5. Over the long-term (i.e., beyond the three-year investment horizon of its current Plan), review alternative, non-build resiliency measures, such as local generation and storage technologies, in lieu of traditional investments. *(note: after completion of the initial Guidehouse review, CenterPoint Houston added a microgrid pilot project to its Resiliency Plan*)
6. Resiliency measure-specific recommendations include:
   a. **Digital Substation** – Examine in greater detail additional potential benefits associated with the Digital Substation resiliency measure, considering increased value associated with enhanced communications, automation, visualization, and operational consideration.
   b. **Substation Physical Security Fencing** – Consider more robust security fencing such as concrete walls for the Substation Physical Security Fencing resiliency measure in lieu of wire mesh.
   c. **Substation Flood Control** – Refine proposed Substation Flood Control elevation levels using flood inundation results.
   d. **Distribution Resiliency – Circuit Rebuilds** – Prioritize Distribution Resiliency – Circuit Rebuild upgrades using more targeted hurricane and wind studies.
   e. **Advanced Aerial Imagery Platform / Digital Twin** – Identify additional applications and benefits associated with the Advanced Aerial Imagery Platform / Digital Twin resiliency measure beyond those listed in our report.
   f. **IGSD Installation Resiliency Measure** – Analyze the benefits of transitioning to fully automated IGSD schemes for new (and potentially existing) schemes.

6.4 Review of Technology Resiliency Measures

6.4.1 Findings

Guidehouse reviewed the five CenterPoint Houston technology resiliency measures and identified the effectiveness and benefits of each measure in a qualitative comparative analysis process that compared relevant functions and security practices in each resiliency measure with industry best practices described in the NIST CSF. Based on analysis of the correlation between CenterPoint Houston's proposed resiliency measures and the NIST CSF framework, Guidehouse finds that CenterPoint Houston's Technology Resiliency Measures are all reasonable for inclusion in CenterPoint Houston's Resiliency Plan.

The technology resiliency measures included in CenterPoint Houston's Resiliency Plan target centralized management of assets and data, communication and control for critical electrical systems and the personnel responsible for those systems, detection and response to cybersecurity threats, information protection, data security, access control, and continuous monitoring for security. By targeting these areas, CenterPoint Houston should bolster its resilience against cybersecurity threats and meet its objective to enhance electric grid resilience in an increasingly digital landscape. Further, many of these resiliency measures are fundamental to CenterPoint Houston's ability to effectively manage and quickly recover from extreme weather events by enabling communication, control, and visibility during such events.

Guidehouse finds that CenterPoint Houston's Resiliency Plan appropriately prioritizes technology resiliency measures that help mitigate cybersecurity risk. CenterPoint Houston is deploying measures that can be classified as enabling technologies per the IEEE by aiming to optimize operations, improve reliability, and ultimately ensure uninterrupted service delivery. Further, findings from a peer utility benchmarking survey indicates that proposed technology resiliency measures included in CenterPoint Houston's Resiliency Plan are consistent with those deployed at other utilities and are: 1) appropriate for addressing the physical security and cybersecurity risks each measure faces; 2) aligned with industry best practices; and 3) beneficial to customers and communities served by CenterPoint Houston. Based on these findings, as well as Guidehouse's analysis of the correlation between CenterPoint Houston's proposed resiliency measures and the NIST CSF framework, Guidehouse finds that CenterPoint Houston's technology resiliency measures are reasonable for inclusion in CenterPoint Houston's Resiliency Plan.

6.4.2 Recommendations

Guidehouse offered the following recommendations related to CenterPoint Houston's proposed technology resiliency measures to further enhance its current and future resiliency plans:

1. **Networking, Vulnerability, and Security – Data Management** – Investigate if downstream applications support encryption for data-in-transit, as applications that do not support encryption for data-in-transit may be affected in relation to uptime, availability, and general resilience. For vulnerability, review patterns in deployment, such

as applications, components, or any other system component that has repeatable settings and configurations so that CenterPoint Houston is aligned to industry general and cybersecurity best practices. For network, analyze network component and system best practices so that CenterPoint Houston's network environment is further logically secured to ensure network zones are locked down and isolated.

2. **Data Center Refresh** – When considering any type of data migration, ensure that all on premises options such as application, workflow, and process optimizations are investigated to determine if they can be migrated, as migrating data to any new environment will affect uptime, application reliability, and support overall resilience. This is due to the eccentricities of any new environment, regardless of cloud or another on premise environment.
3. **Voice and Mobile Data Refresh – Field Devices** – Leverage multiple sources of asset (field device) information in accordance with visual checks to ensure all legacy technology is properly tracked and decommissioned. Assets with end-of-life software that are still attached to the system and unaccounted for can either affect uptime/ resilience of the overall system if there is a malfunction, as well as become an attack vector for an external threat.
4. **Backhaul Microwave Communication – Device Migration** – Develop a settings checklist, or asset configuration guide, so they can be easily replicated and installed on all new field devices, removing the opportunity for incorrect settings being applied. This could potentially impact communication and responses in a weather-driven or other event that could impact the electric distribution and transmission systems.
5. **IT/OT-Cybersecurity Monitoring** – During implementation and deployment of Splunk and Nozomi, notify all users of the deployment, including detail on expectations to limit false flags while ensuring suspicious events and alerts and unexpected interactions are addressed. For the Splunk Integration, tune ingested information to minimize false alarms and unnecessary resource usage. Lastly, for the Nozomi Integration, refine vulnerability scanning so that only relevant suspicious or anomalous code is present in reports and Nozomi's finding and vulnerability dashboards.
6. **Metrics for All Technology Resiliency Measures** – Identify and establish metrics to determine risks, especially around loss, misuse, or compromise of systems and equipment. This will assist with ensuring CenterPoint Houston is aware of events and trends so that it can take appropriate actions to increase resilience.

Guidehouse

Exhibit ELS-2 – Appendix A: Resiliency Planning Regulatory Jurisdiction Benchmarking

Prepared for:

CenterPoint Energy Houston Electric, LLC

Submitted by: Guidehouse

April 2024

Table of Contents

Disclaimers

This deliverable (the "Report") was prepared for CenterPoint Energy Houston Electric, LLC ("CenterPoint Houston"), on terms specifically limiting the liability of Guidehouse Inc. ("Guidehouse"), for use in connection with a filing by CenterPoint Houston at the Public Utility Commission of Texas ("PUCT" or "Commission") seeking approval of CenterPoint Houston's transmission and distribution system resiliency plan pursuant to 16 Tex. Admin. Code § 25.62 (the "Resiliency Plan Proceeding"). Other than for use in the Resiliency Plan Proceeding as provided by applicable laws and rules, the Report is not to be distributed without Guidehouse's prior written consent and subject to execution of a third-party access agreement. Guidehouse's conclusions are the results of the exercise of its reasonable professional judgment and are based, in part, upon facts provided to Guidehouse by CenterPoint Houston, which Guidehouse has accepted with CenterPoint Houston's permission as true and accurate without independent verification or inquiry.

Use of the Report is limited solely to the Resiliency Plan Proceeding. Other than as permitted by the laws and rules applicable to the Resiliency Plan Proceeding, the Report may not be distributed to any third party without Guidehouse's express prior written consent. Guidehouse has used reasonable care and exercised its reasonable professional judgement in preparing the Report, but does not make any representations or warranties of any kind to any third party with respect to the Report. Guidehouse accepts no liability of any kind whatsoever for any claims, liabilities and damages, if any, alleged by third parties as a result of decisions made, or not made, or actions taken, or not taken, based on this Report.

1. Executive Summary

This report is intended to provide insights into the range of approaches utilities in different U.S. jurisdictions have taken for planning resiliency-focused investments. This information provides indication of the types of resiliency investments that are "industry best practice" and examples of how other jurisdictions and utilities are approaching resiliency planning for the electric utility industry. More specifically, this report covers the following topics for the purpose of this jurisdictional benchmarking scan:

- Distinctions made between electric grid resiliency and reliability
- Example investments included in electric utility resiliency plans
- Magnitude thresholds used to define resiliency events
- Criteria used to identify the need for resiliency investments
- Methods for determining cost effectiveness of resiliency investments
- Resiliency planning reporting requirements
- Considerations of equity and environmental justice communities
- Cybersecurity, information technology (IT), and operational technology (OT) investments

Table 1 summarizes which jurisdictions and utilities were researched for inclusion in this report.

Table 1
Jurisdictions and Utilities Researched for this Report

Jurisdictions	Electric Utilities
Alaska	Alaska Village Electric Cooperative
California	Southern California Edison (SCE) and San Diego Gas and Electric (SDG&E)
Connecticut	Connecticut Light and Power Company
Florida	Florida Power and Light (FP&L), Duke Energy Florida (DEF) and Tampa Electric Company (TECO)
Georgia	N/A
Hawaii	Hawaiian Electric (HECO) Companies
Illinois	Commonwealth Edison and Ameren Illinois
Louisiana	Entergy
Massachusetts	Eversource
Michigan	Detroit Edison Electric Energy (DTE)
New Jersey	Public Service Electric and Gas Company (PSE&G)
New York	Consolidated Edison (Con Edison) and National Grid
North Carolina	Duke Energy
Ohio	American Electric Power (AEP)
Oregon, Washington, Idaho, Wyoming	Avista and PacifiCorp
Puerto Rico	Puerto Rico Electric Power Authority
South Carolina	N/A
Utah	Rocky Mountain Power
Vermont	Green Mountain Power
Virginia	Dominion Energy

Table 2 provides a summary of types of resiliency investments proposed or otherwise generally considered "in-scope" for a selection of the jurisdictions researched. The majority of jurisdictions researched include within scope similar types of distribution investment/programs (referred to as Resiliency Measures) such as pole replacement and hardening.

Table 2
Summary of Types of Resiliency Investments Identified in Other Jurisdictions

	CT	FL	HI	LA	NJ	NY	OH	OR	VT	VA	MI	NC	GA	SC	IL
Pole Replacement / Hardening	X	X	X	X	X	X			X	X	X	X			X
Substation Flood Control			X	X	X	X			X			X	X	X	
Vegetation Management	X	X		X		X		X		X					X
Undergrounding Circuits	X		X	X	X	X			X	X	X	X	X		X
Substation Physical Security						X				X					
Transmission		X	X	X					X	X	X				X
Cyber Security										X	X				X
Other			DERs / Microgrid		Outage Mgmt. System Upgrade	DERs Microgrid	DERs/ Microgrid	DERs	Generation	Microgrid		Microgrid		Microgrid	

1.1 Key Takeaways

Key takeaways and themes identified through this research include:

1. **Electric resiliency planning is observed in many jurisdictions, either driven by policy and regulation or through proactive requests made by investor-owned utilities with their regulator** – Policymakers and electric transmission and distribution utilities across the country are actively involved in electric grid resiliency efforts, regardless of specific topological or climate conditions. The range of in-scope resiliency investments seems to be influenced by which resiliency risks are most prominent in the jurisdiction and whether a competitive generation market exists. In jurisdictions with vertically integrated utilities (i.e., generation, transmission, and distribution service) the scope of resiliency planning seems to broader to often include distributed energy resources (DERs), microgrids, and/or generation facility resiliency projects.
2. **CenterPoint Energy's proposed Resiliency Plan seems similar in scope to what is observed in other jurisdictions** – State regulatory commissions have approved resiliency plans with similar scope to what CenterPoint Energy is filing with the Public Utility Commission of Texas (PUCT) for its Houston Electric service area. In particular, pole replacement/hardening and substation flood control are often within scope.
3. **Magnitude threshold can have different meanings depending on utility and location** – A magnitude threshold often refers to a specific wind speed, hurricane category, flood level, or other well-known term used to measure the severity of the event. Electric system resiliency plans typically aim to mitigate the risk of electric grid infrastructure failure by ensuring the electric grid infrastructure can withstand a specific magnitude threshold of wind, hurricane, flood, or other resiliency event. The actual magnitude threshold can vary based on location and geography given the differences in resiliency risk profiles across different locations and geographies. In some jurisdictions, magnitude threshold is also

considered in the context of estimated impacts of the event on the system and customers so that the performance of resiliency measures later be evaluated against those potential impacts identified.

4. **Metrics are commonly used to identify the need for resiliency grid investments and to measure their effectiveness** – In order for utilities to gain regulatory approval of capital investments in their resiliency plans, utilities typically must demonstrate the need for such investments. One way of demonstrating the need for resiliency investments that has been used in many other jurisdictions is demonstrating that proposed investments can meet certain metrics that determine the need for such investments (e.g., positive benefit-cost ratio). Metrics can be quantitative or qualitative and can often be used to track performance of resiliency investments over time. Tracking the performance of resiliency plans over time can determine how well they are mitigating resiliency event impacts or if additional or new investments may be needed. A key to success of utility resiliency plans is to have an agreed upon set of resiliency plan investment metrics with regulators that can be used to demonstrate the need and effectiveness of resiliency capital investments.
5. **Benefit-cost analysis is a commonly used measure to determine effectiveness** – Utilities typically must justify the amount of their spending request in resiliency plans to gain regulatory approval from regulators. The most common way this is done is by doing a Benefit-Cost Analysis (BCA) or other type of methodology to introduce quantifiable evidence that the benefits of investments can justify the costs. Failure to provide such quantifiable evidence may result in an amended resiliency plan, resulting in a lower amount of approved spend by a regulator or outright rejection of certain resiliency measures proposed.
6. **Reporting requirements commonly accompany utility resiliency investments** – Utilities typically report progress of resiliency investments as they are being deployed or on a periodic basis to regulators and other stakeholders. In addition, utilities typically report the status of how well the mitigation measures of the investments perform against the resiliency events they were deployed to mitigate after investments have been deployed. As a result, performance metrics of resiliency investments are made public and analyzed to determine how well resiliency measures mitigate resiliency events which informs future investment needs.
7. **Equity and environmental justice are considerations that some utilities are beginning to account for in resiliency planning** – Impact of resiliency investments on low-income customers, disadvantaged communities, and/or environmental justice communities is sometimes taken into consideration in jurisdictions researched for this report. In those jurisdictions, resiliency investments are generally deployed in a way to positively address the needs of low-income customers and disadvantaged communities while not being overly burdensome from a cost perspective.
8. **Protection against cybersecurity threats is an emerging area for utility resiliency planning** – Cybersecurity risk mitigation is a foundational area of risk management for electric utilities. Utilities in some jurisdictions include cybersecurity or other IT/OT as in-scope resiliency investments. In these jurisdictions, cybersecurity event risk is treated similar to weather event risk.

2. Introduction: Electric System Resiliency Planning Precedent in Other Jurisdictions

Over the past several decades, increased frequency and severity of extreme weather events has led to greater attention by electric transmission and distribution (T&D) utilities and their regulatory bodies on the need to build a more resilient electric system. Many electric utilities are making operational changes to improve the resiliency of their systems during and after extreme weather events, including increasing investment in resiliency-focused programs and projects. Further, the rising risk of physical security and cybersecurity threats has brought these emergent risks into the fold for electric utility resiliency planning and regulation.

Regarding electric sector resilience, the federal government has pursued a number of initiatives and executive orders, including the U.S. Department of Energy (DOE) Partnership for Energy Sector Climate Resilience and State and Local Energy Assurance Planning initiatives as well as the Federal Energy Regulatory Commission (FERC) and DOE joint effort to incentivize electric utility resilience planning.[1] The U.S. Department of Energy (DOE) has produced numerous resources related to resiliency planning for the electric sector, further demonstrating the increased emphasis on this topic at the national level.[2] Further, electric sector resiliency is a primary component of the Bipartisan Infrastructure Law that passed in late 2021 with $11 billion in grants available for states, tribes, and utilities to enhance resilience of electric infrastructure against disruptive events such as extreme weather and cyber attacks.[3] While the Electric Reliability Council of Texas (ERCOT) power region located solely in Texas is outside of FERC's jurisdiction, these examples provide useful context on how the broader U.S. is considering the importance of resiliency planning.

