 attacks are types of resiliency events that can affect technology. Please refer to the
19 testimony of Company witnesses Mr. Mercado, Mr. Tumlinson, Mr. Pryor, Mr.
20 Tutunjian and Mr. Easton for Resiliency Events related to weather.

³ 16 TAC § 25.62.

1 **Q. PLEASE SUMMARIZE RESILIENCY EVENTS THAT THE COMPANY**
 2 **HAS EXPERIENCED THAT IMPACTED THE COMPANY'S**
 3 **TECHNOLOGY INFRASTRUCTURE AND/OR SOFTWARE.**

4 A. The following table summarizes the IT-related Resiliency Events experienced by
 5 the Company in the past five years:

6 **Figure RB-3**

7 **Resiliency Events Impacting Technology 2020 - 2024**
 8

Year	Resiliency Event(s) Impacting Technology
2020	Hurricane Laura
2021	Tropical Storm Nicholas, Winter Storm Uri; Akamai Internet Outage
2023	January Storm, June Storm; AT&T/Comcast Fiber Cuts
2024	Derecho, May 28th Storms, Hurricane Beryl

9 **Q. DID THE COMPANY DEVELOP ITS SRP WITH THE INTENT TO**
 10 **MITIGATE THE IMPACT OF CERTAIN RESILIENCY EVENTS,**
 11 **INCLUDING RESILIENCY EVENTS THAT MAY IMPACT THE**
 12 **COMPANY'S TECHNOLOGY INFRASTRUCTURE AND/OR**
 13 **SOFTWARE?**

14 A. Yes. The IT and Communications Resiliency Measures in the Company's SRP are
 15 intended to enhance the resiliency of the Company's technology infrastructure to
 16 withstand and limit interruptions of service during certain Resiliency Events.

17 **Q. HOW DID THE COMPANY DETERMINE THE IT AND**
 18 **COMMUNICATIONS RESILIENCY MEASURES THAT IT SEEKS TO**
 19 **IMPLEMENT AS PART OF ITS SRP?**

1 A. The resiliency strategy focuses on investments to improve, modernize, or maintain
 2 technology operations and infrastructure to ensure secure and reliable technological
 3 systems during Resiliency Events. In determining which IT and Communications
 4 Resiliency Measures to implement as part of its SRP, the Company selected
 5 complementary measures in alignment with operational resiliency measures,
 6 referenced previous resiliency measures to supplement and expand on resiliency
 7 for key operations and infrastructure related to resiliency, and addressed the known
 8 threats to cybersecurity.

9 **Q. IS THE COMPANY'S METHODOLOGY IN DETERMINING WHICH IT**
 10 **AND COMMUNICATIONS RESILIENCY MEASURES TO IMPLEMENT**
 11 **AS PART OF ITS SRP CONSISTENT WITH THE COMPANY'S**
 12 **APPROACH IN INVESTING IN AND IMPLEMENTING PREVIOUS**
 13 **TECHNOLOGY PROJECTS?**

14 A. Yes.

15 **V. IT AND COMMUNICATIONS RESILIENCY MEASURES**

16 **Q. PLEASE IDENTIFY THE TECHNOLOGY PORTIONS OF THE SRP**
 17 **THAT YOU SUPPORT.**

18 A. I sponsor the following IT Resiliency Measures:

- 19 1. Spectrum Acquisition;
- 20 2. Data Center Modernization;
- 21 3. Voice & Mobile Data Radio System; and
- 22 4. Backhaul Microwave Communication

As explained above, I also co-sponsor, along with Mr. Pryor, Mr. Mercado and Mr. Easton, the following grid modernization, flood mitigation, and the technology elements necessary to support the IT to Support Operations Resiliency Measures:

1. IGSD Installation (Pryor)
2. Loadshed IGSD (Pryor)
3. Wildfire IGSD (Easton)
4. Advanced Aerial Imagery Platform/Digital Twin (Easton)
5. Substation Flood Control (Mercado)

Descriptions of each measure are contained in the CenterPoint's SRP. The table below describes the estimated costs associated with each of the four IT and communications infrastructure-related Resiliency Measures.

Figure RB-4

**Technology-Related Resiliency Measures Estimated Costs and CMI
(in millions)**

Resiliency Measure	Resiliency Event to be Mitigated	T&D SRP Rule Category	Estimated Capital Costs 2026-2028 (millions)	Estimated O&M Costs 2026-2028 (millions)	Estimated Total Costs 2026-2028 (millions)	Estimated CMI Savings (millions)
Spectrum Acquisition (RM-28)	All	Information Technology	\$42.0	None	\$42.0	N/A*
Data Center Modernization (RM-29)	All	Information Technology	\$12.7	\$1.3	\$13.9	N/A*
Voice & Mobile Data Radio System (RM-36)	All	Information Technology	\$20.9	None	\$20.9	N/A*
Backhaul Microwave Communication (RM-37)	All	Information Technology	\$12.7	None	\$12.7	N/A*
Total			\$88.2	\$1.3	\$89.5	

*Note: Please see Section 5 of Exhibit ELS-2 for a qualitative benefit analysis of this Resiliency Measure.

1 **Q. ARE ANY OF THE IT AND COMMUNICATIONS RESILIENCY**
2 **MEASURES**

3 **COORDINATED EFFORTS WITH FEDERAL STATE, OR LOCAL**
4 **GOVERNMENT PROGRAMS AND FUNDING OPPORTUNITIES?**

5 A. No, although CenterPoint has pursued opportunities to obtain available federal,
6 state, and local funding as described by Mr. Brownell in his testimony.

7 **VI. CONCLUSION**

8 **Q. IS IMPLEMENTING THE RESILIENCY MEASURES IN YOUR**
9 **TESTIMONY IN THE PUBLIC INTEREST?**

10 A. Yes.

11 **Q. SHOULD THE COMMISSION APPROVE THE COMPANY'S 2026-2028**
12 **T&D SRP?**

13 A. Yes.

14 **Q. DOES THIS CONCLUDE YOUR DIRECT TESTIMONY?**

15 A. Yes

STATE OF Texas §
COUNTY OF Harris §

AFFIDAVIT OF RONALD W. BAHR

BEFORE ME, the undersigned authority, on this day personally appeared RONALD W. BAHR who having been placed under oath by me did depose as follows:

1. "My name is RONALD W. BAHR. I am of sound mind and capable of making this affidavit. The facts stated herein are true and correct based upon my personal knowledge.
2. I have prepared the foregoing Direct Testimony and the information contained in this document is true and correct to the best of my knowledge."

Further affiant sayeth not.

Ronald W Bahr
RONALD W. BAHR

SUBSCRIBED AND SWORN TO BEFORE ME on this 8th day of January,
2025.

Petra Custer
Notary Public in and for the State of Texas

My commission expires: 3/14/2025

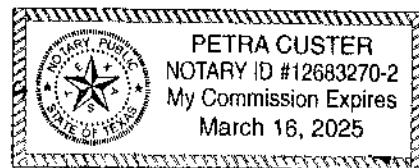


Exhibit RB-1: Glossary of Acronyms

2026-2028 T&D SRP or SRP	The Company's 2026-2028 Transmission and Distribution System Resiliency Plan
CIP	Critical Infrastructure Protection
Company	CenterPoint Energy Houston Electric, LLC
CNP	CenterPoint Energy, Inc.
Commission	Public Utility Commission of Texas
DOE	Department of Energy
ERCOT	Electric Reliability Council of Texas
Greater Houston	The area in and about the City of Houston where Company's facilities or customers are located.
IGSD	Intelligent Grid Switching Device
IT	Information Technology
O&M	Operations and maintenance
OT	Operational Technology
REP	Retail Electric Provider
Resiliency Event	An event involving extreme weather conditions, wildfires, cybersecurity threats, or physical security threats that poses a material risk to the safe and reliable operation of the Company's transmission and distribution systems
Resiliency Measure	A measure designed to prevent, withstand, mitigate, or more promptly recover from the risks posed to the Company's transmission and distribution system by a Resiliency Event
T&D SRP Rule	16 Tex. Admin. Code § 25.62

This page was
intentionally left
blank.

EXHIBIT 8

THE DIRECT TESTIMONY OF COMPANY WITNESS MR. CHRISTOPHER FORD

This page was
intentionally left
blank.

DOCKET NO. 57579

APPLICATION OF CENTERPOINT	§	
ENERGY HOUSTON ELECTRIC,	§	PUBLIC UTILITY
LLC FOR APPROVAL OF ITS 2026-	§	
2028 TRANSMISSION AND	§	COMMISSION OF TEXAS
DISTRIBUTION SYSTEM	§	
RESILIENCY PLAN	§	

DIRECT TESTIMONY OF

CHRISTOPHER W. FORD

ON BEHALF OF

CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC

JANUARY 2025

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	ES-1
I. INTRODUCTION.....	1
II. OVERVIEW OF TESTIMONY	2
III. OVERVIEW OF CYBERSECURITY	3
IV. CYBERSECURITY-RELATED RESILIENCY MEASURES	12
V. CONCLUSION	14

TABLE OF EXHIBITS

<u>Exhibits</u>	<u>Description</u>
Exhibit CF-1	Glossary of Acronyms

TABLE OF FIGURES

Figure CF-1 - Cybersecurity-Related Resiliency Measures Estimated Costs and CMI (in millions)	1
Figure CF-2 - Operations Witnesses and Corresponding Testimony Subjects.....	3
Figure CF-3 - NERC CIP Reliability Standards	9
Figure CF-4 - Cybersecurity-Related Resiliency Measures Estimated Costs and CMI (in millions)	13

EXECUTIVE SUMMARY

The Company's 2026-2028 T&D SRP aims to strengthen the Company's transmission and distribution system to maintain reliable service for its customers during Resiliency Events. The SRP contains thirty-nine (39) Resiliency Measures. As the Director of IT Security for CNP, I am responsible for three (3) Resiliency Measures related to the Company's cybersecurity:

- IT/OT Cybersecurity Monitoring;
- Network Security and Vulnerability Management; and
- Cloud Security, Product Security, and Risk Management.

These three Resiliency Measures are intended to mitigate the impact of cyber attacks and the impact of other resiliency events. As summarized in the table below, the three cybersecurity Resiliency Measures will cost approximately \$24.9 million in capital costs and \$12.2 million in incremental O&M expenses from 2026-2028.

Figure CF-1

**Cybersecurity-Related Resiliency Measures Estimated Costs and CMI
(in millions)**

Resiliency Measure	Resiliency Event to be Mitigated	T&D SRP Rule Category	Estimated Capital Costs 2026-2028	Estimated O&M Costs 2026-2028	Estimated Total Costs 2026-2028	Estimated CMI Savings
Network Security & Vulnerability Management (RM-30)	Cybersecurity event	Cybersecurity	\$7.5	\$2.0	\$9.5	N/A*
IT/OT Cybersecurity Monitoring (RM-31)	Cybersecurity event	Cybersecurity Modernization	\$13.4	\$4.2	\$17.6	N/A*
Cloud Security, Product Security & Risk Management	Cybersecurity event	Cybersecurity	\$4.0	\$6.0	\$10.0	N/A*

Resiliency Measure	Resiliency Event to be Mitigated	T&D SRP Rule Category	Estimated Capital Costs 2026-2028	Estimated O&M Costs 2026-2028	Estimated Total Costs 2026-2028	Estimated CMI Savings
(RM-32)						
Total			\$24.9	\$12.2	\$37.1	
*Note: Please see Section 5 of Exhibit ELS-2 for a qualitative benefit analysis of this Resiliency Measure.						

- 1 The Company will use its well-established processes to ensure the Company has
- 2 sufficient personnel and material to implement the cybersecurity Resiliency
- 3 Measures, and the Company can and will augment and increase personnel, typically
- 4 through the staffing of additional external contractors, if needed.

I. INTRODUCTION

Q. PLEASE STATE YOUR NAME AND CURRENT POSITION.

A. My name is Christopher W. Ford, and I am employed by CNP as Director, IT Security.

Q. PLEASE SUMMARIZE YOUR EDUCATIONAL AND WORK EXPERIENCE.

A. I earned my Bachelor of Science degree in Computer Science from Southeastern Louisiana University, and a Master of Business Administration degree with a concentration in Information Systems from Louisiana State University. I have over 20 years of IT and cybersecurity experience. Prior to joining CNP in May 2018, I was the Cyber Security Operations Manager at Chicago Bridge & Iron Company, an engineering, procurement, and construction company that specializes in the design and construction of storage facilities, tanks, and terminals. My roles included overseeing global IT infrastructure and networks, enterprise architecture, and cybersecurity operations. I have extensive experience in IT network operations, IT disaster recovery, application development and management, and cybersecurity incident response.

Q. DO YOU HOLD ANY PROFESSIONAL LICENSES OR CERTIFICATES?

A. Yes. I am a Certified Information Systems Security Professional and hold a certificate from the Information Technology Infrastructure Library V3 Foundation.

Q. WHAT ARE YOUR CURRENT RESPONSIBILITIES FOR CNP?

A. As Director, IT Security for CNP, I oversee:

- management of CNP's Cybersecurity Operations Center, which monitors, detects, assesses, and responds to cybersecurity-related issues on a 24/7/365 basis;
- threat and vulnerability management;
- software patch management;

- 1 ▪ penetration testing;
- 2 ▪ cybersecurity incident response; and
- 3 ▪ threat intelligence and collaboration with government entities.

4 The cybersecurity organization has approximately 44 employees that are
5 responsible for cybersecurity oversight for CNP. This includes providing cybersecurity
6 services to all of CNP and its operating utilities. Additionally, my organization manages
7 numerous external contractors that provide cybersecurity-related services to CNP or the
8 Company.