State governments are also taking action on electric utility resiliency. While each state in the U.S. faces unique climate conditions and associated resiliency risk, the trend of increased attention on extreme weather events and cybersecurity is seen across many different parts of the U.S. Examples of such efforts are identified in Table 3.

[1] MJ Bradley & Associates Issue Brief. (2020 February). *Key Considerations for Electric Sector Climate Resiliency Policy and Investments.* [MJB&A Issue Brief]. (p. 3). mjba_keyconsiderationsforclimateresiliencepolicyandinvestment.pdf (erm.com)

[2] U.S. DOE, Energy Resilience in the Public Sector. https://www.energy.gov/scep/slsc/energy-resilience-public-sector.

[3] U.S. DOE, DOE Fact Sheet: The Bipartisan Infrastructure Deal Will Deliver for American Workers, Families and User in the Clean Energy Future. https://www.energy.gov/articles/doe-fact-sheet-bipartisan-infrastructure-deal-will-deliver-american-workers-families-and-0

Table 3
Summary of Electric Utility Resiliency Activities by Jurisdiction[4]

State/ Territory	Utility	Description	Relevant Legislation	Relevant Regulatory Dockets
California	All investor-owned utilities (IOUs) and SCE	Various regulatory proceedings in California address resiliency including climate adaptation and vulnerability assessments (with focus on disadvantage communities), equity resilience maps.[5], physical risk assessment and mitigation plans for distribution assets, a DER framework that focuses on resilience value, funding for grid safety and resilience, wildfire mitigation plans, and interconnection processes, tariffs, and partnerships to support resilience projects like microgrids.[6] More recently, the state legislature established the Strategic Reliability Reserve Fund to help improve electric grid reliability and resiliency given climate change and increase in extreme weather events..[7]	Senate Bill (SB) 699 (2014) SB 901 (2018) SB 1339 (2018)	Rulemaking on Physical Security of Electrical Corporations Pursuant to Senate Bill 699 (Docket R.15-06-009) Rulemaking to Create a Consistent Regulatory Framework for the Guidance, Planning and Evaluation of Integrated DERs (Docket R. 14-10-003) Rulemaking to consider strategies and guidance for climate change adaption R.18-04-019 Application of SCE for approval of its Grid Safety and Resiliency Program (Docket A.18-09- 002) Rulemaking to Implement Electric Utility Wildfire Mitigation Plans Pursuant to Senate Bill 901 (Docket R.18-10-007) Rulemaking Regarding Microgrids Pursuant to Senate Bill 1339 and Resiliency Strategies (Docket R. 19-09- 009)
California	SDG&E	SDG&E has developed a flexible adaptation pathways framework with adjustable metrics to enable the utility to flexibly adjust the plan as new information is gathered.[8]	SB 379 (2015) SB 246 (2015)	CPUC Rulemaking 13-11-006
Connecticut	All IOUs	Regulatory proceedings in Connecticut have led to development of a framework for advancing equitable grid modernization and enhanced resilience through distribution system planning as well as targets and metrics to improve effectiveness of utility resilience programs..[9]	SB 7 (2018)	Investigation into Distribution System Planning of the Electric Distribution Companies (Docket 17-12-03) Resilience and Reliability Standards and Programs (Docket 17-12-03RE08)

[4] This table differs slightly from the list of jurisdictions reviewed in greater depth for the purpose of this report. This list was based on an initial broad scan of resiliency planning efforts in other jurisdictions. Specific jurisdictions were then selected for more in-depth research as listed in Table 1.

[5] U.S. Department of Energy Grid Modernization Laboratory Consortium. (2022 September). *Considerations for Resilience Guidelines for Clean Energy Plans For the Oregon Public Utility Commission and Oregon Electricity Stakeholders.* [Resilience Guidelines for Oregon]. (pp. 17-18, 24-25). Considerations for Resilience Guidelines for Clean Energy Plans (pnnl.gov)

[6] Pacific Northwest National Laboratories, Bosque Advisors, and Sandia National Laboratories. (2023 September). *Resilient Electric Grid: Defining Measuring, and Integrating Resilience into Electricity Sector Policy and Planning.* [PNNL report on Resilient Electric Grid]. (p. 12). Resilient Electric Grid (pnnl.gov)

[7] London Economics. (2023). (pp. 33-34). *Resilience in the electricity distribution sector and related policy questions.* [London Economics Resilience Report]. Project Documents | Distribution Sector Resilience, Responsiveness & Cost Efficiency | Engage with Us (oeb.ca)

[8] MJB&A Issue Brief. (p. 16).

[9] PNNL report on Resilient Electric Grid. (p. 12).

State/ Territory	Utility	Description	Relevant Legislation	Relevant Regulatory Dockets
Florida	All IOUs	Florida has a long history of leading in resilience planning, beginning in 1992 when the utility regulator developed its first storm cost risk mitigation plan for IOUs..[10] In 2017, the regulator conducted a review of electric utility preparedness and restoration activities to identify opportunities to improve resilience..[11] More recently, in 2019, legislation was adopted that requires utilities to submit an electric transmission and distribution storm protection plan on an annual basis looking outward 10 years.[12]	SB 796 (2019)	Review of Florida's Electric Utility Hurricane Preparedness and Restoration Actions (Docket 2017-0215-EU)
Hawaii	All IOUs	Several regulatory proceedings in Hawaii have considered resilience including: 1) grid modernization planning with a focus on resilience value of DERs, 2) a microgrid services tariff to increase resilience and reliability, and 3) an integrated grid planning effort informed by stakeholder engagement on resilience priorities..[13]	House Bill (HB) 2110 (2018)	HECO's Grid Modernization Strategy (Docket 2017-0226) Investigation into Establishment of a Microgrid Services Tariff Pursuant to House Bill 2110 (Docket 2018-01633) Investigation into Integrated Grid Planning (Docket 2018-0165)
Illinois	Commonwealth Edison and Ameren Illinois	Several regulatory proceedings have considered resilience including a microgrid proceeding that identified resilience benefits and development of resilience metrics as part of a broader set of performance metrics. Additionally, the utility has worked collaboratively with the City of Chicago since 2018 to identify opportunities for increased energy resilience. This included the co-development of the city's first resilience plan to include several goals related to building a more resilient energy system.[14] The Multi-Year Integrated Grid Plan (MYIGP) highlights a set of operating investments designed to meet customer expectations, achieve performance metrics, and support the objectives outlined in Section 16-105.17(d). The investments are driven by four priority areas for the Company's future electric grid vision: Safety and Reliability, Resiliency, Clean Energy Transition, and Customer Experience.[15]	Section 16-108.18(e) of the Public Utilities Act (220 ILCS 5/16-105.17) Sec. 16-105.17. MYIGP	Commonwealth Edison Company Petition Concerning the Implementation of a Demonstration Distribution Microgrid (Docket 17-0331) Commonwealth Edison Company Petition for the Establishment of Performance Metrics (Docket 22-0067) Order Requiring Commonwealth Edison to file an Initial Multi-Year Integrated Grid Plan (22-0486) Order Requiring Ameren Illinois Company to file an Initial Multi-Year Integrated Grid Plan (22-0487)
Massachusetts	Eversource	At the urging of the utility regulator, Eversource has pursued a number of climate mitigation and resilience strategies including investments in advanced technologies, a vegetation management resiliency pilot, a tree resilience program, and development of a Climate Adaptation Plan..[16]	N/A	Preparation and Response of National Grid to the October 29, 2017 Wind Storm (Docket 18-02)

[10] MJB&A Issue Brief. (p. 13).

[11] MJB&A Issue Brief. (p. 13).

[12] MJB&A Issue Brief. (p. 14).

[13] PNNL report on Resilient Electric Grid. (p. 12).

[14] MJB&A Issue Brief. (pp. 23-24).

[15] Ameren Illinois Multi-Year Integrated Grid Plan. (2023 January). (p. 9). https://www.icc.illinois.gov/docket/P2022-0487/documents/332988/files/580139.pdf

[16] MJB&A Issue Brief. (pp. 6-8).

811

State/ Territory	Utility	Description	Relevant Legislation	Relevant Regulatory Dockets
Michigan	DTE	Michigan Public Service Commission approved a rate increase for DTE Energy customers supporting its roadmap to improve reliability and resiliency. DTE's 2023 Distribution Grid Plan included investments aimed at improving reliability and resiliency, accelerating response to customer outages, and increasing grid capacity..[17]	N/A	Michigan Commission's motion for DTE Electric to develop and submit draft five-year investment and maintenance distribution plans (Case U-20147)
New Jersey	PSE&G	Regulator approved funding for hardening/modernizing electric and gas infrastructure to enhance resilience in response to Superstorm Sandy..[18]	Infrastructure Investment Program N.J.A.C. 14:3 2A (2018)	Petition of PSE&G for Approval of the Second Energy Strong New Jersey Program (Docket EO18060629) Value of DERs (Case 15-E-0751)
New York	Con Edison	Following Superstorm Sandy, regulator approved funding for storm hardening and resilience driven by a Storm Hardening and Resiliency Collaborative. DER valuation as part of the Reforming the Energy Vision initiative also considers resilience benefits..[19] More recently, the utility regulator ordered the utility to develop a Climate Change Vulnerability Study which included a Conceptual Resilience Management Framework for monitoring "signposts" that will inform the development of flexible solutions and further prioritization of assets and options to increase system-wide resilience..[20] As part of these efforts, Con Edison developed an analytical framework to evaluate resiliency investments including a risk assessment and prioritization model and cost-benefit analysis model..[21]	Subdivision 29 to Public Service Law 66 (2022)	Rates, Charges, Rules and Regulations of Con Edison for Electric Service (Case 13-E0030) Proceeding on Motion of the Commission in Regard to Reforming the Energy Vision (Case 14-M-0101) Proceeding on Motion of the Commission Concerning Electric Utility Climate Studies and Plans (Case 22-E-0222)
Puerto Rico	Puerto Rico Electric Power Authority	Regulatory proceedings that consider resilience include: 1) utility's integrated resource plan which considers resilience through DER investments and, 2) regulation on microgrid development..[22] In 2019, the Puerto Rico Grid Modernization Plan proposed investments in the following to promote resiliency: transmission and substations, distribution, generation and infrastructure, technology, and microgrids.[23]	N/A	Puerto Rico Electric Power Authority Integrated Resource Plan (Docket CEPRAP-2018-0001) Regulation om Microgrid Development (Regulation 9028)
South Carolina	All IOUs	To address lessons learned from Winter Storm Uri in 2021, regulator now requires utilities to assess extreme cold weather threats, impacts, vulnerabilities, and resilience solutions. [24]	N/A	Regarding Measures to Be Taken to Mitigate Impact of Threats to Safe and Reliable Utility Service (Docket 2021-66-A)

[17] Michigan PSC Case No: U-20147. (2023 September). [DTE 2023 Distribution Grid Plan]. (p. 13). *DTE 2023 Distribution Grid Plan.* 0688v00000A4YUXAA3 (site.com)

[18] PNNL report on Resilient Electric Grid. (p. 12).

[19] PNNL report on Resilient Electric Grid. (pp. 12-13).

[20] MJB&A Issue Brief. (pp. 8-10).

[21] London Economics Resilience Report. (pp. 21-27).

[22] PNNL report on Resilient Electric Grid. (p. 13).

[23] Autoridad de Energia Electricia and Central Office for Recovery, Reconstruction and Resiliency. The Grid Modernization of Puerto Rico. (p. 9). Grid Modernization for Puerto Rico (pr.gov)

[24] PNNL report on Resilient Electric Grid. (p. 13).

812

State/ Territory	Utility	Description	Relevant Legislation	Relevant Regulatory Dockets
Various Gulf Coast States	Entergy	Utility developed a "Building a Resilient Energy Gulf Coast Plan" that includes a cost-benefit analysis framework that incentivizes forward-looking resilience planning..[25]	N/A	N/A
Virginia	Dominion Energy	Utility developed a grid modernization plan that includes resilience measures such as intelligent grid devices, operations and automated control systems, and grid hardening..[26]	SB 966 (2018)	Petition of Dominion Energy Virginia for Approval of a Plan for Electric Distribution Grid Transformation Projects (Case PUR2018-00100)

[25] MJB&A Issue Brief. (p. 12).

[26] PNNL report on Resilient Electric Grid. (p. 13).

3. Distinction Between Resiliency and Reliability

A common issue regulatory jurisdictions have sought to address as resiliency-focused efforts have emerged in the electric utility industry is clearly defining the distinction between traditional reliability investments (e.g., routine pole replacement at end of useful life) and resiliency investments. Looking across how this is addressed in jurisdictions examined, resiliency generally refers to the ability of the electric grid to withstand and/or quickly recover from damages caused by extreme weather (including natural disasters), physical security and cybersecurity attacks, or other disruptive events. Reliability, on the other hand, generally refers to the ability of the electric grid to adequately serve load during normal operating conditions.

3.1 Electric grid "resiliency" definition examples

The following is a listing of example definitions of "resilience" or "resiliency" in different jurisdictions.

- **Connecticut:** Resilience is the ability of the distribution system to withstand and reduce the magnitude and/or duration of disruptive events which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event.[27]
- **Hawaii:** Resilience is the ability of a system or its components to adapt to changing conditions and withstand and rapidly recover from disruptions which can be interpreted as the ability to anticipate, absorb, adapt to, and rapidly recover from a catastrophic event.[28]
- **Louisiana:** Resilience shall mean a capability to anticipate, prepare for, respond to, and recover from significant multi hazard threats with minimal damage to social well-being, the economy, infrastructure, and the environment.[29]
- **New York:** Resilience is resistance of a utility's facilities to weather–induced failure or the ability to restore service following a weather-induced service outage.[30]
- **Oregon:** Resiliency is the ability of the system to prepare for and adopt to changing conditions and withstand and recover rapidly form disruptions, including the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.[31]
- **Utah:** Resiliency refers to operating through and recovering from a major disruption.[32]

[27] State of Connecticut Public Utilities Regulatory Authority. *Investigation into Distribution System Planning of the EDCs – Resilience and Reliability Standards and Programs*. (2022 August). (p. 35.) 171203RE08-083122.pdf (state.ct.us)

[28] Hawaiian Electric Resilience Working Group Recap Stakeholder Council Pre-Read. (2021 November). [Hawaiian Electric Resilience Working Group] (p. 3). https://www.hawaiianelectric.com/a/10002

[29] 2023 Louisiana Statewide Resilience Annual Report. (2023). [LA Resilience Report]. (p. 8). https://resilience.la.gov/media/5o0lgdit/statewide-resilience-report-final.pdf

[30] London Economics Resilience Report. (p. 22).

[31] U.S. Department of Energy Grid Modernization Laboratory Consortium. (2022 September). *Considerations for Resilience Guidelines for Clean Energy Plans For the Oregon Public Utility Commission and Oregon Electricity Stakeholders.* [Resilience Guidelines for Oregon]. (p. 6).

[32] PacifiCorp 2023 Integrated Resource Plan Volume 1. [PacifiCorp IRP]. (p. 115). 2023_IRP_Volume_I.pdf (pacificorp.com)

- **Vermont:** Resiliency is the ability to recover from certain types of disaster and failure, including remaining functional from the customer's perspective while recovering.[33]
- **Virginia:** A resilient grid is one that can self-heal and prevent cascading failure.[34]

3.2 Electric grid "reliability" definition examples

The following is a listing of example definitions of "reliability" used in some of the same jurisdictions where this distinction could be clearly identified.

- **Connecticut:** Reliability is the ability of the power system to deliver electricity in the quantity and with the quality demanded by users.[35]
- **Oregon:** Reliability is the ability of the system or its components to withstand instability, uncontrolled events, cascading failures, or unanticipated loss of system components.[36]
- **Vermont:** Reliability is about keeping the power on and the ability to deliver on the planned outcome to do so.[37]

[33] Green Mountain Power Final Climate Plan. [GMP Power Climate Plan]. (p. 4). GMP-Final-Climate-Plan-As-Approved.pdf (greenmountainpower.com)

[34] Sandia National Laboratories and Synapse Energy Economics. *The Resilience Planning Landscape for Communities and Electric Utilities.* (2021 April). [Sandia National Lab Report on Resilience Planning Landscape]. (p. 37). https://www.osti.gov/biblio/1782684

[35] State of Connecticut Public Utilities Regulatory Authority. Investigation into Distribution System Planning of the EDCs – Resilience and Reliability Standards and Programs. (p. 35).

[36] U.S. Department of Energy Grid Modernization Laboratory Consortium. (2022 September). *Considerations for Resilience Guidelines for Clean Energy Plans For the Oregon Public Utility Commission and Oregon Electricity Stakeholders.* [Resilience Guidelines for Oregon]. (p. 6).

[37] GMP Power Climate Plan. (p. 4).

4. Guidance on 'In-Scope" Resiliency Investments

Table 4 provides a summary table of types of resiliency investments that have been proposed or generally considered "in-scope" in other jurisdictions. The majority of jurisdictions researched include within scope similar types of distribution investment/programs (referred to as Resiliency Measures), such as pole replacement and hardening, that CenterPoint is proposing in its Resiliency Plan. Some of the jurisdictions also include transmission and cybersecurity investments similar to investments/programs proposed by CenterPoint.

Table 4
Summary of Types of Resiliency Investments Identified in Other Jurisdictions

	CT	FL	HI	LA	NJ	NY	OH	OR	VT	VA	MI	NC	GA	SC	IL
Pole Replacement / Hardening	X	X	X	X	X	X			X	X	X	X			X
Substation Flood Control			X	X	X	X			X			X	X	X	
Vegetation Management	X	X		X		X		X		X					X
Undergrounding Circuits	X		X	X	X	X			X	X	X	X	X		X
Substation Physical Security						X				X					
Transmission		X	X	X					X	X	X				X
Cyber Security										X	X				X
Other			DERs / Microgrid		Outage Mgmt. System Upgrade	DERs Microgrid	DERs/ Microgrid	DERs	Generation	Microgrid		Microgrid		Microgrid	

The following provides more specific detail on the types of resiliency investments proposed or otherwise identified as within scope in other state regulatory jurisdictions researched for this report:

- **Connecticut:** In-scope resiliency investments/programs include system hardening such as stronger wood poles, steel poles, fiberglass cross arms, converting bare wire to covered conductor, vegetation management, and underground circuits.[38]
- **Florida:** In-scope resiliency investments/programs include tree trimming, pole inspections and replacement, hardening of feeders and laterals, and undergrounding.[39]
- **Hawaii:** Areas identified within scope include: (1) enhanced vegetation management, particularly in critical grid areas susceptible to damage from wind and falling debris; (2) hardening and reinforcing critical transmission circuits including upgrading wind criteria and flood mitigation, upgrading structures, and using enhanced construction methods, and materials; and (3) expanding water resistant underground cables and re-locating equipment outside flood prone areas.[40]

[38] State of Connecticut Public Utilities Regulatory Authority. Investigation into Distribution System Planning of the EDCs – Resilience and Reliability Standards and Programs. (p. 57).

[39] Florida Public Service Commission Review of Electric Utility Hurricane Preparedness and Restoration Actions. (2018 June). [Florida PUC Review of Electric Utility Hurricane Preparedness]. (p. 9). https://www.floridapsc.com/pscfiles/library/filings/2018/04847-2018/04847-2018.pdf

[40] Hawaiian Electric Resilience Working Group. (p. 13).

- **Louisiana:** Entergy's 10-Year Resiliency Plan presents an infrastructure hardening plan specifically designed to improve overall system resilience over 10 years from 2024 to 2033. The 10-year $9.6 billion plan includes approximately 9,600 proposed distribution and transmission projects that will collectively harden more than 269,000 structures over 11,000-line miles as well as enhanced vegetation management.[41]
- **Michigan:** In-scope investments/programs in DTE's Roadmap to improved reliability (referred to as its Distribution Grid Plan) includes various infrastructure resilience and hardening efforts such as upgrading poles, transformers, and substation equipment. Additionally, underground system improvements and grid modernization and 4.8kV Hardening are included..[42]
- **New Jersey:** In-scope resiliency investments/programs include electric substation flood mitigation, contingency reconciliation, grid modernization communication systems, and grid modernization advanced distribution management system (ADMS) activities.[43]
- **New York:** Resilience investments are categorized into three areas: (1) Resilience-Driven Asset Investments, (2) Incorporation of Resilience Into Planning Design and Operations, and (3) Application of New Technologies.[44]
- **Ohio:** In-scope resiliency investments/programs include portable DERs and microgrids.[45]
- **Oregon:** In-scope resiliency investments/programs include system design/modeling, threat analysis, tree trimming, asset redesign, emergency drills, spare equipment, mutual aid agreements, customer-sited generation, and energy efficiency.[46]
- **Vermont:** In-scope resiliency investments/programs include generation projects, undergrounding and grid hardening.[47], transmission and distribution system projects, information technology / operational technology (IT/OT) systems, supervisory control and data acquisition (SCADA) software, geographic information systems (GIS), and microgrids.[48]
- **Virginia:** In-scope resiliency investments/programs include intelligent grid devices, operations and automated control systems, grid hardening (e.g., replace and rebuild targeted main feeder segments and implement new vegetation management programs),

[41] Entergy Future Resilience Filing One Pager. (2022 December). [Entergy Resilience Filing]. https://cdn.entergy-louisiana.com/userfiles/content/future/Resilience-filing-one-pager.pdf

[42] DTE 2023 Distribution Grid Plan. (pp. 13-14).

[43] New Jersey Board of Public Utilities PSE&G Approval of the Second Energy Strong Program (Energy Strong II). [NJ Board of Public Utilities PSE&G Program]. (p. 6). 9-11-19-2F.pdf (nj.gov)

[44] Con Edison Climate Change Resilience Plan 2023 November). [Con Edison Climate Change Resilience Plan]. (p. 22). Climate Change Resilience Plan (azureedge.net)

[45] Public Utilities Commission of Ohio. Application of Ohio Power Company for Authority to Establish a Standard Service Offer in the Form of an Electric Security Plan. (2023 December). [AEP Ohio Electric Security Plan Application]. (p. 15). ViewImage.aspx (state.oh.us)

[46] U.S. Department of Energy Grid Modernization Laboratory Consortium. (2022 September). *Considerations for Resilience Guidelines for Clean Energy Plans For the Oregon Public Utility Commission and Oregon Electricity Stakeholders.* [Resilience Guidelines for Oregon]. (p. V).

[47] Green Mountain Power Launches First in Nation 2030 Zero Outages Initiative. (2023 October). Green Mountain Power Launches First in Nation 2030 Zero Outages Initiative - Green Mountain Power

[48] GMP Power Climate Plan. (pp. 5-9).

telecommunications infrastructure, cyber and physical security, and predictive analytics.[49]

- **North Carolina:** In-scope resiliency investments include elevating electrical facilities, undergrounding equipment, and pole management.[50]
- **Georgia:** In-scope resiliency investments include elevating electrical facilities, undergrounding equipment, and microgrids.[51]
- **South Carolina:** In-scope resiliency investments include elevating electrical facilities and microgrids.[52]
- **Illinois**: In-scope resiliency investments include: pole replacement/hardening, vegetation management, undergrounding circuits, sub-transmission, and cyber security .[53]

Figure 1 below is an example of in-scope National Grid New York resiliency investments defined by project type and mitigated climate hazard.

[49] Dominion Petition to Virginia State Corporation Commission for Approval of a Plan for Electric Distribution Grid Transformation Projects. (2019 January). [Dominion Petition for Approval of Electric Distribution Grid Transformation Projects]. (p. 1). 4dv801!.PDF (virginia.gov)

[50] United States Government Accountability Office. Opportunities Exist for DOE to Better Support Utilities Improving Resilience to Hurricanes. (2021 March). (p. 8). GAO-21-274, ELECTRICITY GRID: Opportunities Exist for DOE to Better Support Utilities in Improving Resilience to Hurricanes

[51] United States Government Accountability Office. (p. 8).

[52] Ibid.

[53] Ameren Illinois Multi-Year Integrated Grid Plan. (2023 January). (pp. 105-130).

Figure 1
National Grid In-Scope Resiliency Investments[54]

Physical Project	Mitigated Climate Hazard	Description
1. Overhead Distribution and Sub-transmission Line Design Upgrades*	Wind Gusts and Ice	Update distribution line standards to move from Class 3 poles to Class 1 for main lines and poles that carry heavy equipment (approximately 8,000 poles/year) and update sub-transmission line standards to use Class 1 poles for single circuit structures, Class H1 for double circuit structures, and Class H2 for double circuit with distribution underbuilds (approximately 900 poles/year).
2. Overhead Transmission Line Design Upgrades*	Wind Gusts and Ice	Build T-Lines to withstand 120 mph wind gusts in high wind areas (46 currently planned) by using more steel and larger foundations. Planned projects include 44–115kV lines and 2–230KV lines (approximately 1,300 circuit miles covered).
3. Distribution Targeted Undergrounding	Wind Gusts and Ice	Targeted undergrounding of 1–2 miles per year of 3-phase main line in highest wind and icing areas.
4. Spare Transmission Line Structures	Wind Gusts and Ice	Purchase 10 T-Line spare structures per division (30 total) designed for 120 mph gusts to speed restoration.
5. Substation Flood Walls	Flooding	Install flood walls at 18 substations in high-risk areas (approximately 17,000 linear feet of flood walls total).
6. Distribution and Transmission Substation Transformer Specification Upgrades*	Extreme Heat	Update transformer spec from 32°C (90°F) to 35°C (95°F). Current plans include 35 distribution projects (81 transformers) and 24 transmission projects (37 transformers) with installs and replacements.

[54] National Grid Climate Change Resilience Plan. (2023 November). (p. 7). https://www.nationalgridus.com/media/pdfs/our-company/national-grid-climate-change-resilience-plan_2023.pdf

5. Magnitude Thresholds Used to Define Resiliency Events

"Magnitude threshold" with respect to resiliency events can have multiple meanings based on this jurisdictional research. For example, wind speed, hurricane category designation, level of flood, or type of cyber security event are specific measures or descriptions used to determine the magnitude of the event the utility is planning to withstand. Another meaning of "magnitude threshold" is the magnitude of the impact of a resiliency event with respect to the outcomes of a resiliency events such as loss of customer load, customer outages, restoration times, dollar amount of electric grid infrastructure damaged, and dollar amount of spend required for restoration efforts. For example, the Connecticut Event Level Matrix shown in Figure 2 categorizes the "magnitude threshold" (i.e., event level) of a resiliency event using multiple outcome-based criteria.

Figure 2
Connecticut Event Level Matrix[55]

Event Level	Customer Outages	Typical No. of Outage Orders	Typical No. of Non-Outage Orders	Typical Lineworker Needs at Storm Onset	Typical Lineworker Needs at Peak	Typical Restoration Duration
5 minor	less than 5,000	n/a	n/a	6 to 12	6 to 18	less than 12 hrs.
5 moderate	5,000 to 10,000	25 to 50	more than 50	12 to 18	106	12 to 24 hrs.
5	10,000 to 31,356	50 to 75	75 to 100	131 to 156	131 to 206	24 to 48 hrs.
4	31,356 to 95,799	75 to 400	100 to 500	156 to 206	156 to 206	2 to 5 days
3	95,800 to 159,967	400 to 1,000	500 to 1,000	216 to 271	216 to 556	5 to 7 days
2	159,967 to 223,549	1,000 to 2,000	500 to 1,000	271 to 436	271 to 646	7 to 9 days
1A	223,549 to 287,421	2,000 to 3,000	1,000 to 2,500	436 to 601	436 to 706	9 to 14 days
1	more than 287,421	more than 3,000	more than 2,500	601 to 1,096	601 to 1,206	more than 14 days

[55] State of Connecticut Public Utilities Regulatory Authority. Investigation into Distribution System Planning of the EDCs – Resilience and Reliability Standards and Programs. (p. 12).

Figure 3 and Figure 4 show examples of magnitude thresholds used in Hawaii as part of "threat scenarios" tied to the type of weather-driven or human threat considered. Figure 5 shows thresholds used in National Grid's Climate Change Resilience Plan for New York.

Figure 3
Hawaii Magnitude Threshold Examples for Weather-Driven Threat Events.[56]

Threat Scenario: Hurricane, Wind, Flood
O'ahu, Hawai'i Island, and Maui County

- Moderate
  - Category 2
  - 96-110 mph winds
  - 10 foot storm surge
  - Coastal infrastructure damage
  - Damage to distribution lines and poles due to wind, falling trees/branches, and flying debris
  - 5-8% of transmission circuits have sustained outage and restored in 3-7 days
  - 20-30% of distribution circuits out and restored in 1-4 weeks
  - Roads cleared 3-4 days
  - Fuel supply available within 3-4 days
- Severe
  - Category 4
  - 130-156 mph winds
  - 20' storm surge
  - Coastal infrastructure destroyed
  - Damage to transmission lines, poles and towers due to wind, falling trees/branches, and flying debris
  - 25-30% of transmission lines have sustained outage and restored over four months
  - 50-75% of distribution lines out of service and restored over four months
  - Fuel resupply available after four weeks

Figure 4
Hawaii Magnitude Threshold Examples for Human Threat Events.[57]

Threat Scenario: Physical/Cyber Attack
O'ahu, Hawai'i Island, and Maui County

- Moderate
  - Most critical substation sustains physical damage from high powered rifles and several explosive devices
  - 50% of transformers can be repaired within two weeks
  - 50% of transformers are permanently damaged and require 12-18 months for permanent replacement
  - Lines and switchgear can be repaired in two to six weeks
- Severe
  - Two most critical substations sustain physical damage from high powered rifles and several explosive devices
  - 50% of transformers can be repaired within two weeks
  - 50% of transformers are permanently damaged and require 12-18 months for permanent replacement
  - Lines and switchgear can be repaired in two to six weeks
  - Cyber attack disables control center situational awareness and primary voice communications for 8 hours

[56] Hawaiian Electric Integrated Grid Planning: Resilience Working Group Meeting. (2019 October). [Hawaiian Electric Integrated Grid Planning: Resilience Working Group]. (p. 35). https://www.hawaiianelectric.com/a/6949

[57] Ibid.

Figure 5
New York National Grid Climate Change Resilience Plan Resiliency Thresholds[58]

Operational Project/Program	Mitigated Climate Hazard(s)	Applicable Asset Type	Description
1. Substation Transformer Specification Changes	Extreme Heat	Substations	Due to increasing ambient average and maximum temperatures, transformer specifications will be updated from 32°C (90°F) to 35°C (95°F) for future builds.
2. Update Transmission Structure Standards	Wind Gusts	Transmission	Update transmission structure design guidelines to withstand wind gust projections of up to 120 mph based on structure locations and wind gust maps derived from Massachusetts Institute of Technology (MIT) wind speed projection data.
3. Electric Load Forecasting	Extreme Heat	Distribution	Evaluate climate scenarios in the load forecasting practice.
4. Transmission Facility Rating Methodology Changes	Extreme Heat	Transmission	Update transmission facility rating methodology ambient temperature from present assumption of 35°C (95°F) to 40°C (104°F). Revised facility ratings will be incorporated into transmission system models and used in planning studies.