9 **Q. ON WHOSE BEHALF ARE YOU TESTIFYING IN THIS PROCEEDING?**

10 A. I am testifying on behalf of the Company.

11 **Q. HAVE YOU TESTIFIED PREVIOUSLY?**

12 A. No.

13 **Q. WHAT EXHIBITS HAVE YOU INCLUDED WITH YOUR TESTIMONY?**

14 A. I have included the one exhibit listed in the Table of Contents as part of my testimony.

15 **Q. WAS YOUR TESTIMONY PREPARED BY YOU OR BY OTHERS WORKING**
16 **UNDER YOUR DIRECTION AND CONTROL?**

17 A. Yes.

18 **II. OVERVIEW OF TESTIMONY**

19 **Q. WHAT IS THE PURPOSE OF YOUR TESTIMONY AND HOW IS IT**
20 **ORGANIZED?**

21 A. There are six operations witnesses – Mr. Deryl Tumlinson, Mr. David Mercado, Mr.
22 Randy Pryor, Mr. Eric Easton, Mr. Ronald Bahr, and me – addressing the following
23 subjects.

Figure CF-2**Operations Witnesses and Corresponding Testimony Subjects**

Witness	Subject of Testimony
Mr. Deryl Tumlinson	Overhead Distribution System
Mr. David Mercado	Transmission System and Substations
Mr. Randy Pryor	Strategic Undergrounding and Vegetation Management
Mr. Eric Easton	Damage Prediction, Use of Advanced Analytics, and Wildfire Mitigation
Mr. Ronald Bahr	Information Technology
Mr. Christopher Ford	Cybersecurity Operations

My testimony provides a general overview of the cybersecurity issues that organizations like the Company face and the day-to-day activities conducted by the Company to identify, monitor, assess, prevent and recover from cybersecurity issues. My testimony also highlights significant Resiliency Events impacting or impacted by cybersecurity. With this context in mind, my testimony then describes the costs and benefits associated with three cybersecurity-related Resiliency Measures in the Company's 2026-2028 T&D SRP. More detailed descriptions of these Resiliency Measures and the methodology used to select them are provided in the Company's SRP and Guidehouse Report.

III. OVERVIEW OF CYBERSECURITY

Q. WHAT IS CYBERSECURITY?

A. There are many ways to define the term "cybersecurity," but I will use the NIST definition. NIST defines cybersecurity as: "The ability to protect or defend the use of cyberspace from

cyber attacks.”¹ The NIST also defines the terms “cyberspace” and “cyber attack.”

- Cyberspace: A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers.²
- Cyber attack: An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.³

Colloquially, cybersecurity is protecting hardware (e.g., computers, routers, switches, gateways, technology devices) and software (e.g., operating systems, applications, programs, databases) against unwanted or unauthorized access by persons or programs.

Q. HOW IMPORTANT IS CYBERSECURITY?

A. Cybersecurity is vital. Cybersecurity is needed to protect against theft, fraud, unintentional acts, and most importantly, intentional acts to disable, destabilize, or harm society. The digital world we live in is a target for threat actors, and hardware and software is vital to maintaining its stability. Digital stability, in turn, supports real world functions from enabling communications and commercial transactions to ensuring personally identifying information is kept private. Without actively improving and protecting these hardware and software systems, threat actors would be more able to inflict widespread damage.

¹ NIST Special Publication 800-39.

² *Id.* I would note that NIST has multiple, but similar, definitions of the term cyberspace.

³ *Id.* I would note that NIST has multiple, but similar, definitions of the term cyber attack.

1 **Q. HOW IMPORTANT IS CYBERSECURITY TO UTILITIES?**

2 A. Cybersecurity is vital to utilities, in particular. For utilities like the Company that provide
3 electric delivery service to the public, there must be robust cybersecurity processes in place
4 and robust investment in cybersecurity-related equipment and software. Without these
5 processes, a cyber attack on a utility has the potential to have far-ranging consequences
6 that may impair our ability provide power to customers, compromise public health and
7 safety, as well as provide unauthorized access to sensitive personal data and potential
8 interruptions in service to customers. The real-world operations vital to utilities such as
9 water management, oil and gas pipeline service, and electricity providers have been targets
10 for malware. These attacks, some of which are discussed below, have forced the victims to
11 temporarily cease operations, preventing or significantly impeding their ability to deliver
12 critical resources, like water or gas, to consumers.

13 **Q. PLEASE EXPLAIN.**

14 A. Below are known examples of cyber attacks on public-serving infrastructure:

- 15 ▪ Ukraine electric grid (December 23, 2015): Malware infected SCADA and other IT
16 infrastructure that controlled Ukraine's electric grid, causing outages to thousands of
17 customers during frigid winter temperatures.
- 18 ▪ Colonial Pipeline (May 7, 2021): Colonial Pipeline owns and operates a major pipeline
19 that transports gasoline, diesel, and jet fuel to the eastern seaboard of the United States.
20 In response to a ransomware attack, Colonial Pipeline shut down pipeline operations,
21 causing fuel shortages at gas stations and airports throughout the southern United
22 States.
- 23 ▪ Municipal Water Authority of Aliquippa (November 25, 2023): Water pressure

1 monitoring equipment was compromised, thus causing a shut down and transition to
2 manual operation of the water system.

- 3 ■ American Water (October 3, 2024): American Water, the largest water utility in the
4 United States, experienced unauthorized activity on its computer network. As a result,
5 American Water's customer-facing website was unavailable and American Water was
6 forced to cease its billing activities.

7 In addition, private companies that are critical to energy operations have been targeted by
8 malware:

- 9 ■ Halliburton Cyber Attack (August 21, 2024): Halliburton Company, a major oil field
10 services company and a critical player in the United States' energy supply, experienced
11 unauthorized third-party access to its systems. In order to prevent further damage,
12 Halliburton was forced to shut down certain operations and was unable to access critical
13 business applications, including billings and collections.⁴ Halliburton is still evaluating
14 the damage caused by this event, but has stated it believes that the hackers were able to
15 exfiltrate information from their system.⁵
- 16 ■ Salt Typhoon Attack (Ongoing): The hacking group, Salt Typhoon, gained access to
17 the technology infrastructure of at least eight major telecommunications companies,
18 including AT&T and Verizon. Once they infiltrated the system, Salt Typhoon was able
19 to access the metadata of devices on the network. The full scope of this hack is unclear,
20 but it appears to affect millions of Americans, including high profile political actors.
21 Salt Typhoon has been associated with the Chinese-linked "Volt Typhoon" hacking

⁴ Matt Egan, *Halliburton Confirms a Cyberattack Forced it to Take Its Systems Offline*, CNN (August 23, 2024) <https://www.cnn.com/2024/08/23/tech/halliburton-cyberattack/index.html>.

⁵ Halliburton Company, 8-K (September 9, 2024).

operation which targets utilities and critical infrastructure.⁶

In addition to these high-profile incidents that garnered mainstream media attention, lesser-known incidents that had a similar potential to disrupt vital utility functions occurred in past years. For the electric utility industry, there were four (4) cybersecurity-related incidents that were reported to the DOE in 2023, nine (9) in 2022, and five (5) in 2021.

Q. PLEASE GENERALLY DESCRIBE HOW ENTITIES MANAGE AND ADDRESS CYBERSECURITY RISKS.

A. While cybersecurity policies are tailored for each entity to meet the entity's specific cybersecurity needs, there is conceptual overlap. Generally, entities use the cybersecurity framework established by NIST. NIST's cybersecurity framework uses a functional approach that assigns roles and responsibilities based on function. The functions and corresponding task categories in NIST's current cybersecurity framework are:⁷

- Govern: Organizational context; risk management strategy; roles, responsibilities, and authorities; policy; oversight; and cybersecurity supply chain risk management.
- Identify: Asset management; risk assessment; and improvement of assets.
- Protect: Identity management, authentication, and access control; awareness and training; data security; platform security; and technology infrastructure resilience.
- Detect: Continuous monitoring and adverse event analysis.
- Respond: Incident management; incident analysis; incident response reporting and

⁶ Raphael Satter and A.J. Vicens, *US Government Tells Officials, Politicians To Ditch Regular Calls And Texts*, (December 18, 2024) <https://www.reuters.com/world/us/us-cyber-watchdog-tells-senior-officials-immediately-adopt-end-to-end-encryption-2024-12-18/>.

⁷ NIST's current cybersecurity framework is available online at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>.

1 communication; and incident mitigation.

- 2 ■ Recover: Incident recovery plan execution and incident recovery communication.

3 **Q. DOES THE COMPANY HAVE CYBERSECURITY POLICIES CONSISTENT**
4 **WITH THE NIST CYBERSECURITY FRAMEWORK?**

5 A. Yes. Below is a summary of the Company's cybersecurity policies and processes in
6 reference to each function:

- 7 ■ Govern: CNP has a department, headed by a Chief Information Security Officer, which
8 oversees CNP's cybersecurity policies at the corporate level and for each CNP utility
9 subsidiary. CNP has written policies that address cybersecurity issues such as data
10 classification and control; user account management; enterprise network connectivity;
11 remote access; acceptable use of technology; removable storage devices; cloud
12 security; and vulnerability management. The Company is subject to CNP's
13 cybersecurity policies as applicable.
- 14 ■ Identify: The Company's equipment and software are inventoried; categorized based
15 on criticality, resources, and impact; and vulnerabilities are identified, validated, and
16 recorded. Additionally, the Company's equipment and software are tracked and
17 managed through their respective life cycles.
- 18 ■ Protect: The Company has physical and electronic access controls to equipment and
19 software that limit and monitor access. The Company has robust cybersecurity
20 awareness and training for Company personnel that work on equipment and software.
21 The Company's infrastructure is separated and segmented from CNP's corporate
22 infrastructure, thus minimizing cybersecurity risk to both the Company and CNP.
- 23 ■ Detect: The Company's equipment and software are monitored 24/7/365 by CNP's

Cybersecurity Operations Center. The Cybersecurity Operations Center has dedicated personnel that analyze and respond to potential cybersecurity issues.

- Respond: The Company has an incident response plan that outlines the processes to respond to potential cybersecurity issues, mitigate the impact of a cybersecurity event, and conduct a post-cybersecurity event analysis.

Q. ARE THERE CYBERSECURITY-RELATED FEDERAL REQUIREMENTS WITH WHICH THE COMPANY MUST COMPLY?

- A. Yes. As a NERC-registered entity, the Company is required to comply with applicable NERC CIP Reliability Standards. The NERC CIP Reliability Standards are consistent with the NIST cybersecurity framework. Below is a summary of the NERC CIP Reliability Standards:

Figure CF-3

NERC CIP Reliability Standards

NERC CIP Reliability Standard	Description
CIP-002 (BES Cyber System Categorization)	The Company is required to have processes to identify and categorize cyber assets by function.
CIP-003 (Security Management Controls)	The Company is required to have processes regarding personnel and training, physical security of cyber assets, security management, incident reporting and response, recovery plans, and configuration change management.
CIP-004 (Personnel and Training)	The Company is required to have processes regarding personnel risk assessments and personnel training physical access, electronic access, visitors, handling and storage of cyber information, and identification of and response to a cybersecurity incident.
CIP-005 (Electronic Security Perimeters)	The Company is required to have processes that control inbound and outbound traffic to a network.
CIP-006 (Physical Security of BES Cyber Systems)	The Company is required to have processes that address physical access, including maintenance, testing, detection, response and recordkeeping.

NERC CIP Reliability Standard	Description
CIP-007 (System Security Management)	The Company is required to have processes related to port management, patch management, password management, authentication of user access, and the detection, prevention, and deterrence of malicious code.
CIP-008 (Incident Reporting and Response Planning)	The Company is required to have processes regarding the identification of, classification of, and response to cybersecurity incidents.
CIP-009 (Recovery Plans for BES Cyber Systems)	The Company is required to have recovery plans for cyber-related IT equipment and software.
CIP-010 (Configuration Change Management and Vulnerability Assessments)	The Company is required to have processes for the development, monitoring, and change of baseline configurations of cyber assets.
CIP-011 (Information Protection)	The Company is required to have processes on the identification, protection, and handling of sensitive and confidential cyber information.
CIP-012 (Communications Between Control Centers)	The Company is required to have processes on confidentiality, integrity, and availability of real-time data transmitted between control centers.
CIP-013 (Supply Chain Risk Management)	The Company is required to have processes to mitigate cybersecurity risks associated with IT products or services procured from vendors.
CIP-014 (Physical Security)	The Company is required to have processes for the periodic risk assessment of certain facilities.

The Company undergoes periodic compliance audits by the Texas Reliability Entity, which enforces NERC CIP Reliability Standards in the ERCOT power region, with the most recent audits occurring in 2022 and 2019. The next audit is scheduled for 2025.

Q. PLEASE PROVIDE SPECIFIC AND TANGIBLE EXAMPLES OF THE COMPANY'S CYBERSECURITY PROCESSES.

A. Below are examples of Company's cybersecurity processes as they relate to people, places, and things.

- People: Access to critical equipment and software is granted on an as-needed basis,

1 and background checks are conducted on Company personnel that have access to
2 critical equipment and software. Personnel receive annual cybersecurity training that
3 train them to identify common cybersecurity attack vectors (e.g., phishing), and the
4 Company periodically conducts simulated suspicious cyber activity to assess personnel
5 response.

- 6 ■ Places: The Company's equipment and software are protected by multiple layers of
7 physical and personal security that monitor 24/7/365. Physical access is granted to
8 personnel on an as-needed basis.
- 9 ■ Things: The Company's equipment and software are protected by electronic access
10 controls and monitored 24/7/365. Electronic access is granted to personnel on an
11 as-needed basis.

12 **Q. DO THE COMPANY'S CYBERSECURITY PROCESSES AND**
13 **CORRESPONDING CYBERSECURITY-RELATED EQUIPMENT AND**
14 **SOFTWARE PROVIDE A RESILIENCY BENEFIT TO CUSTOMERS?**

15 A. Yes. The Company relies on equipment and software to provide safe and reliable electric
16 delivery service. Equipment and software, such as SCADA equipment, is needed by the
17 Company to monitor and control the Company's transmission and distribution system and
18 to communicate with field personnel. Cybersecurity-related equipment and software are
19 needed to protect the Company's transmission and distribution system against cyber
20 attacks. Without cybersecurity-related equipment and software, the Company's
21 transmission and distribution system would be at a greater risk of a cyber attack. Given the
22 Company's public-serving responsibilities and the customer information it holds, it would
23 be irresponsible for the Company not to have robust and extensive cybersecurity-related

equipment and software.