[58] National Grid Climate Change Resilience Plan. (p. 7).

6. Criteria Used to Identify Need for Resiliency Investments

Many states where electric utilities are active in resiliency planning have defined sets of criteria or metrics to determine which projects qualify and why. In some cases, these criteria or metrics are also used to track performance of the measures over time, the topic of the next section of this report. Table provides an overview of the types of metrics, both qualitative and quantitative, that regulators and utilities are using to justify investments.

Table 5
Summary of Common Metrics by State

Criteria	CA	UT	OH	NY	HI	VT	OR	WA	CT	LA
Indirect/Societal Impact				X	X	X	X		X	
Customer Outage Time/Metric			X	X			X	X	X	X
Natural Hazard/Land Modeling		X								
Qualitative Measures	X		X	X	X	X				

Electric utilities in California and Utah use qualitative and quantitative considerations metrics for wildfire mitigation and vegetation management programs. For example, SCE, in seeking approval of its Grid Safety and Resiliency Program, included an independent Tree Removal Study by an outside consulting firm to evaluate the need and effectiveness of its current "Tree Calculator" tool for determining where tree removal should be targeted to reduce wildfire risks..[59] PacifiCorp, also for the purpose of reducing wildfire risk, implemented a fire threat classification for specific conditions and established goals for increased inspection frequencies in high-risk locations and reduction of correction timeframes for fire threat conditions..[60] Due to rising threats in Utah, Rocky Mountain Power created a new Fire High Consequence Area (FHCA) rebuild program and justified it by claiming that a comprehensive approach will be the most efficient way to upgrade all equipment on a line at one time and make it more resilient against wildfires. All lines included in the rebuild must be partially in the FHCA, and they use the age of poles as a metric for which are hand-selected for rebuild based on local knowledge of the infrastructure..[61]

AEP Ohio has used a measure of aging equipment on electric lines as an indicator of need..[62]

Other electric utilities such as Con Edison, Green Mountain Power, and HECO, have taken a similar approach to California electric utilities to evaluate resiliency investments that consider their unique risk profile. These utilities use a mix of qualitative and quantitative metrics that help identify investments that avoid the largest number of outages, enhance safety, and/or have the

[59] California PUC Application of Southern California Edison Company for Approval of Its Grid Safety and Resiliency Program. (2020 April). [SCE Approval of Grid Safety and Resiliency Program]. (p. 24). 334734573.PDF (ca.gov)

[60] PacifiCorp IRP. (p. 133).

[61] Rocky Mountain Power Utah Wildland Fire Protection Plan to Utah PSC. (2020 June). [Rocky Mountain Power Fire Protection Plan]. (p. 55). 20-035-28_RMP_Wildland_Fire_Protection_Plan.pdf (rockymountainpower.net)

[62] AEP Ohio Electric Security Plan Application. (p. 11). ViewImage.aspx (state.oh.us)

greatest impact on critical load customers. HECO is an example where a stakeholder process was established to determine resiliency investment qualification criteria by forming a Resiliency Working Group. Qualification criteria developed through this process include:

- Reduce the likelihood of power outages during a severe event
- Reduce the severity and duration of any outages that do occur during and after a severe event
- Reduce restoration and recovery times following a severe event
- Reduce critical infrastructure customers' power rapidly to enable mutual support and recovery during an emergency
- Return all customers to service within appropriate times
- Limit environmental impacts of a severe event.[63]

Additionally, some utilities such as HECO incorporate the "Bowtie Method" Risk- Threat Assessment process to determine specific prevention and mitigation solutions (see Figure 6).

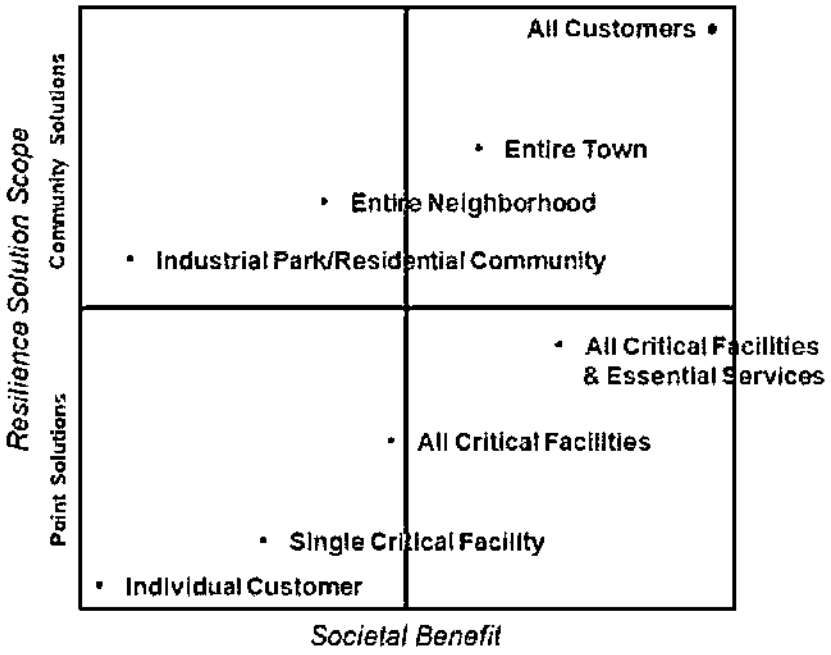
Figure 6
"Bowtie Method" Risk-Threat Assessment[64]

Hawaiian Electric the considers risk mitigation solutions identified through this process into a Resilience Solution Portfolio. The matrix shown in Figure 7 shows how the utility evaluates the options with consideration of scope and potential customer benefits.

[63] Hawaiian Electric Resilience Working Group. (p. 4).

[64] Hawaiian Electric IGP Resource Adequacy Workplan and Finalized Grid Needs Methodology. (2022 September). [Hawaiian Electric IGP Resource Adequacy Workplan]. (p. 241). IGP Resource Adequacy Workplan and Finalized Grid Needs Methodology (hawaiianelectric.com)

Figure 7
Resilience Solution Portfolio[65]



Source: De Martini for PNNL

A more data-centric approach has been taken by some jurisdictions/utilities to determine the value of resiliency investments, focusing primarily on calculating customer benefits and outage times. For example, PacificCorp and Avista have begun using the metric "Customers Experiencing Multiple Sustained and Momentary Interruptions" (CEMSMI) to measure reliability and resiliency needs..[66] CEMSMI measures the number of customers experiencing more than a certain number of interruptions a year, including both momentary and sustained outages. Another example is the Louisiana Public Service Commission's Storm Resilience Model which calculates the customer benefit of hardening projects through reduced utility restoration costs and impacts to customers measured by customer minutes interrupted (CMI). The Louisiana Commission prioritizes hardening projects with the highest resilience benefit per dollar invested into the system, determining funding levels based on this measure of customer benefits..[67] Figure 8 shows the resiliency framework used by the Connecticut Public Utilities Regulatory Authority (Connecticut PURA) established for electric distribution companies to model performance and implement their reliability-based and resilience-based capital programs..[68]

[65] Hawaiian Electric IGP Resource Adequacy Workplan (p. 242)

[66] U.S. Department of Energy Grid Modernization Laboratory Consortium. (2022 September). *Considerations for Resilience Guidelines for Clean Energy Plans For the Oregon Public Utility Commission and Oregon Electricity Stakeholders.* [Resilience Guidelines for Oregon]. (p. 23).

[67] Entergy New Orleans Application for Approval of Future Ready Resilience Plan (Phase 1). [Entergy Future Ready Resilience Plan]. (April 2023). Resilience Investment and Benefits Report (p. 7). Resilience-filing-4-17-2023.pdf (entergy-neworleans.com)

[68] State of Connecticut Public Utilities Regulatory Authority. Investigation into Distribution System Planning of the EDCs – Resilience and Reliability Standards and Programs. (p. 61).

Figure 8
Criteria to Identify and Prioritize Vulnerable Zones.[69]

Criteria	Category	Rank
All-in SAIDI (for last four years)	Outage-based	Primary
All-in SAIFI (for last four years)		Secondary
All-in CAIDI (for last four years)		
Major Storm-only SAIDI		
Major Storm-only SAIFI		
No. of Customers per Zone	System Characteristics	
Mainline length		
Density and Type of Vegetation		
Feeder Type: Backbone or Lateral		
Feeder ties		
Site Access Difficulty (e.g., hard to access right-of-ways)		
Municipal Priorities including Blocked Roads	Community Priorities	
No. of Commercial and Industrial Customers per Zone		
Located in Distressed Municipality		
Located in Environmental Justice Community		
No. of Life Support Customers		

Green Mountain Power, for substation upgrades and investments, used floodplain modeling and analysis, considering 100-year and 500-year flooding events to determine which facilities should be relocated or rebuilt at higher elevation at the same site. Projects are being prioritized if they are needed to address 100-year floodplain levels or have a history of flooding, with additional prioritization given to substations serving a higher number of customers. For resiliency investments related to electric distribution circuit performance improvements, the utility uses criteria to rank circuits based on the magnitude of the impact grid hardening investments will have in terms of number of customers and load served. The project prioritization is then based on a combination of a static assessment of these criteria paired with the local experience of field resources and consideration of the ratio of capital dollars spent to customer hours out for each project..[70]

Lastly, Figure 9 shows resilience metrics identified by the Grid Modernization Laboratory Consortium for the Oregon Public Utilities Commission based on its own benchmarking analysis. These were proposed to aid the resilience analysis process, including helping to characterize threats and consequences..[71]

[69] Ibid.

[70] GMP Power Climate Plan. (p. 7).

[71] U.S. Department of Energy Grid Modernization Laboratory Consortium. (2022 September). *Considerations for Resilience Guidelines for Clean Energy Plans For the Oregon Public Utility Commission and Oregon Electricity Stakeholders.* [Resilience Guidelines for Oregon]. (p. 5).

Figure 9
Consequence Categories for Consideration in Developing Resilience Metrics[72]

Consequence Category	Resilience Metric
Direct	
Electrical Service	Cumulative customer-hours of outages
	Cumulative customer energy demand not served
	Average number (or percentage) of customers experiencing an outage during a specified time period
Critical Electrical Service	Cumulative critical customer-hours of outages
	Critical customer energy demand not served
	Average number (or percentage) of critical loads that experience an outage
Restoration	Time to recovery
	Cost of recovery
Monetary	Loss of utility revenue
	Cost of grid damages (e.g., repair or replace lines, transformers)
	Cost of recovery
	Avoided outage cost
Indirect	
Community Function	Critical services without power (e.g., hospitals, fire stations, police stations)
	Critical services without power for more than *N* hours (e.g., *N*> hours of backup fuel requirement)
Monetary	Loss of assets and perishables
	Business interruption costs
	Impact on Gross Municipal Product or Gross Regional Product
Other Critical Assets	Key production facilities without power
	Key military facilities without power

[72] Ibid.

7. Methods Used to Determine Cost-Effectiveness of Resiliency Investments

Cost-benefit, or benefit-cost, analyses (CBA/BCA) are the most commonly used practice for determining cost-effectiveness of resiliency investments. Electric utilities across various jurisdictions use this method to measure projected costs against estimated avoided costs. Examples of electric utilities using CBA/BCA for resiliency planning include:

- **Duke Energy:** Used CBA to justify their multiyear rate plan (MYRP) for resiliency-focused transmission projects..[73]
- **Entergy New Orleans:** Resiliency filing used a Storm Resilience model to calculate the resilience costs and estimated benefits of hardening assets in terms of avoided customer minutes interrupted and avoided future storm restoration costs..[74]
- **Dominion**: Ran into challenges with getting regulatory approval for grid hardening investments after the Virginia utility commission found that certain programs only benefited 4.3% of Dominion's customer base. Cost-effectiveness was measured as the overall customer impact relative to cost..[75]
- **Con Edison:** At the direction of the New York Public Service Commission, Con Ediso a CBA approach for resiliency investments using two models: 1) a risk assessment and prioritization model to measure resiliency efforts in terms of risk reduced per dollar spent, and 2) a CBA model that calculates the risk reduction value of resiliency projects..[76] The models included the following components:
    - Location-specific information regarding high-rise residential buildings
    - Location-based flood probabilities combined with asset elevation data
    - Wind damage probabilities from historical wind gust frequency distributions
    - Data on heat wave events
    - Storm hardening project costs
    - Projected outage durations
    - Estimates of asset risk pre-hardening and post-hardening in terms of changes to damage probability or outage duration

Figure 10 and Figure 11 show defined categories of costs and benefits of resilience investments identified by the Grid Modernization Laboratory Consortium in the report they prepared for the Oregon Public Utilities Commission to help them establish prudent industry resiliency standards for Oregon investor-owned utilities.

[73] Application of Duke Energy for Adjustment of Rates and Charges (MYRP) to the North Carolina utilities Commission. (2023 March). [Duke Energy MYRP Application]. (p. 68). ViewFile.aspx (ncuc.gov)

[74] Entergy New Orleans Application for Approval of Future Ready Resilience Plan (Phase 1). [Entergy Future Ready Resilience Plan]. (April 2023). Resilience Investment and Benefits Report (p. 7).

[75] Dominion Petition for Approval of Electric Distribution Grid Transformation Projects. (p. 14).

[76] London Economics Resilience Report. (p. 22).

Figure 10
Categories of Costs of Resilience Investments.[77]

Type	Impact	Utility System	Host Customer	Community	Society[28]
Project Implementation	Installation, Operation, and Maintenance	X	X	X	
	Transaction	X	X	X	
	Interconnection	X	X	X	
	Financial Incentives	X			X
	Program Administration	X			
	Utility Performance Incentives	X			

Figure 11
Potential Benefits of Resilience Investments.[78]

Type	Impact	Utility System	Host Customer	Community	Society [31]
Generation, Transmission & Distribution, Energy and Capacity	Reducing Emergency Staff Deployment Costs	X			
	Avoiding Energy Infrastructure Damages	X			
Non-Energy: Economic[32]	Avoiding Damages to Goods and Infrastructure		X	X	X
	Avoiding Lower Revenues from Lower Production and Fewer Sales of Goods and Services		X		X
	Reducing Emergency Staff Deployment Costs		X	X	
	Avoiding Departure of Customers Important to the Community			X	
	Avoiding Lost Economic Development, Education, and Recreation Opportunities			X	X
Non-Energy: Public Health, Safety, and Security	Reducing Medical and Insurance Costs	X	X	X	X
	Avoiding Loss of Quality of Life	X	X	X	X

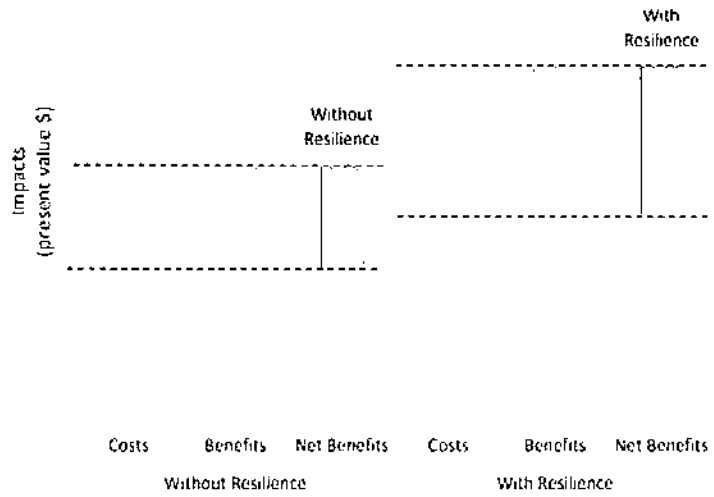
Another example of the concept of CBA/BCA being used for resiliency planning is illustrated in Figure 12, which shows how a battery system can help avoid upgrades to the electric utility's transmission and distribution system. The report where this example was provided summarizes

[77] U.S. Department of Energy Grid Modernization Laboratory Consortium. (2022 September). *Considerations for Resilience Guidelines for Clean Energy Plans For the Oregon Public Utility Commission and Oregon Electricity Stakeholders.* [Resilience Guidelines for Oregon]. (p. 35).