Q. DOES THE COMPANY'S CYBERSECURITY PROCESSES AND CORRESPONDING CYBERSECURITY-RELATED EQUIPMENT AND SOFTWARE NEED TO BE PERIODICALLY UPGRADED OR REPLACED?

A. Yes. The cybersecurity landscape is ever-changing because new threats and attack vectors emerge. Entities must anticipate or respond to this ever-changing landscape by periodically revising cybersecurity processes and by periodically upgrading or replacing its equipment and hardware. For example, firewalls must be periodically reviewed and updated to ensure that they have adequate rules in place when considering new cyber issues, new network equipment, and new network configurations.⁸

IV. CYBERSECURITY-RELATED RESILIENCY MEASURES

Q. PLEASE DESCRIBE THE CYBERSECURITY-RELATED RESILIENCY MEASURES IN THE COMPANY'S 2026-2028 T&D SRP ON WHICH YOU ARE PROVIDING TESTIMONY.

A. There are three cybersecurity-related Resiliency Measures in the Company's 2026-2028 T&D SRP. The table below summarizes the cybersecurity Resiliency Measures. Additional detail on each Resiliency Measure and why it was chosen is provided in the Company's SRP and Guidehouse Report.

⁸ A firewall monitors and controls incoming and outgoing computer network traffic.

Figure CF-4

**Cybersecurity-Related Resiliency Measures Estimated Costs and CMI
(in millions)**

Resiliency Measure	Resiliency Event to be Mitigated	T&D SRP Rule Category	Estimated Capital Costs 2026-2028	Estimated O&M Costs 2026-2028	Estimated Total Costs 2026-2028	Estimated CMI Savings
Network Security & Vulnerability Management (RM-30)	Cybersecurity event	Cybersecurity	\$7.5	\$2.0	\$9.5	N/A*
IT/OT Cybersecurity Monitoring (RM-31)	Cybersecurity event	Cybersecurity Modernization	\$13.4	\$4.2	\$17.6	N/A*
Cloud Security, Product Security & Risk Management (RM-32)	Cybersecurity event	Cybersecurity	\$4.0	\$6.0	\$10.0	N/A*
Total			\$24.9	\$12.2	\$37.1	

*Note: Please see Section 5 of Exhibit ELS-2 for a qualitative benefit analysis of this Resiliency Measure.

Q. WILL THESE CYBERSECURITY-RELATED RESILIENCY MEASURES ENHANCE RESILIENCY?

A. Yes. As previously discussed in my testimony, cybersecurity processes and corresponding cybersecurity-related equipment and software must be periodically upgraded or replaced in anticipation of, or in response to, the ever-changing cybersecurity landscape. The cybersecurity-related Resiliency Measures will enhance the Company's cybersecurity posture by strengthening the Company's ability to identify, protect, detect, respond to, and recover from potential cybersecurity events that may negatively impact the Company's equipment and software and, in turn, may affect the Company's ability to safely and efficiently operate its transmission and distribution system for its customers.

V. CONCLUSION

Q. WILL THE RESILIENCY MEASURES IN YOUR TESTIMONY HELP THE COMPANY SERVE ITS CUSTOMERS?

A. Yes. The 2026-2028 T&D SRP is a significant step taken by the Company to implement the commitments made to the customers and communities it has the privilege to serve and make the necessary investments in its transmission and distribution system to be the most resilient coastal grid in the country.

Q. IS IMPLEMENTING THE RESILIENCY MEASURES IN YOUR TESTIMONY IN THE PUBLIC INTEREST?

A. Yes.

Q. SHOULD THE COMMISSION APPROVE THE COMPANY'S 2026-2028 T&D SRP?

A. Yes.

Q. DOES THIS CONCLUDE YOUR DIRECT TESTIMONY?

A. Yes.

STATE OF TEXAS §
COUNTY OF Harris §

AFFIDAVIT OF CHRISTOPHER W. FORD

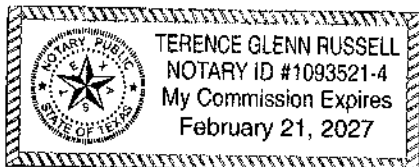
BEFORE ME, the undersigned authority, on this day personally appeared
CHRISTOPHER W. FORD who having been placed under oath by me did depose as follows:

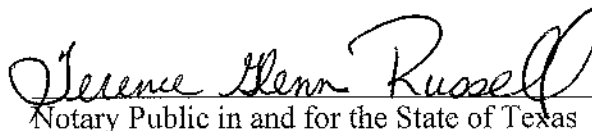
1. "My name is CHRISTOPHER W. FORD. I am of sound mind and capable of making this affidavit. The facts stated herein are true and correct based upon my personal knowledge.
2. I have prepared the foregoing Direct Testimony and the information contained in this document is true and correct to the best of my knowledge."

Further affiant sayeth not.


CHRISTOPHER W. FORD

SUBSCRIBED AND SWORN TO BEFORE ME on this 6th day of JANUARY,
2025.




Notary Public in and for the State of Texas

My commission expires: 02-21-2027

Exhibit CF-1: Glossary of Acronyms

BES	Bulk Electric System
CIP	Critical Infrastructure Protection
Company	CenterPoint Energy Houston Electric, LLC
CNP	CenterPoint Energy, Inc.
Commission	Public Utility Commission of Texas
DOE	Department of Energy
ERCOT	Electric Reliability Council of Texas
Guidehouse	Guidehouse Inc.
Guidehouse Report	The analysis of the Company's resiliency measures provided by Guidehouse.
IT	Information Technology
NERC	North American Electric Reliability Corporation
NERC CIP Reliability Standards	The CIP standards the NERC-registered entities must comply with.
NIST	National Institute of Standards and Technology
O&M	Operations and maintenance
Resiliency Event	An event involving extreme weather conditions, wildfires, cybersecurity threats, or physical security threats that poses a material risk to the safe and reliable operation of the Company's transmission and distribution systems
Resiliency Measure	A measure designed to prevent, withstand, mitigate, or more promptly recover from the risks posed to the Company's transmission and distribution system by a Resiliency Event
SCADA	A supervisory control and data acquisition system
T&D SRP Rule	16 Tex. Admin. Code § 25.62
2026-2028 T&D SRP or SRP	The Company's 2026-2028 Transmission and Distribution System Resiliency Plan
Texas Reliability Entity	The entity that performs compliance audits and enforces the NERC CIP Reliability Standards in the ERCOT power region.

This page was
intentionally left
blank.

EXHIBIT 9

THE DIRECT TESTIMONY OF COMPANY WITNESS MR. BRAD A. TUTUNJIAN

This page was
intentionally left
blank.