[78] Ibid.

that the battery when covered with concrete is protected from hurricane damages, and that "the benefits exceed the costs, with and without the resilience components"..[79]

Figure 12
BCA With and Without Resilience Costs and Benefits.[80]



As an alternative to the traditional CBA/BCA model, HECO and SCE are example utilities that use a risk-spend efficiency (RSE) metric to define the BCA ratio of resilience risk reduction solutions. The benefit is expressed in terms of the magnitude of risk reduction while the costs represent the mitigation expenses (capital and O&M) associated with the project or program (see calculation below, including Figure 13 which shows a summary of the calculation). This process begins with assessing solution value in terms of community and customer resilience risk reduction measured in customer minutes of interruption (CMI) avoided over the planning horizon..[81] The utility then uses the RSE scores to develop a prioritized solutions list within a defined budget.

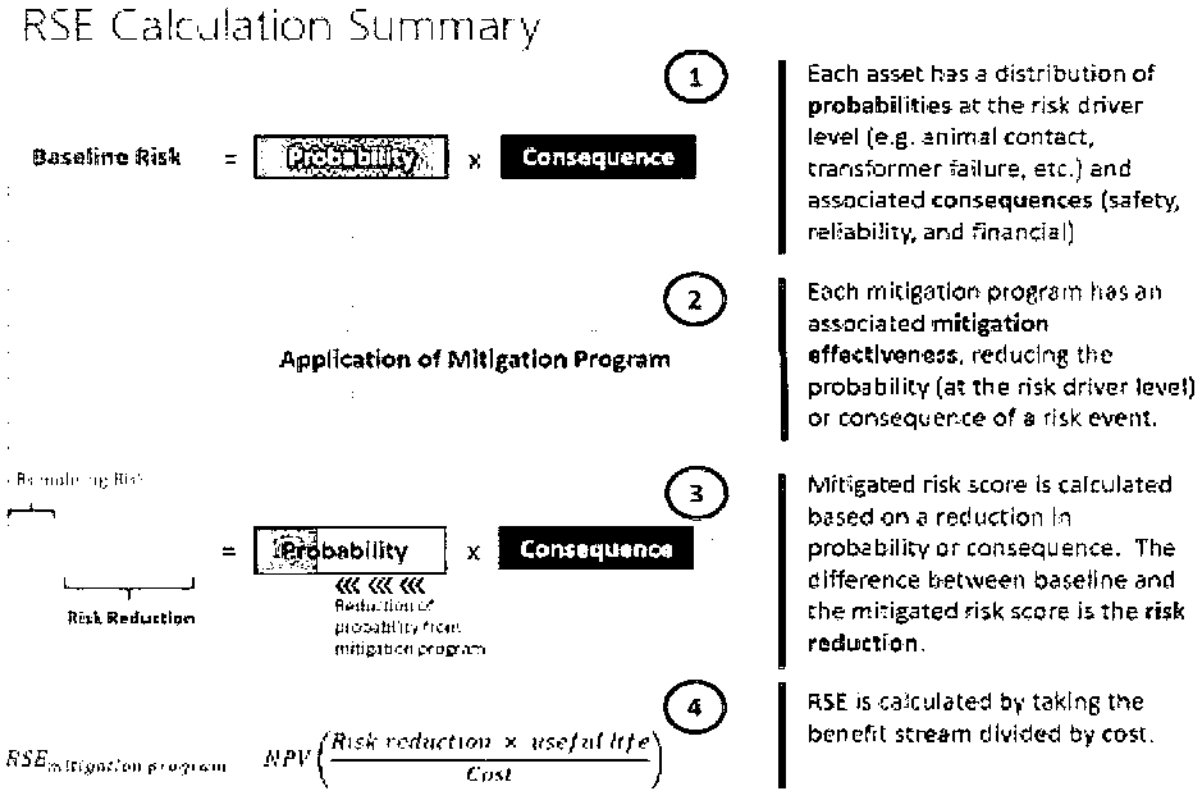
$$\text{Risk Spend Efficiency} = \frac{Risk\ Reduction * Number\ of\ Years\ of\ Expected\ Risk\ Reduction}{Total\ Mitigation\ Cost\ (in\ thousands)}$$

[79] U.S. Department of Energy Grid Modernization Laboratory Consortium. (2022 September). *Considerations for Resilience Guidelines for Clean Energy Plans For the Oregon Public Utility Commission and Oregon Electricity Stakeholders.* [Resilience Guidelines for Oregon]. (p.36)

[80] Ibid.

[81] U.S. Department of Energy Grid Modernization Laboratory Consortium. (2022 September). *Considerations for Resilience Guidelines for Clean Energy Plans For the Oregon Public Utility Commission and Oregon Electricity Stakeholders.* [Resilience Guidelines for Oregon]. (p. 39).

Figure 13
Risk Spend Efficiency Calculation Summary[82]



[82] Ibid.

8. Reporting Requirements

Electric utility resiliency plans approved by state regulatory commissions typically require continued reporting of metrics against the timeline of capital deployment to demonstrate the effectiveness of the capital deployment on mitigating the impact of resiliency events. Con Edison, for example, developed its Climate Resiliency Plan Investment Performance Metrics to track the effectiveness of investments and the implementation of programs..[83] This includes tracking both outcome-based and implementation-based resilience measures on a biennial basis. The outcome-based measures attempt to assess the overall effectiveness of the Company's Resilience Plan while implementation-based measures help assess progress over time using a more traditional project management approach. Categories of outcome-based measures considered include: impact of major storms, network distribution system resiliency, non-network distribution system resiliency, outage communications, and emergency preparedness). Measures are subject to change over time as more peer reviewed and benchmarked measures become widely accepted in the utility industry.

For example, Con Edison will meets with stakeholders at least twice per year and reports every other year on the performance measures and status of resiliency investments..[84] The monitoring and reporting identifies lessons learned about the effectiveness of resilience investments which can be used to determine the need of future investments..[85] Figure 14 shows an example of how resiliency investments are reported by Con Edison as they are being deployed to track project status.

Figure 14
National Grid Project Implementation Reporting Example.[86]

Project Name	Completion Date (Estimated)	Completion Date (Actual)	Planned Cost[34] ($K)	Cost to Date ($K)
Targeted Undergrounding	03/31/2045	In progress	$50,500	$30,000
Spare Transmission Structures	12/21/2026	11/21/2026	$1,500	$1,350
Sugar Hill Station – Transformer upgrade	3/31/2030	Planned	$1,467 ($186)[35]	$800
Transmission Substations Flood Mitigation Program	3/31/2045	In Progress	$16,100	$300
South Oswego to Lighthouse Hill – Transmission line upgrade	11/21/2027	12/21/2027	$960 ($30)	$990

[83] Con Edison Climate Change Resilience Plan. (p. 62).

[84] Con Edison Climate Change Resilience Plan. (p. 5).

[85] Ibid.

[86] National Grid Climate Change Resilience Plan. (p. 46).

9. Requirements Related to Equity and Environmental Justice Communities

An important indicator of an effective electric utility resiliency plan is how widespread the customer benefits are shared. In some jurisdictions, the impact to disadvantaged and marginalized communities (or similar terms used) are emphasized by utility regulators. For example, the California Public Utilities Commission and Washington Utilities and Transportation Commission have begun to require utilities to individually map vulnerable communities in their service territories, and to include them in future climate change assessments and clean energy implementation plans..[87] Another example, on a more local level, is the City of Norfolk Virginia which developed a resilience strategy in partnership with the electric utility that targets funding related to hurricane defense and flood risk adaptation, including special focus on neighborhood resilience, which is a targeted area to alleviate poverty in the city and connect communities..[88]

As another example of equity considerations being made, Con Edison's Climate Change Resilience Plan explains how equity is incorporated into their planning process by tracking the impact of outages in disadvantaged communities relative to impacts in other areas of their system. Additionally, the utility is working with stakeholders such as the NYC Mayor's Office of Climate and Environmental Justice to provide support to vulnerable areas..[89] In addition, the company has formed an Environmental Justice Working Group under an executive committee, with a plan to release a finalized Environmental Justice Policy Statement to apply an equity lens to resilience-driven investments..[90] Key components of the policy statement include:

- Operations will not disproportionately burden Disadvantaged Communities (DACs)
- Con Edison will work to understand DAC concerns
- Clean energy investments will benefit DACs
- Con Edison will provide opportunities for employment in their clean energy future.[91]

National Grid in New York also takes equity and environmental justice into consideration with respect to resiliency investments. National Grid considers how disadvantaged communities may be disproportionately affected by climate change and what they can do to enhance resilient service to those communities..[92] National Grid recognizes the central role of equity in resilience planning and is committed to ensuring equity is appropriately incorporated during investment planning..[93]

---

[87] U.S. Department of Energy Grid Modernization Laboratory Consortium. (2022 September). *Considerations for Resilience Guidelines for Clean Energy Plans For the Oregon Public Utility Commission and Oregon Electricity Stakeholders.* [Resilience Guidelines for Oregon]. (p. V).

[88] Sandia National Lab Report on Resilience Planning Landscape. (p. 37).

[89] Con Edison Climate Change Resilience Plan. (p. 4).

[90] Con Edison Climate Change Vulnerability Study. (2023 September). (p. 16). https://www.coned.com/-/media/files/ConEd/documents/our-energy-future/our-energy-projects/climate-change-resiliency-plan/climate-change-vulnerability-study.pdf?la=en

[91] Ibid.

[92] National Grid Climate Change Resilience Plan. (p. 15).

[93] National Grid Climate Change Resilience Plan. (p. 16).

10. Consideration of IT, OT, and Cybersecurity Resiliency Investments

Green Mountain Power is an example of a utility that has developed criteria for pursuing IT resiliency investments with the goal of keeping their existing data centers and control centers reliable and efficient. The utility's investment requirements include:.[94]

- **Projects for failover systems:** Selection is based on the ability to provide enhanced levels of redundancy and resiliency to key operational systems that could more easily succumb to extreme weather-related impacts in their current configuration, or those that are critical to customer restorations during extreme weather events
- **Communications projects:** Selected based upon the ability to provide an additional platform for stakeholder and emergency response information and resource sharing with the utility

Additionally, the utility stated that programs will be concentrated in the following three key areas:

1. Projects that improve the resiliency and durability of communications infrastructures that manage and provide telemetry for grid operations
2. IT projects focused on increasing the uninterrupted functionality and durability of key application infrastructures and devices necessary to serve their customers, including their Outage Management System (OMS), SCADA, and GIS
3. Projects that enhance communication and coordination efforts with municipalities, first responders, and customers during severe weather events

Examples of cybersecurity considerations in utility resiliency planning efforts include:

- **Duke Energy North Carolina**: Multi-year rate plan includes cybersecurity monitoring as a key requirement in resiliency investments to increase protection against attacks.[95]
- **SCE:** Application for approval of its Grid Safety and Resiliency Program was criticized by small business advocates who had concerns about privacy with publicly available weather information and lack of cybersecurity technology.[96]
- **Dominion Energy Virginia:** In 2023, the Virginia regulator approved the utility's Phase 3 Electric Grid Transformation Projects, which included investments in advanced metering infrastructure, a customer information platform, voltage optimization enablement, a DER management system and outage management system, and a non-wires alternative pilot..[97]
- **Ameren Illinois:** The expected increase in the number of sensors, potential control points, and reliance on public networks will increase the attack surface for nefarious activities by hackers. As devices proliferate, so does the utility's reliance on monitoring

[94] GMP Power Climate Plan. (p. 7).

[95] Duke Energy MYRP Application. (p. 72).

[96] SCE Approval of Grid Safety and Resiliency Program. (p. 13).

[97] 50 States of Grid Modernization Q1 2022 Quarterly Report Executive Summary. NC Clean Energy Technology Center. (2022 April). (p. 6). Q12022_gridmod_exec_final.pdf (ncsu.edu)

their state and potentially controlling their performance to maintain reliability and resilient grid conditions..[98]

[98] Ameren Illinois Multi-Year Integrated Grid Plan. (p. 98).

Appendix B: BCA Sensitivity Analysis for VOLL: $5,000/MWh to $65,000/MWh

Resiliency Measure	Capital Cost ($MM)	O&M Cost ($MM)	BCA (VOLL: $5,000/ MWh)	BCA (VOLL: $9,000/ MWh)	BCA (VOLL: $25,000/ MWh)	BCA (VOLL: $65,000/ MWh)
System Hardening						
Transmission System Hardening	$376.0	$0.75	1.2	2.1	6.0	15.5
S90 Tower Replacements	$103.8	$0.00	1.0	1.8	4.9	12.8
69kV-138kV Conversion Projects	$268.4	$0.00	0.4	0.7	1.9	5.0
Coastal Resiliency Upgrades	$259.0	$0.75	0.3	0.5	1.4	3.7
Substation Transformer Fire Protection Barriers	$2.4	$0.00	1.0	1.5	3.7	9.1
Distribution Pole Replacements/Bracing	$99.3	$0.00	1.4	2.4	6.2	15.9
Distribution Resiliency – Circuit Rebuilds	$312.8	$0.00	1.9	2.9	7.0	17.2
Strategic Undergrounding/Freeway Crossings	$31.2	$0.00	1.1	1.7	3.8	9.1
System Hardening Subtotal	**$1,452.9**	**$1.50**	**1.0**	**1.7**	**4.5**	**11.5**
Grid Modernization						
Trip Saver®	$58.9	$0.03	13.5	23.0	61.3	156.95
IGSD Installation	$53.8	$0.82	3.2	5.7	15.7	40.9
Texas Medical Center Substation	$102.0	$0.15	0.1	0.3	0.7	1.9
Grid Modernization Subtotal	**$214.7**	**$1.00**	**5.8**	**9.1**	**22.4**	**55.4**
Flood Control						
Substation Flood Mitigation	$30.6	$0.00	1.7	2.9	7.5	19.2
Control Center Facility Upgrades	$7.0	$0.00	3.0	4.9	12.5	31.3
Flood Control Subtotal	**$37.6**	**$0.00**	**1.9**	**3.2**	**8.4**	**21.4**
Information Technology for Operations						
Advanced Aerial Imagery Platform/Digital Twin	$9.9	$0.06	0.6	1.2	3.4	8.9
Advanced Distribution Technology	$225.8	$15.00	0.1	1.0	4.8	14.3
Digital Substation	$25.0	$(0.60)	0.6	1.0	1.9	4.4
IT for Operations Subtotal	**$260.7**	**$14.46**	**0.3**	**1.1**	**4.6**	**13.2**
System Security						
Substation Physical Security Fencing	$15.0	$0.00	3.2	5.7	15.6	40.3
Substation Security Upgrades	$19.5	$0.09	3.6	6.9	19.9	52.5
System Security Subtotal	**$34.5**	**$0.09**	**3.5**	**6.4**	**18.0**	**47.2**
Vegetation Management						
Targeted Critical Circuit Vegetation Management	$0.0	$12.00	0.4	0.7	1.8	4.5
Group Subtotal	**$0.0**	**$12.00**	**0.4**	**0.7**	**1.8**	**4.5**
Totals	**$2,000.4**	**$42.05**	**1.4**	**2.4**	**6.6**	**17.2**

*Average BCA weighted by resiliency measure cost

Source: Guidehouse BCA of CenterPoint Houston's proposed resiliency measures

EXHIBIT ELS-3
Glossary of Acronyms

ADT	Advanced Distribution Technology
AMS	Advanced Meters
AOC	Addicks Operation Center
BCA	Benefit Cost Analysis
CenterPoint Houston or the Company	CenterPoint Energy Houston Electric, LLC
Commission	Public Utility Commission of Texas
CMI	Customer Minutes Interrupted
CNP	CenterPoint Energy, Inc.
DEM	Digital Elevation Model
DI Apps	Distributed Intelligent Applications
ERCOT	Electric Reliability Council of Texas
GCMs	Global Climate Models
ICC	Illinois Commerce Commission
IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronics Engineers
IGSD	Intelligent Grid Switching Device
kV	kilovolt
Mph	Miles per Hour
NASA	National Aeronautics and Space Administration
NCEI	National Center for Environmental Information
NESC	National Electrical Safety Code
NJBPU	New Jersey Board of Public Utilities
NOAA	National Oceanic and Atmospheric Administration
O&M	Operations and maintenance
OT	Operational Technology
PMR	Pole Mounted Router
Resiliency Event	A low frequency, high impact event that, if not mitigated, poses a material risk to the safe and reliable operation of the Company's transmission and distribution system.
Resiliency Measure	A measure designed to mitigate the risks posed to the Company's transmission and distribution system by a Resiliency Event
SAIDI	System Average Interruption Duration Index
Service Company	CenterPoint Energy Service Company, LLC
T&D	Transmission and Distribution
TDEM	Texas Department of Emergency Management
TMC	Texas Medical Center
UFLS	Under-frequency load shedding
VM	Vegetation Management
VOLL	Value of Lost Load

DOCKET NO. 56548

APPLICATION OF CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC FOR APPROVAL OF ITS RESILIENCY PLAN	**§ § § §**	**PUBLIC UTILITY COMMISSION OF TEXAS**

DIRECT TESTIMONY OF

DR. JOSEPH B. BAUGH

ON BEHALF OF

CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC

April 2024

TABLE OF CONTENTS

TABLE OF EXHIBITS AND WORKPAPERS

Exhibits	Description
Exhibit JBB-1	Professional Experience of Dr. Joseph B. Baugh
Exhibit JBB-2	Glossary of Acronyms

Workpapers	Description
N/A	

I. SUMMARY OF GUIDEHOUSE'S INDEPENDENT ANALYSIS AND REVIEW

Guidehouse performed two types of independent analysis and review related to technology resiliency measures in CenterPoint Houston Electric, LLC's ("CenterPoint Houston") Resiliency Plan:

- Qualitative assessment of physical security and cybersecurity risks faced by electric utilities like CenterPoint Houston; and
- Qualitative assessment of the reasonableness of each technology and cyber security resiliency measure considered for inclusion in CenterPoint Houston's Resiliency Plan.

Guidehouse reviewed the five CenterPoint Houston technology resiliency measures shown in the table below and identified the effectiveness and benefits of each resiliency measure in a qualitative comparative analysis process that compared relevant functions and security practices for each resiliency measure with industry best practices located in the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF").

Summary of CenterPoint Houston's Technology Resiliency Measures

Technology Resiliency Measures	Split		Project	CAP $MM	O&M $MM
	T%	D%	Duration	2025-2025	2025-2027
Voice and Mobile Data Radio System Refresh	50%	50%	7 years	$ 15.60	$ -
Backhaul Microwave Communication	50%	50%	3 years	$ 12.10	$ -
Data Center Refresh	50%	50%	4 years	$ 2.90	$ 0.25
Network Security and Vulnerability Management	50%	50%	7 years	$ 1.00	$ -
IT/OT-Cybersecurity Monitoring	50%	50%	7 years	$ 22.50	$ -
Total Costs for Technology Resiliency Measures				$ 54.10	$ 0.25

Guidehouse finds that CenterPoint Houston's Resiliency Plan appropriately prioritizes technology resiliency measures that help mitigate cybersecurity risk. Guidehouse's physical security and cybersecurity risk assessment confirms that the frequency and magnitude of physical attacks and cyber-attacks is likely to increase over time, suggesting the need for continued resiliency investments in these areas. Given this, I also concur with the findings included in Mr.

Shlatz' testimony that support CenterPoint Houston's proposed physical security resiliency measures (Substation Physical Security Fencing and Substation Security Upgrades) that also address risks associated with physical attacks on substations.

Further, the peer utility benchmarking survey described in Section VI of my testimony indicates that proposed resiliency measures included in CenterPoint Houston's Resiliency Plan are consistent with those deployed at other utilities.

In summation, I conclude the five technology resiliency measures in CenterPoint Houston's Resiliency Plan are:

- appropriate for addressing the physical security and cybersecurity risks CenterPoint Houston faces;
- aligned with industry best practices; and
- beneficial to customers and communities served by CenterPoint Houston.

II. INTRODUCTION

Q. PLEASE STATE YOUR NAME AND CURRENT POSITION.

A. My name is Dr. Joseph B. Baugh. I have been employed in various capacities by Guidehouse Inc. ("Guidehouse")[1] since 2019, as an Associate Principal in Guidehouse's Energy, Sustainability, and Infrastructure Practice, working primarily on the Cybersecurity and Compliance team. My business address is 111 Congress Avenue, Suite 2500, Austin TX 78701

Q. PLEASE SUMMARIZE YOUR BACKGROUND AND CURRENT RESPONSIBILITIES.

A. I have over 50 years' experience in electric utility and power system operations, including specialization in network and information security associated with electric utility information technology ("IT") and operational technology ("OT") systems. At the onset of my career with cyber systems, I worked at a power generation and electric transmission utility in Arizona for 29 years and was responsible for implementing numerous cyber system and business process improvement projects. After retiring from the utility, I worked at Western Electricity Coordinating Council ("WECC") on the cybersecurity audit team and was responsible for audits, investigations, and evaluations of physical security and cyber systems for compliance with North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") Reliability Standards. My experience includes implementations, risk assessments and evaluations, as well as multiple audits of electric system reliability and security protective resiliency measures and controls,

[1] Previously, Navigant Consulting, Inc.

including physical and cyber security systems located at power generation facilities, electric substations, and power system control centers.

Over the past four years at Guidehouse, I have been involved in the evaluation of the current states of numerous energy sector clients to manage physical and cyber security risk. These evaluations include assessing current cybersecurity states and program maturity, using common frameworks such as the Department of Energy ("DOE") Cybersecurity Capability Maturity Model ("C2M2") and the NIST CSF, as well as developing feasible recommendations on actions the client can take to achieve a desired target state in alignment with its goals and objectives. I have also developed compliance programs to meet the requirements of new and changing reliability standards. For example, I worked on several projects related to complying with the California Public Utilities Commission Decision 19-01-018 (Physical Security Decision) to improve physical security at electric distribution substations.

Overlapping my tenures at WECC and Guidehouse, I served as an expert witness for WECC in enforcement cases involving violations of the NERC CIP Standards. I hold a Bachelor of Science ("BS") degree in Computer Science from the University of Arizona and a Master of Business Administration ("MBA") degree from the Eller College of Management at the University of Arizona. My Doctor of Philosophy ("Ph.D.") was conferred by Capella University. My dissertation examined the impacts of deregulation and other market forces in the electric utility industry on management strategies, organizational structures, and organizational cultures at a non-profit generation and transmission electric cooperative.

I currently hold the NERC Certified System Operator Balancing and Interchange ("NCSO-BI") credential, the Project Management Professional ("PMP") certification, several globally recognized cybersecurity certifications (e.g., Certified Information Systems Security Professional ("CISSP"), Certified Information Systems Auditor ("CISA"), Certified in Risk and Information Systems Control ("CRISC"), Certified Information Security Manager ("CISM"), and the NIST Cybersecurity Professional ("NCSP") – Practitioner" certification. I am one of fewer than 300 Triple Crown holders worldwide of the American Society for Industrial Security ("ASIS") International physical security certifications: Physical Security Professional ("PSP"), Certified Protection Professional ("CPP"), and Professional Certified Investigator ("PCI"). My unique combination of energy sector experience in power system operations, business process improvement, and IT/OT systems, combined with academic and technical training backgrounds, and relevant professional certifications provides a high level of expertise across the 16 CISA critical infrastructure sectors, including the energy sector. This expertise was applied to this engagement with CenterPoint Houston.

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

A. I am testifying on behalf of CenterPoint Houston.

Q. IS GUIDEHOUSE'S ANALYSIS AND REVIEW OF CENTERPOINT ENERGY HOUSTON ELECTRIC'S RESILIENCY PLAN INDEPENDENT AND UNBIASED?

A. Yes. Guidehouse regularly consults for electric investor-owned, municipal, and cooperative utilities in addition to state and federal agencies. As a matter of practice, Guidehouse is committed to maintaining an independent and unbiased approach to its

engagements. Specific to our analysis and review of CenterPoint Houston's Resiliency Plan, we took the following steps to maintain independence:

- Applying a consistent methodology for assessing the reasonableness of technology resiliency measures proposed for inclusion in CenterPoint Houston's Resiliency Plan;
- Performing a critical assessment of CenterPoint Houston's proposed resiliency measures to those adopted by other utilities that have successfully implemented resiliency measures. Recommendations were provided to further improve CenterPoint Houston's proposed resiliency measures;
- Providing independent analysis of physical and cyber security risks faced by electric utilities like CenterPoint Houston based on our knowledge and expertise;
- Comparing CenterPoint Houston's resiliency measures to those of leading utility practices obtained from an independent survey of electric utility resiliency measures conducted by a reputable firm with expertise in benchmarking;
- Proposing metrics reporting and effectiveness measures that CenterPoint Houston and the Public Utility Commission of Texas ("Commission") can rely on to determine if CenterPoint Houston's proposed resiliency measures are delivering value to its customers over time; and.
- Enhancing the resiliency of physical and cyber security systems associated with CenterPoint Houston's transmission and distribution system, potentially reducing adverse impacts on customers, restoration times, and restoration costs due to outages caused by resiliency events.

Q. HAVE YOU TESTIFIED PREVIOUSLY?

A. Yes, as noted above I served as an expert witness for WECC in enforcement cases involving violations of the NERC CIP Standards. However, I have not previously testified before a state utility commission.

III. OVERVIEW OF TESTIMONY

Q. WHAT IS THE PURPOSE OF YOUR TESTIMONY?

A. The purpose of my testimony is to provide an overview of Guidehouse's independent analysis and review of CenterPoint Houston's Resiliency Plan with a focus on proposed technology resiliency measures. My testimony that follows provides evidence that the technology resiliency measures CenterPoint Houston proposes over the years 2025 through 2027 are reasonable and appropriate to include in its Resiliency Plan.. Specially, my testimony and exhibits confirm that CenterPoint Houston's proposed technology resiliency measures and the corresponding resiliency-focused investments can provide value to customers and communities located within its service area by reducing adverse impacts on customers, restoration times, and restoration costs due to an outage caused by a resiliency event involving physical or cyber-attack. My testimony also supports the direct testimony of Mr. Ronald Bahr as it relates to the evaluation and justification of each CenterPoint Houston Resiliency Plan technology resiliency measure for which it seeks approval from the Commission.

Q. WHAT QUALIFICATIONS DOES GUIDEHOUSE HAVE AS AN INDEPENDENT EXPERT IN RESILIENCY PLANNING FOR ELECTRIC UTILITIES?

A. Guidehouse has conducted several engagements addressing resiliency planning. Examples include:

1. **Duke Energy Florida** – Guidehouse conducted a detailed analysis of storm

hardening investment to support two successive Storm Protection Plans that were approved by the Florida Public Service Commission.

2. **New Jersey Board of Public Utilities ("NJBPU")** – Guidehouse was engaged by the NJBPU to conduct an independent investigation of Jersey Central Power & Light's emergency storm procedures, restoration practices, and resiliency measures to address customer interruptions caused by Hurricane Sandy. Guidehouse's recommendations were approved by the NBJPU.
3. **AEP Kentucky Power** – Guidehouse recently assessed Kentucky Power's storm reliability performance and proposed resiliency measures to enhance distribution system resiliency. Our assessment included an electric utility benchmark survey similar to the First Quartile benchmarking of resiliency measures.
4. **Commonwealth Edison** – Guidehouse conducted an independent assessment of Commonwealth Edison's maintenance and operational practices in response to an investigation by the Illinois Commerce Commission ("ICC") to address customer interruptions during major storms.

Q. WHAT EXHIBITS HAVE YOU INCLUDED WITH YOUR TESTIMONY?

A. I have prepared or supervised the preparation of the exhibits listed in the table of contents, including Exhibit JBB-2 which is a full-length report for Guidehouse's Independent Analysis and Review of CenterPoint Energy Houston Electric's Resiliency Plan. With regards to Exhibit JBB-2, my responsibility was primarily focused on the assessment of physical and cyber security threats and review of technology resiliency measures considered for inclusion in CenterPoint Houston's Resiliency Plan.

Q. WHAT INFORMATION RELATIVE TO THE FIVE TECHNOLOGY

RESILIENCY MEASURES IS CONTAINED IN THE GUIDEHOUSE REPORT PROVIDED AS EXHIBIT ELS-2?

A. The Guidehouse report includes

- **Background** – Guidehouse's understanding of resiliency risks CenterPoint Houston must manage and the policy context for how Texas and other states are addressing resiliency of the electric system.
- **Purpose of Guidehouse's Analysis and Review** – Overview of Guidehouse's qualification as an independent expert on resiliency planning for electric systems as well as the objectives and approach taken to perform Guidehouse's independent analysis and review of CenterPoint Houston's Resiliency Plan.
- **Resiliency Risk Analysis** – Independent assessment of resiliency risks facing CenterPoint Houston's service area, including physical and cyber security threats and vulnerabilities (e.g., cyber threats to CenterPoint Houston's IT/OT systems).
- **Resiliency Plan Review** – Independent review of CenterPoint Houston's Resiliency Plan, including benchmarking against best practices in resiliency planning among peer utilities, analysis of potential benefits for resiliency measures included in the Resiliency Plan, and recommendations provided to CenterPoint Houston based on this review.
- **Benchmark Survey** – Results of independent survey of industry resiliency measures and practices covering a range of resiliency measures, many of which are similar to those proposed by CenterPoint Houston.
- **Summary Findings** – Summary of the findings, conclusions, and recommendations from Guidehouse's independent analysis and review.

Q. WHAT WERE THE OBJECTIVES OF GUIDEHOUSE'S ANALYSIS AND REVIEW OF CENTERPOINT ENERGY HOUSTON'S RESILIENCY PLAN?

A. The purpose of Guidehouse's independent analysis and review of CenterPoint Houston's Resiliency Plan is to present evidence of the potential need and value of resiliency-focused investments for CenterPoint Houston's service area.

Specific objectives included:

1. Advise CenterPoint Houston on best practices in electric utility resilience planning based on Guidehouse industry expertise and experience working with utilities in other jurisdictions on resiliency planning efforts;
2. Provide independent analysis of human threat risks faced by CenterPoint Houston, including physical and cyber security trends that could be used as evidence of the potential need for investments that address specific physical and cyber security resiliency events; and
3. Conduct an independent review and analysis of CenterPoint Houston's Resiliency Plan, including all resiliency measures under initial consideration by CenterPoint Houston, to help inform CenterPoint Houston's selection and prioritization of resiliency measures to pursue. This includes a comparison of proposed technology resiliency measures and resiliency measures to those adopted by electric utilities in response to physical and cyber security risks.