DOCKET NO. 57579

**APPLICATION OF CENTERPOINT
ENERGY HOUSTON ELECTRIC,
LLC FOR APPROVAL OF ITS 2026-
2028 TRANSMISSION AND
DISTRIBUTION SYSTEM
RESILIENCY PLAN**

**§
§
§
§
§**

**PUBLIC UTILITY
COMMISSION OF TEXAS**

DIRECT TESTIMONY OF

BRAD A. TUTUNJIAN

FOR

CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC

JANUARY 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY	ES-1
I. INTRODUCTION.....	1
III. OVERVIEW OF TESTIMONY	2
IV. MICROGRID PILOT PROGRAM	3
V. CONCLUSION	11

TABLE OF EXHIBITS

<u>Exhibits</u>	<u>Description</u>
BT-1	Glossary of Acronyms

TABLE OF FIGURES

Figure BT-1- Operations Witnesses and Corresponding Testimony Subjects	3
Figure BT-2 - Microgrid Illustration.....	4

EXECUTIVE SUMMARY

The Company presents the SRP to the Commission for review and approval, including the specific Resiliency Measures detailed in the SRP, pursuant to the Commission's System Resiliency Rule. The Resiliency Measures detailed in the SRP will support the continued safe and reliable operation of Company's transmission and distribution system through various Resiliency Events, including extreme weather events. The Company estimates that it will incur a total of approximately \$5.543 billion in capital costs and approximately \$210.7 million in incremental O&M expense over 2026-2028 to implement the Resiliency Measures in the Company's SRP. The Company anticipates that its SRP will benefit customers by mitigating the impact of certain Resiliency Events that occur in the Company's service area such as extreme weather conditions, thus reducing overall outage times, avoiding approximately 1,309 million CMI, the number of customers impacted, and system restoration costs.

In addition to the proposed Resiliency Measures, the Company's SRP also seeks Commission approval of a Microgrid Pilot Program through which the Company would coordinate with selected third-party entities in the study, design, implementation, and operation of utility scale microgrids in the Company's service area. Through the proposed Microgrid Pilot Program, the Company would obtain additional operational data and experience to inform both the Company and the Commission on the demonstrated benefits of utility scale microgrids as a Resiliency Measure, as well as the further development and refinement of engineering and operational standards for utility scale microgrids and potential future integration of utility scale microgrids in the Company's service area. The Company's SRP is in the public interest, and the Company requests that the Commission approve the Company's SRP, including the proposed Microgrid Pilot Program.

I. INTRODUCTION

Q. PLEASE STATE YOUR NAME AND CURRENT POSITION.

A. My name is Brad Tutunjian. I am the Vice President, Texas Gas for CNP.

Q. PLEASE SUMMARIZE YOUR EDUCATIONAL AND WORK BACKGROUND.

A. I graduated from Texas Tech University in 1997 with a Bachelor of Science Degree in Mechanical Engineering. I am a licensed Professional Engineer in the State of Mississippi. From my 1997 graduation to the present, I have been employed by CNP or one of its affiliates. My positions within CNP have included Graduate Engineer; Distribution Designer; Distribution Operations Manager; District Manager; Service Area Director, Electric Distribution Operations; Division Vice President – Natural Gas Regional Operations (Mississippi/Louisiana); Division Vice President – Regional Operations (Minnesota); Vice President of Distribution Operations and Service Delivery; and Vice President, Regulatory Policy.

Q. WHAT ARE YOUR MOST RECENT RESPONSIBILITIES AT CNP?

A. I was named Vice President, Regulatory Policy in 2023, at which time I assumed responsibility for supporting regulatory initiatives on behalf of CNP before various regulatory bodies on matters of policy impacting various CNP business units. Effective January 1, 2025, I became Vice President, Texas Gas, responsible for CNP's gas utility in Texas, which serves approximately 1.9 million customers throughout the Greater Houston area, East Texas, and South Texas. Given my regulatory policy role as the Company was developing its SRP, I remain the witness addressing the proposed Microgrid Pilot Program.

1 Q. ON WHOSE BEHALF ARE YOU TESTIFYING IN THIS PROCEEDING?

2 A. I am testifying on behalf of the Company.

3 Q. HAVE YOU TESTIFIED PREVIOUSLY?

4 A. Yes. I filed testimony with the Commission in Docket Nos. 53442 and 54825,
5 which were both DCRF proceedings, Docket No 56211, the most recent base rate
6 proceeding, as well as Docket No 56548, the Company's prior System Resiliency
7 Plan, which this plan replaces. I have also testified in two gas utility rate
8 proceedings before the Minnesota Public Utilities Commission in Docket Nos. G-
9 008/GR-17-285 and G-008/GR-19-524 as well as in Texas before the Railroad
10 Commission in Case No. OS-23-00015513.

11 **Q. WHAT EXHIBITS HAVE YOU INCLUDED WITH YOUR TESTIMONY?**

12 A. I have included the one exhibit listed in the Table of Contents as part of my
13 testimony.

14 Q. WAS YOUR TESTIMONY PREPARED BY YOU OR BY OTHERS
15 WORKING UNDER YOUR DIRECTION AND CONTROL?

16 A. Yes.

17 **III. OVERVIEW OF TESTIMONY**

18 **Q. WHAT IS THE PURPOSE OF YOUR TESTIMONY?**

19 A. The purpose of my testimony is to demonstrate that it is in the public interest for
20 the Commission to approve the proposed Microgrid Pilot Program included in the
21 Company's SRP.

22 Q. ARE OTHER COMPANY WITNESSES PROVIDING DIRECT
23 TESTIMONY IN THIS DOCKET?

1 A. Yes. Company witness Nathan Brownell provides an overview of the SRP as well
 2 as the Company's service territory and customer profile. Additionally, there are six
 3 operations witnesses – Mr. Deryl Tumlinson, Mr. David Mercado, Mr. Randy
 4 Pryor, Mr. Eric Easton, Mr. Ronald Bahr, and Mr. Christopher Ford – addressing
 5 the following subjects.

6 **Figure BT-1**

7 **Operations Witnesses and Corresponding Testimony Subjects**

Witness	Subject of Testimony
Mr. Deryl Tumlinson	Overhead Distribution System
Mr. David Mercado	Transmission System and Substations
Mr. Randy Pryor	Strategic Undergrounding and Vegetation Management
Mr. Eric Easton	Damage Prediction, Use of Advanced Analytics, and Wildfire Mitigation
Mr. Ronald Bahr	Information Technology
Mr. Christopher Ford	Cybersecurity Operations

8

9 Company witnesses Muss Akram and Jeff Garmon provide testimony on customer
 10 affordability and accounting related to the SRP, respectively. A summary of the
 11 topics covered by each witness is provided in the testimony of Nathan Brownell.

12

IV. MICROGRID PILOT PROGRAM

13

Q. WHAT IS A MICROGRID?

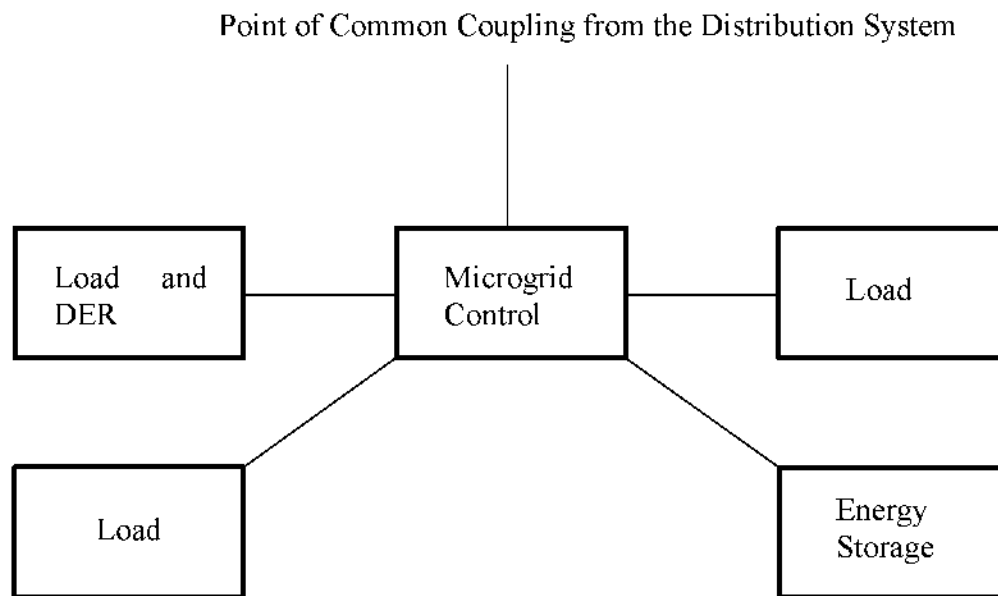
14

A. Generally, a microgrid consists of a group of interconnected loads and local
 15 generation resources that are isolated from and can be switched in such a way as to

act as a single controllable entity with respect to the distribution system.¹ The illustration below generally depicts a microgrid.

Figure BT-2

Microgrid Illustration



Q. DOES THE COMPANY CURRENTLY HAVE MICROGRIDS THAT OPERATE IN THE COMPANY'S SERVICE AREA?

A. Yes, but not utility-scale microgrids.

Q. WHAT IS THE DEFINITION OF UTILITY-SCALE MICROGRIDS?

A. A utility-scale microgrid is a microgrid that consists of multiple points of delivery interconnected through the utility's distribution system which can operate in parallel with the distribution system or isolate and operate in an islanded mode in an emergency load shed condition.

¹ This definition for microgrid was developed by the National Renewable Energy Laboratory. *Grid Modernization: Microgrids*, THE NATIONAL RENEWABLE ENERGY LABORATORY (available online at: <https://www.nrel.gov/grid/microgrids.html>).

1 **Q. HAS THE COMPANY RECEIVED INQUIRIES AND INTEREST FROM**
2 **MICROGRID DEVELOPERS ABOUT THE POSSIBILITY OF**
3 **OPERATING A UTILITY-SCALE MICROGRID IN THE COMPANY’S**
4 **SERVICE AREA?**

5 A. Yes. Throughout the past few years, the Company has received inquiries from a
6 number of third parties about operating utility-scale microgrids in the Company’s
7 service area.

8 **Q. WHAT IS THE COMPANY PROPOSING RELATED TO MICROGRIDS?**

9 A. The Company is proposing a Microgrid Pilot Program that will be leveraged to test
10 these isolated islands and provide input on their effects to customers and the grid
11 as a whole during appropriate Resiliency Events.

12 **Q. WHY IS THE COMPANY PRESENTING THE UTILITY-SCALE**
13 **MICROGRID AS A PILOT PROGRAM AND NOT AS A RESILIENCY**
14 **MEASURE?**

15 A. The Company has presented the utility-scale microgrid as a pilot program, and not
16 as a Resiliency Measure, for several reasons. First, the Company wants to provide
17 the Commission with a wholistic picture of its resiliency efforts. Setting aside
18 resources to innovate, respond to customer interests, and explore new strategies is
19 essential for the Company to create new solutions to reliability issues. The
20 Microgrid Pilot Program is a part of the Company’s systematic approach to improve
21 the resiliency of its system and become a model for other utilities to follow. Second,
22 the Company has not collected sufficient evidence on utility-scale microgrids to
23 demonstrate the requirements of a Resiliency Measure to the Commission.

1 However, as demonstrated by the third-party support, the Company believes that
2 they do have potential to provide reliability benefits to customers. Investing in
3 modern solutions now allows the Company to adapt as its system and customers
4 become more complex.

5 **Q. PLEASE DESCRIBE THE COMPANY’S MICROGRID PILOT**
6 **PROGRAM.**

7 A. Under the Company’s proposed Microgrid Pilot Program, the Company would
8 coordinate with third-party entities that are chosen in an RFP process (estimated
9 number of 3-5 third party developers expected to be awarded) on the study, design,
10 implementation, and operation of utility scale microgrids in the Company’s service
11 area.

12 **Q. WHAT IS THE PURPOSE OF THE COMPANY’S MICROGRID PILOT**
13 **PROGRAM?**

14 A. The Company believes that utility-scale microgrids will provide a benefit to
15 customers during certain Resiliency Events. Our initial focus is on Resiliency
16 Events that might otherwise lead to load shedding. In the event that a Resiliency
17 Event damages the distribution system such that loads interconnected to a utility-
18 scale microgrid cannot be served from the distribution system but the utility scale
19 microgrid region remains intact, a utility-scale microgrid would be available to
20 enable service to the interconnected loads to be restored, leveraging the energy from
21 the distributed energy resource(s) interconnected to the utility scale microgrid to
22 feed customers. The Company seeks to obtain additional operational data and
23 experience as to how a utility-scale microgrid—including utility-scale microgrids

1 that serve a city or city facilities—would perform during a Resiliency Event. The
2 Company is therefore proposing the Microgrid Pilot Program so that the Company
3 can obtain additional operational data and experience to inform both the Company
4 and the Commission regarding the demonstrated benefits of utility scale microgrids
5 as a Resiliency Measure, the further development and refinement of engineering
6 and operational standards for utility scale microgrids, and potential future
7 integration of utility scale microgrids in the Company's service area.

8 **Q. PLEASE DESCRIBE THE IMPLEMENTATION PROCESS FOR THE**
9 **MICROGRID PILOT PROGRAM.**

10 A. At a general level, the implementation process for the Microgrid Pilot Program will
11 entail the following:

- 12 ▪ Request for Proposal: The Company will issue a RFP to interested parties. The
13 RFP will contain the relevant technical, operational, and financial requirements
14 needed to qualify for the Company's Microgrid Pilot Program.
- 15 ▪ Evaluation: The Company will evaluate the bids submitted by interested parties.
16 Submitted bids will be evaluated considering criteria such as total amount of
17 load that would be interconnected to the utility scale microgrid; total amount of
18 local generation that would be interconnected to the utility scale microgrid;
19 modifications to the Company's distribution system, telecommunications
20 network, information technology, and operational technology needed to ensure
21 safe and reliable operations; and the type of load that would be interconnected
22 to the utility scale microgrid (e.g. critical load, public infrastructure,
23 residential). The Company would seek out and prioritize one or more bids for a

utility scale microgrid specifically serving a city or city facilities (as opposed to private businesses or residential developments, for example).

- Study, Design, and Engineering: Upon determining which submitted bids will be part of the Company's Microgrid Pilot Program, the Company will commence the study, design, and engineering phase.
- Construction and Installation: The Company will construct or install the equipment and facilities necessary for the safe and reliable operation of the Company's distribution system.
- Operations: Upon commencement of operations, the Company's Microgrid Pilot Program will operate as called upon by the Company.