Q. HAVE YOU REVIEWED THE DIRECT TESTIMONIES OF OTHER CENTERPOINT ENERGY HOUSTON ELECTRIC WITNESSES PROVIDING DIRECT TESTIMONY IN THIS DOCKET?

A. Yes. I have reviewed the testimonies of CenterPoint Energy Houston Electric witnesses

Jason Ryan, Brad Tutunjian, Ronald Bahr, and Jeff W. Garmon. My testimony is consistent with and supports the findings and conclusions provided by each witness, particularly for Mr. Ronald Bahr who addresses each of CenterPoint Energy's technology resiliency measures. I have also reviewed the testimony of Guidehouse witness Eugene L. Shlatz, who addresses certain weather-driven and climate resiliency measures included in CenterPoint Houston's Resiliency Plan that impact physical security attributes.

Q. HOW IS YOUR TESTIMONY ORGANIZED?

A. My testimony is organized as follows: First, I provide a summary of Guidehouse's independent analysis of resiliency risk attributed to human threats (i.e., physical and cyber security) for CenterPoint Houston's service area, including a summary of how its current and forecasted risk profile justifies the need for resiliency investments. Then, I provide a summary of Guidehouse's independent review and analysis of CenterPoint Houston's Resiliency Plan for technology resiliency measures including qualitative evidence of how those resiliency measures can provide benefits to customers and communities served by CenterPoint Energy in its Houston Electric service area. Next, I present the results of an independent survey of electric utilities that have implemented resiliency measures and programs. Finally, I summarize the findings and recommendations made by Guidehouse to CenterPoint Houston based on our independent analysis and review of its Resiliency Plan related to technology resiliency measures projects.

IV. INDEPENDENT ANALYSIS OF RESILIENCY RISK FOR CENTERPOINT ENERGY'S HOUSTON ELECTRIC SERVICE AREA

Q. WHAT APPROACH DID GUIDEHOUSE FOLLOW TO CONDUCT ITS ANALYSIS OF RESILIENCY RISK FOR CENTERPOINTHOUSTON'S SERVICE AREA?

A. The Technology resiliency measures in the Company`s Resiliency Plan are intended to enhance the resiliency of the Company's technology infrastructure to withstand and limit interruptions of service during certain Resiliency Events. Weather events that include extreme wind, water, temperatures, or fire, construction impacting network fiber cables, vendor outages, and cybersecurity attacks are types of resiliency events that can affect technology. Please refer to the testimony of Mr. Tutunjian for Resiliency Events related to weather. Guidehouse researched a variety of public sources for current and historical trends over a five-year period to identify specific physical and cybersecurity risks relevant to the CenterPoint Houston operating environment. The results of this research and analysis of resiliency risk for the five technology resiliency measures are detailed below.

Q. WHAT SPECIFIC TYPES OF RESILIENCY RISKS DID YOU ANALYZE AND WHY?

A. Guidehouse reviewed increasing trends in physical and cyber attacks in the CenterPoint Houston service area, including physical damage to cyber systems and their host facilities by insider and external actors as well as common cyber attack vectors. Specific resiliency risks included loss or misuse of the technology resiliency measure systems under review and associated adverse impacts to the CenterPoint Houston electric delivery system. These risks were considered during the analysis phase to ensure the applicable resiliency

functions and security solutions for each resiliency measure aligned with industry best practices and controls defined by the NIST CSF.

Q. WHAT IS YOUR UNDERSTANDING OF PHYSICAL AND CYBER SECURITY THREATS TO ELECTRIC UTILITIES SUCH AS CENTERPOINT HOUSTON?

A. A review of historical physical and cyber attacks across the electric industry, as described below, indicates CenterPoint Houston cyber systems and their host facilities are subject to both physical damage by bad actors and a wide range of cyber attack methodologies and techniques including:

- Ransomware
- Distributed Denial-of-Service ("DDoS")
- Malware
- Phishing
- Exploitation of known but unpatched vulnerabilities
- Social engineering
- Supply chain attacks
- System misconfigurations
- Missing or poor encryption practices
- Insider threats and external actors via physical and cyber attacks

Resiliency risks associated with these attack methodologies and techniques were analyzed through the comparative analysis of the functions and security solutions of the five resiliency measures under review with the NIST CSF best practices and protective resiliency measures that counter these risks.

Physical and cyber security benefits are difficult to measure with a traditional return on investment ("ROI") calculation as the benefits of security projects are generally realized in avoided costs and other avoided negative impacts. As examples of potential avoided costs and negative impacts, Security Made Simple identifies major cost components related to cyberattacks, including falling stock prices, loss of customers, cyber insurance costs, lawsuits, compliance penalties and sanctions, and business interruption costs.[2] Each of these cost factors may or may not be included in the cost of data breaches statistics described below, depending on the rigor of the underlying data collection instrument.

Statista reports the average cost of data breaches in the United States increased steadily from $5.4 million dollars in 2013 to $9.5 million dollars in 2023.[3] This upward trend indicates a strong probability the annual average cost of a single data breach will continue to increase over the next five-year period. IBM reported similar annual averages for overall data breach costs in the U.S.[4] IBM further identified a 2.3% increase in the average cost of a data breach between 2022 and 2023.[5] In addition, IBM reported the cost of a data breach escalates with longer detection times and increased system downtime.[6] Combating these deleterious impacts requires a comprehensive approach to physical security and cyber security efforts. In a 2021 study, Claroty reported, "organizations have internalized the lessons learned from high-profile cyberattacks and are prioritizing cybersecurity by increasing investments and implementing new or updated processes and

[2] Security Made Simple. (2021 August 25). *What does a cyberattack do to a company's value?* https://securitymadesimple.org/cybersecurity-blog/what-does-a-cyberattack-do-to-a-companys-value/

[3] Statista (2024 January). *Average cost of a data breach in the United States from 2006 to 2023.* https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/#:~:text=As%20of%202023%2C%20the%20average,dollars%20in%20the%20previous%20year

[4] IBM. (2023). *Cost of a Data Breach Report* [IBM Technical Report, Figure 3, pp. 11-12]. https://www.ibm.com/reports/data-breach

[5] Ibid. (*Figure 4*, p. 13)

[6] Ibid. (p. 7)

controls."[7] This finding aligns with the current CenterPoint approach to implement diverse technology resiliency measures. While rejecting a comprehensive approach to cyber resiliency is always an option, Claroty stated, "[t]he cost for critical infrastructure organizations of doing nothing is not tolerable. The longer an organization goes without the right cyber-physical systems security capabilities in place, the more likely they are to experience a major breach."[8] I concur with this statement, as the more CenterPoint integrates technology and cyber systems into its overall operational model, the more critical a robust defense-in-depth cybersecurity strategy becomes to develop a strong and resilient network.

Guidehouse considered "avoided cost" as a benefit of each of the resiliency measures analyzed below without itemizing specific costs. The more salient analysis is regarding the resilience impact of each of the resiliency measures because a benefit of each of them is avoided cost. While Guidehouse reviewed the technology and cyber security resiliency measures included in CenterPoint Houston's Resiliency Plan individually, it should be noted that the benefit of these resiliency measures is cumulative toward ensuring a strong and diverse cybersecurity posture that identifies, detects, deters, and defends against physical or cyber-attacks and ensures a resilient operational posture that can respond to and recover from any successful attacks. This means that, in general, the benefits of these resiliency measures can increase exponentially as more resiliency measures are adopted (i.e., the whole is greater than the sum of its parts).

[7] Claroty. (2021). *The Global State of Industrial Cybersecurity 2021: Resilience amid Disruption* [White Paper, p. 6]. https://claroty.com/resources/reports/the-global-state-of-industrial-cybersecurity

[8] Claroty. (2022 December 20). *How Cyber-Physical Security Maximizes ROI* [Technical Blog]. https://claroty.com/blog/how-cyber-physical-system-security-maximizes-roi

Q. WHAT IS THE HISTORICAL, CURRENT, AND FUTURE RISK TO CENTERPOINT HOUSTON'S SERVICE AREA FOR PHYSICAL SECURITY EVENTS BASED ON YOUR ANALYSIS?

A. My assessment of the physical security risk to CenterPoint Houston's system is based on my knowledge and expertise in this area as well as research of publicly available documents that provide additional context for the region served by CenterPoint Houston. For example, the Texas Department of Homeland Security ("TDHS") Texas Homeland Security Strategic Plan ("THSSP") identifies specific physical security threats to the energy sector in and around the CenterPoint Houston electric system, which TDHS cites as a lifeline critical public infrastructure sector.[9] Resiliency is critically important for the electric sector not only for the operation of its own systems, but also for the operation of other critical infrastructure sectors that rely on a stable electric supply. In the context of physical security risk, TDHS describes as a key risk for Texas cartels that use military and terrorist tactics to accomplish their goals and expand their control of criminal activities in Texas. Domestic terrorism has become more prevalent in recent years and poses a credible threat to the electric sector as well. In addition, "Texas-based homegrown violent extremists continue to aspire to conduct attacks in Texas, and individuals sympathetic to foreign terrorist organizations continue to provide them material support in the form of recruitment, financial resources, and propaganda. All terrorist actors will continue to utilize digital media to facilitate radicalization/recruitment and communicate, and law

[9] Texas Department of Homeland Security [TDHS]. (2021 June). *Texas Homeland Security Strategic Plan: 2021-2025* [THSSP: TDHS Technical Report, p. 21]. https://gov.texas.gov/uploads/files/press/HSSP_2021-2025.pdf

enforcement's ability to detect planned criminal activity will be challenged as such actors move to more secure communication platforms."[10]

Historical and Current Physical Security Risk Profile

Given the Centerpoint Houston cyber system footprint, it is particularly susceptible to physical and cyber attacks. In its report on reliability risk priorities, NERC states physical security and cybersecurity risks are rising, and the nature of the attacks continues to evolve: "there has been an uptick in physical security events, including copper theft and ballistic damage, against the BPS [Bulk Power System] and specifically at distribution substations. Vulnerabilities to such events are exacerbated by commodity prices, supply chain constraints, environmental activists, and domestic violent extremists."[11]

Current protective resiliency measures to mitigate malicious activities at electric infrastructure facilities have necessarily focused on substations that have been identified as particularly critical using various threat and vulnerability assessments and physical security plans. Coordinated attacks on multiple substations that target expensive electric elements, such as the sniper attacks at Metcalf substation in 2013 that focused on transformers and other critical electrical equipment with long replacement lead-times, could have a significant impact on the safety and well-being of U.S. citizens and the economy.[12] CBS News reported a 71% increase in physical attacks on electric grid facilities in 2022 alone.[13] Citing 25 physical attacks on nationwide electric infrastructure, including

[10] TDIIS. TIISSP. (p. 21)
[11] NERC. (2023. p. 36)
[12] Smith, R. (2014 March 12). *U.S. Risks National Blackout from Small-Scale Attack.* https://www.wsj.com/articles/SB10001424052702304020104579433670284061220
[13] Sganga, N. (2023 February 22). *Physical attacks on Power Grids rose by 71% last year, compared to 2021.* https://www.cbsnews.com/news/physical-attacks-on-power-grid-rose-by-71-last-year-compared-to-2021/

one in the El Paso area in 2022, the Dallas Morning News examined vulnerabilities associated with Texas substations and concluded a coordinated attack on power infrastructure could cause a cascading failure of the Texas power grid.[14] CenterPoint operates over 300 electric substations and other physical locations, such as control centers, IT data centers, and service centers, each of which contain IT/OT cyber systems, providing a large physical attack surface for malicious actors.

From an IT/OT cyber system perspective, the risks of physical attacks are somewhat less, but still significant, due to the impact of physical intrusions and ballistic attacks on critical electric facilities. Most cyber systems associated with electric grid and business operations rely on hardened facilities, such as secure buildings or locked enclosures, to prevent physical damage to critical cyber systems, such as protective relays, SCADA systems, and telecommunications systems.

Future Physical Security Risk Profile

The NERC report on reliability risk priorities indicates physical security and cyber security risks are rising, while the nature of the attacks continues to evolve.[15] As an example, ballistic attacks on electric facilities using drones as a delivery vehicle is an emerging threat. Combining the trends cited above, including the increasing rate of domestic terrorism in Texas and other physical security risks in CenterPoint Houston's electric service area, Guidehouse expects physical attacks on CenterPoint facilities containing IT/OT cyber systems to increase in number and severity over the next five years.

[14] Williams, M. (2023 February 9. *Plots, attacks against power grids are increasing nationwide. How vulnerable is Texas?* https://www.dallasnews.com/news/2023/02/09/plots-attacks-against-power-grids-are-increasing-nationwide-how-vulnerable-is-texas/
[15] NERC. (2023, p. 32)

Q. WHAT IS THE HISTORICAL, CURRENT, AND FUTURE RISK TO CENTERPOINT HOUSTON'S SERVICE AREA FOR CYBERSECURITY EVENTS BASED ON YOUR ANALYSIS?

A. My assessment of cybersecurity risk to CenterPoint Houston's system is based on my knowledge and expertise in this area as well as research of publicly available documents that provide additional context for the region served by CenterPoint Houston. For example, the TDHS THSSP report describes cyber threats as follows: "[c]yberattacks and intrusions can be used by criminals, terrorists, insiders, and hostile foreign nations to disrupt delivery of essential services, mask other attacks, or shake citizens' confidence in the government. Cyberattacks are relatively easy to execute and challenging to disrupt and investigate, as demonstrated in the August 2019 ransomware attack that impacted 23 local government entities in Texas, and the frequency of attacks and intrusions has increased significantly during the past five years. As the cyber threat continues to grow and evolve, a particular concern is the potentially severe consequence of an effective cyberattack against critical infrastructure facilities and systems. Cyber threats could also result in the denial or disruption of essential services, including [electric] utilities."[16]

Historical and Current Cybersecurity Risk Profile

As stated above, cyber attacks across all critical infrastructure sectors have increased in number and severity over the past five years with notable examples including the 2021 Colonial pipeline attack, numerous known vulnerability exploitations of poorly patched cyber systems, and the rise of malware and ransomware attacks targeting business

[16] TDHS. (p. 23)

process cyber systems, supply chains, and other vulnerabilities by foreign and domestic cyber threat vectors.

Future Cybersecurity Risk Profile

As noted above, CenterPoint Houston operates over 400 electric substations and other physical locations. Collectively, these locations host approximately 375 IT/OT cyber systems, which provides a significant digital attack surface for malicious actors. The NERC report on reliability risk priorities identified physical security and cybersecurity risks as rising, while the nature of the attacks continues to evolve beyond current protective resiliency measures and controls.[17] Additional factors leading to an increased future cybersecurity risk profile for CenterPoint and other electric utilities include the following:[18]

- The emergence of Artificial Intelligence ("AI") and machine learning tools being deployed by cyber adversaries is likely to increase both the number and types of attacks, as well as the probability of attack success.
- An increasing trend to virtualize and host critical cyber systems in cloud environments may create additional cyber risk during use, transmission, and storage of data.
- Supply chain risks derived from compromise of critical cyber system components during the development and procurement cycles.
- Increasing deployment of distributed energy resources ("DERs") and DER aggregators, which are largely unregulated, presents increased cybersecurity risk to

[17] NERC. (2023, p. 32)
[18] NERC. (2023, p. 37)

the electric grid because their control systems could become compromised and used as an attack vector into electric systems.[19]

- Increasing lack of a robust cyber workforce requires organizations in the electric sector and other critical infrastructure sectors to rely heavily on automated tools to develop robust cybersecurity defenses.
- Increasing remote work by utility workers also increases the risk of compromise of critical cyber systems, which can be mitigated by hardening telecommunications platforms to protect data in transit.