Q. HOW MANY MICROGRIDS WOULD BE PART OF THE COMPANY'S MICROGRID PILOT PROGRAM?

A. Instead of determining the number of utility scale microgrids, the Company will engage developers and track this pilot program based on load demand and megawatts of necessary microgrid generation capacity. The Company will strive to achieve load diversity in participating utility scale microgrids (e.g. critical load, public infrastructure, residential). As noted above, ideally, the Company will seek to include one or more microgrids serving a city or city facilities.

Q. WHY DOES THE COMPANY PLAN TO PRIORITIZE A MICROGRID SERVING A CITY OR CITY FACILITIES?

A. Cities in which the Company operates are important stakeholders and serve an important public function because cities oftentimes provide critical services to the public such as first responder service (i.e., police, fire, emergency medical),

1 emergency management and disaster relief, and water and wastewater services.
 2 Prioritizing microgrids that serve a city or city facilities provides societal benefits
 3 to customers and the public by allowing the city or city facility that is connected to
 4 a microgrid to continue to provide critical services.

5 **Q. WHICH RESILIENCY EVENTS IS THE COMPANY'S MICROGRID**
 6 **PILOT PROGRAM INTENDED TO ADDRESS?**

7 A. The Company's Microgrid Pilot Program is intended to address Resiliency Events
 8 that may disrupt service to the Company's customers, particularly Resiliency
 9 Events which might prompt ERCOT to direct the Company to shed load. Such
 10 Resiliency Events will primarily be attributable to certain extreme weather events
 11 or generation shortfall.

12 **Q. WHAT IS THE PROPOSED EFFICACY METRIC OR CRITERIA, AND**
 13 **WHAT IS THE EXPECTED EFFICACY FOR THE MICROGRID PILOT**
 14 **PROGRAM?**

15 A. Since the Microgrid Pilot Program will be implemented on a pilot basis, the
 16 Company will monitor the operational performance of the participating utility scale
 17 microgrids and will report to the Commission the Company's findings.

18 **Q. DOES THE COMPANY HAVE A REQUEST RELATED TO COSTS**
 19 **ASSOCIATED WITH THE MICROGRID PILOT PROGRAM?**

20 A. Yes. The Company requests that it be permitted to defer the Company's costs in
 21 the requested regulatory asset associated with study, design, implementation, and
 22 operation of the Company's Microgrid Pilot Program. The Company also requests
 23 that it be permitted to recover such costs in a future proceeding. The Company

1 commits that the total cost associated with the study, design, implementation, and
2 operation of the Company's Microgrid Pilot Program will not exceed \$35 million.

3 **Q. WHAT KINDS OF COSTS WILL THE COMPANY INCUR?**

4 A. The Company will incur costs of an engineering study and any equipment related
5 to the creation of the island condition (reclosers, switches, and monitors mainly).
6 There will also be costs associated with the monitoring of these pieces of equipment
7 within our SCADA system, providing the ability to shut down the Microgrid
8 remotely in the event of any safety concerns. The Company will not incur costs
9 from the purchase of a generator but may make payments to vendors who provide
10 microgrid services to the Company.

11 **Q. IS THE COMPANY REQUESTING TO RECOVER THE INSTALLATION
12 AND MAINTENANCE COSTS OF THE MICROGRID GENERATOR
13 ITSELF?**

14 A. No. The design, installation and maintenance of the Microgrid generator will be the
15 responsibility of the Microgrid generator owner. The Company is only seeking to
16 recover the necessary utility costs to facilitate the configuration and ability of the
17 Microgrid island equipment to communicate, operate, and provide interconnection
18 for this supplemental electric supply on its distribution system when called upon
19 during an extreme weather event, along with any costs associated with studying and
20 evaluating the performance of the Microgrid on the distribution system as
21 previously described.

22 **Q. WHAT COSTS IS THE COMPANY NOT SEEKING TO RECOVER?**

23 A. The company is not seeking to recover direct generator costs (costs to purchase and

1 maintain a generator). As noted above, however, the Company may incur charges
2 associated with the operation of these generators, such as fuel, by vendors providing
3 microgrid services to the Company.

4 **V. CONCLUSION**

5 **Q. SHOULD THE COMMISSION APPROVE IMPLEMENTATION OF THE**
6 **MICROGRID PILOT PROGRAM IN THE COMPANY'S SYSTEM**
7 **RESILIENCY PLAN AS BEING IN THE PUBLIC INTEREST?**

8 A. Yes, for the same reasons as discussed in my testimony.

9 **Q. SHOULD THE COMMISSION APPROVE THE COMPANY'S**
10 **RESILIENCY PLAN?**

11 A. Yes.

12 **Q. DOES THIS CONCLUDE YOUR DIRECT TESTIMONY?**

13 A. Yes.

STATE OF TEXAS §
COUNTY OF HARRIS §

AFFIDAVIT OF BRAD A. TUTUNJIAN

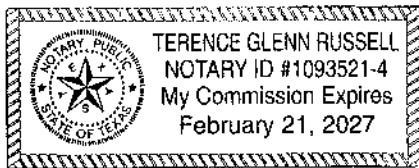
BEFORE ME, the undersigned authority, on this day personally appeared BRAD A. TUTUNJIAN who having been placed under oath by me did depose as follows:

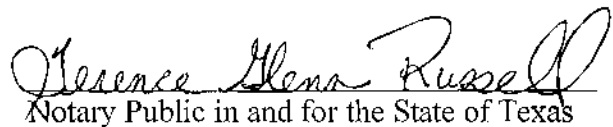
1. "My name is BRAD A. TUTUNJIAN. I am of sound mind and capable of making this affidavit. The facts stated herein are true and correct based upon my personal knowledge.
2. I have prepared the foregoing Direct Testimony and the information contained in this document is true and correct to the best of my knowledge."

Further affiant sayeth not.


BRAD A. TUTUNJIAN

SUBSCRIBED AND SWORN TO BEFORE ME on this 6 day of January
2025.




Notary Public in and for the State of Texas

My commission expires: 02-21-2027

Exhibit BT-1: Glossary of Acronyms

2026-2028 T&D SRP or SRP	The Company's 2026-2028 Transmission and Distribution System Resiliency Plan
Company	CenterPoint Energy Houston Electric, LLC
CNP	CenterPoint Energy, Inc.
CMI	Customer minutes interrupted
Commission	Public Utility Commission of Texas
ERCOT	Electric Reliability Council of Texas
O&M	Operations and maintenance
Resiliency Event	An event involving extreme weather conditions, wildfires, cybersecurity threats, or physical security threats that poses a material risk to the safe and reliable operation of the Company's transmission and distribution systems
Resiliency Measure	A measure designed to prevent, withstand, mitigate, or more promptly recover from the risks posed to the Company's transmission and distribution system by a Resiliency Event
RFP	Request for Proposal

This page was
intentionally left
blank.

EXHIBIT 10

THE DIRECT TESTIMONY OF COMPANY WITNESS MR. MUSSADIQ AKRAM