Considering these trends as well as previously discussed physical security trends of the increasing rate of domestic terrorism in Texas and continued attacks by foreign adversaries, Guidehouse expects cybersecurity risk to increase in CenterPoint Houston's service area absent additional cybersecurity investments. In particular, the risk of coordinated attacks that combine physical and cyber intrusions across multiple facilities is expected to increase.

Q. FOR EACH TYPE OF RESILIENCY EVENT ANALYZED, DOES YOUR ANALYSIS INDICATE THAT RESILIENCY RISK IS EXPECTED TO INCREASE OVER TIME AND THAT RESILIENCY INVESTMENTS ARE NEEDED IN CENTERPOINT HOUSTON'S SERVICE AREA TO REDUCE RESILIENCY RISK AND IMPROVE THE SAFETY, RELIABILITY, AND RESILIENCY OF ITS ELECTRIC SYSTEM?

[19] NERC. (2022 December). *Cyber Security for Distributed Energy Resources and DER Aggregators*. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf

A. Yes, my testimony supports the expectation that physical and cyber security risk will continue to increase over time. This is supported by the fact that the average cost of data breaches has trended upward from 2013 to 2023. In addition, the average weekly number of cyber attacks has increased over the past five years.[20] Given the evolving nature of cyber attacks and multiple malicious actors targeting the electric grid, I conclude that physical security and cybersecurity risk will continue to increase over the next five years. This indicates that risk mitigation measures to address these types of resiliency events is becoming increasingly needed for CenterPoint Houston.

CenterPoint Houston's operational and cyber systems are interconnected, thus protective resiliency measures and controls for its systems can better support operational resiliency by developing a "defense-in-depth" strategy that emphasizes redundancy, data confidentiality, integrity, and availability measures, and effective business continuity and disaster recovery planning. The average annual cost of a single data breach and other cyber intrusion has steadily increased from 2013 to 2023 to $9.8 million per incident, with the upper bound for successful attacks, such as ransomware, extending much higher. This trend indicates a strong probability for higher annual avoided costs over the next five-year period through successful resiliency measures for CenterPoint Energy's technology and cyber systems.

Q. DID CENTERPOINT ENERGY MAKE MODIFICATIONS TO ITS RESILIENCY PLAN BASED ON THE FINDINGS AND

[20] Casanovas, M., & Ngheim, A. (2023 August 1). *Cybersecurity – is the power system lagging behind?*. [International Energy Agency Technical Report - *Table: Average number of weekly cyberattacks per organisation in selected industries, 2020-2022*] https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind

RECOMMENDATIONS PROVIDED BY GUIDEHOUSE RELATED TO RESILIENCY RISK?

A. CenterPoint Houston used the Guidehouse analysis found in its report to make adjustments to its plan as stated in Mr. Tutunjian's testimony.

V. INDEPENDENT REVIEW AND ANALYSIS OF CENTERPOINT HOUSTON's RESILIENCY PLAN

Q. WHAT APPROACH DID GUIDEHOUSE FOLLOW TO CONDUCT ITS ANALYSIS AND REVIEW OF CENTERPOINT ENERGY HOUSTON ELECTRIC'S RESILIENCY PLAN?

A. Guidehouse critically reviewed each of CenterPoint Houston's proposed technology resiliency measures to determine whether the resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's Resiliency Plan. The Technology Resiliency Measures in the Company's Resiliency Plan are intended to enhance the resiliency of the Company's technology infrastructure to withstand and limit interruptions of service during certain Resiliency Events. Weather events that include extreme wind, water, temperatures, or fire, construction impacting network fiber cables, vendor outages, and cybersecurity attacks are types of resiliency events that can affect technology. Please refer to the testimony of Mr. Tutunjian for Resiliency Events related to weather. As noted in the Guidehouse Resiliency Report (Exhibit ELS-2, section 5.1.3.2), it is difficult to quantify the benefits of technology resiliency measures, as they are an enabling function to support the effective operation of electric delivery systems.

A key objective of the Guidehouse assessment was to determine each resiliency measure's effectiveness from a technology resiliency perspective by applying the NIST Cybersecurity Framework. Additionally, Guidehouse applied the Presidential Policy Directive 21 ("PPD-21") definition of resilience, which defines resilience as, "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions [and] the ability to withstand and recover from deliberate attacks, accidents, or

naturally occurring threats or incidents."[21] This definition is commonly used within the cybersecurity field as evidenced by its use in the 2021 CISA Infrastructure Security Division ("CISA-ISD") report on Lessons Learned from the Regional Resiliency Assessment Program.[22] NIST expanded this definition in the context of cybersecurity, stating that resilience is "[t]he ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment".[23] This extension captures cyber system resilience from the business process perspective and supports including IT OT cyber systems as part of a balanced organization-wide resiliency plan.

Due to the difficulty of performing quantitative analyses, environmental uncertainty, and the constantly evolving nature of cyber threats, the International Energy Agency ("IEA") recommends the use of a common framework to provide consistency in assessing resiliency risks associated with disparate cyber systems within their operating environments. IEA identified five potential frameworks,[24] including the Electricity Subsector - Cybersecurity Capability Maturity Model (ES-C2M2, which evaluates the maturity of an organization's cybersecurity capabilities), the NIST Cybersecurity Framework (CSF, which is a general resiliency framework for understanding, prioritizing,

---

[21] The White House. (2013 February 12). *Presidential Policy Directive – Critical Infrastructure Security and Resilience* [PPD-21, p. 12]. https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf

[22] Cybersecurity & Infrastructure Security Agency: Infrastructure Security Division [CISA-ISD]. (2021 June). *Methodology for Assessing Regional Infrastructure Resilience: Lessons Learned from the Regional Resiliency Assessment Program* [CISA-ISD Technical Report], (p. 8). https://www.cisa.gov/sites/default/files/publications/DIS_DIIS_Methodology_Report_ISD%20EAD%20Signed_with%20alt-text_0.pdf

[23] NIST Glossary: *Definition of Cyber Resiliency*. https://csrc.nist.gov/glossary/term/cyber_resiliency

[24] International Energy Agency [IEA]. (2021). *Enhancing Cyber Resilience in Electricity Systems* [see *Table 4. Overview of regularly referred to instruments for cybersecurity in the electricity sector*, pp. 30-32]. https://iea.blob.core.windows.net/assets/0ddf8935-bc23-4d5f-b798-3aad1f32432f/Enhancing_Cyber_Resilience_in_Electricity_Systems.pdf

and managing cybersecurity risks), the NISTIR 7628 Guidelines (which focus on smart grid characteristics, risks, and vulnerabilities), ISO/IEC TR 27019 (which is applicable to utility process control systems) and ISO 22301 (which relates to business continuity management). After reviewing these five frameworks, Guidehouse chose the NIST CSF as a common framework to support comparative analyses of resiliency features and functions across the five technology and cybersecurity resiliency measures considered for inclusion in CenterPoint Houston's Resiliency Plan.

The NIST CSF[25] is a set of best practices and recommended cybersecurity controls commonly used in the electric utility sector to guide cybersecurity activities and the assessment and mitigation of cybersecurity risks as part of an organization's overall risk management processes. The Framework consists of three parts:

1. Framework Core
2. Implementation Tiers
3. Framework Profiles

The Framework Core (the "Core") is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Framework Profiles, the Framework helps an organization align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Implementation Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing

[25] NIST. (2018 April 16). *Framework for Improving Critical Infrastructure Cybersecurity* [v1.1], https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

cybersecurity risk, which helps with prioritizing and achieving cybersecurity objectives, including resiliency objectives.

For the review of CenterPoint Houston's Resiliency Plan resiliency measures for IT and OT cyber systems, Guidehouse applied a qualitative comparative analysis[26] between the NIST CSF Core functions, categories, and sub-categories and the functions and security solutions in the CenterPoint operating environments, as described by CenterPoint in documentation and interviews or inferred by professional judgement, for each of the five technology resiliency measures included in CenterPoint Houston's Resiliency Plan. Strong correlations between the proposed resiliency measure's functions and security solutions with a given NIST CSF Function Category practice (e.g., the Asset Management category under the Identify function is coded in the CSF as ID.AM) were identified and applied to determine qualitative benefits of these resiliency measures.

In addition to correlations at the NIST CSF Function Category level, the Guidehouse analysis included a review of redundancy, which aligns with the NERC description of "risk reduction benefits associated with added redundancy, diversity, and minimization of very high-risk assets."[27] The CISA-ISD report also described redundancy as a component of the Mitigation building block for resilience that resists or absorbs negative impact, reduces the severity or consequence of an event, and supports the reliability of infrastructure systems.[28]

Guidehouse critically reviewed each of CenterPoint Houston's proposed technology resiliency measures to determine whether the resiliency measure is reasonable

[26] CISA-ISD. (*Comparative Analysis* section. p. 71)
[27] NERC. (2023 August 17). *2023 ERO Reliability Risk Priorities Report* (p. 33). https://www.nerc.com/comm/RISC/Related%20Files%202023/RISC_ERO_Priorities_Report_2023_Board_Approved_Aug_17_2023.pdf
[28] CISA-ISD. (*Part 1*, p. 8)

and beneficial for inclusion in CenterPoint Houston's Resiliency Plan. A key objective of Guidehouse's assessment was to determine the effectiveness of each resiliency measure at mitigating the impact of physical or cyber attacks on CenterPoint Houston's power delivery system. An important element of Guidehouse's assessment was consideration of future forecasted risk attributed to resiliency events as described in Section IV of my testimony. For example, the projected increases in physical and cyber attacks were factors that Guidehouse incorporated into its analysis of potential benefits of CenterPoint Houston's OT Cybersecurity Monitoring resiliency measure.

To complete our assessment, Guidehouse obtained details on CenterPoint Houston's proposed technology resiliency investments and compared CenterPoint Houston's proposed measures with industry best practices based on a peer utility benchmarking survey described in Section VI of my testimony.

Guidehouse analyzed CenterPoint Houston's proposed Resiliency Plan technology resiliency measure investments for each of the following evaluation categories:

- **Resiliency Measure Description** – Guidehouse's understanding of each resiliency measure's objectives and rationale, including how the measure reduces the risk of resiliency events.
- **Alternatives Considered** – Alternatives CenterPoint Houston considered in lieu of the proposed resiliency measure, and why these alternatives were determined to be less effective than the proposed resiliency measure.
- **Resiliency Measure Metrics and Effectiveness** –Metrics resiliency measure metrics and measures CenterPoint Houston proposes to use for each resiliency measure, where applicable.

- **Benefits Analysis** – Qualitative analysis of benefits for each proposed resiliency measure using the NIST CSF to identify key functions and categories that aligned with relevant functions and solutions provided by the proposed resiliency measure.
- **Resiliency measure Assessment and Conclusions** – For each resiliency measure, Guidehouse summarizes its findings and conclusions as to whether and how each resiliency measure achieves Resiliency Plan objectives.
- **Benchmarking** – Guidehouse identified applicable sections of the peer utility benchmarking survey to identify similarities with industry best practice.

Q. WHICH RESILIENCY MEASURES IN CENTERPOINT HOUSTON'S RESILIENCY PLAN ARE YOU ADDRESSING IN YOUR TESTIMONY?

A. Guidehouse evaluated the following five technology resiliency measures considered for inclusion in CenterPoint Houston's Resiliency Plan as outlined in Mr. Bhar's testimony:

- Voice and Mobile Data Radio System Refresh
- Backhaul Microwave Communications
- Data Center Refresh
- Network Security & Vulnerability Management
- IT/OT – Cybersecurity Monitoring

BENEFITS ANALYSIS

Q. WHAT WAS THE PURPOSE OF THE BENEFIT ANALYSIS CONDUCTED FOR CERTAIN RESILIENCY INVESTMENTS INCLUDED IN CENTERPOINT HOUSTON'S RESILIENCY PLAN?

A. Guidehouse performed a comparative analysis for the technology to determine the effectiveness of the five Technology resiliency measures to address the identified physical security and cybersecurity threats, hazards, and vulnerabilities and support the overall resiliency of the CenterPoint Houston electric delivery system.

Q. PLEASE SUMMARIZE THE FINDINGS OF THE BENEFIT ANALYSIS AND HOW THIS PROVIDES AN INDICATOR OF POTENTIAL VALUE OF RESILIENCY INVESTMENTS TO CUSTOMERS AND COMMUNITIES SERVED BY CENTERPOINT HOUSTON.

A. Guidehouse found evidence of resiliency measure effectiveness for each of the five technology resiliency measures (see Section V for details) that add potential value to customers and communities served by CenterPoint Houston. The IT/OT – Cybersecurity Monitoring and the Network Security & Vulnerability Management resiliency investments provide direct value to consumers and communities by improving CenterPoint Houston's ability to detect, deter, and defend against cyber attacks that could adversely impact CenterPoint Houston's electric delivery system. The other four technology resiliency measures also provide direct value as enabling technologies to support efficient and effective customer services. The two communications resiliency measures, Backhaul Microwave Communications and Voice & Mobile Data Radio System Refresh, provide upgraded communications capability to facilitate and expedite system restoration efforts for weather related and other resiliency events, as described in Mr. Shlatz' testimony. The

final technology resiliency measure, Data Center Refresh, replaces end-of-life systems with upgraded functionality, including predictive maintenance, asset management, and other critical functions that increase CenterPoint Houston's capabilities within its operating environment. In summation, Guidehouse found the five technology resiliency measures provide more effective operational capabilities and represent diverse resiliency investments and enabling technologies that add potential value to customers and communities served by CenterPoint Houston.

Q. WHAT RECOMMENDATIONS WERE PROVIDED TO CENTERPOINT HOUSTON FOR CONSIDERATION IN THE DEVELOPMENT OF ITS RESILIENCY PLAN BASED ON THE BENEFIT ANALYSIS?

A. Guidehouse provided a series of recommendations for each of the technology resiliency measures (see Section VII for details) and recommended CenterPoint Houston consider these functions are integrated into the development of the five resiliency measures. These recommendations include:

1. Voice and Mobile Data Refresh – Field Devices: Ensure all legacy technology is properly tracked and decommissioned as it is replaced to avoid latency on the system and unprotected attack vectors;
2. Backhaul Microwave Communication Device Migration: Develop settings checklists or asset configuration guides to remove the opportunity for misconfigurations; and
3. Data Center Refresh: Consider interactions between upgraded hardware and software with legacy systems and applications to avoid migration issues;

4. Networking, Vulnerability, and Security – Data Management: Investigate encryption for data-in-transit for legacy applications, align vulnerability reviews and network analysis processes to industry best practices;
5. IT/OT Cybersecurity Monitoring: Provide user awareness and support training for the new technologies to maximize system benefits.

Q. DID CENTERPOINT HOUSTON MAKE MODIFICATIONS TO ITS RESILIENCY PLAN BASED ON THE FINDINGS AND RECOMMENDATIONS PROVIDED BY GUIDEHOUSE?

A. CenterPoint Houston used the Guidehouse analysis to make adjustments to its plan as stated in Mr. Tutunjian's testimony. For example, as noted in CenterPoint Houston's Resiliency Plan, CenterPoint Houston collaborated with Guidehouse to identify alternatives and metrics included in their Resiliency Plan. It is also my understanding that recommendations offered in the Guidehouse report applicable to implementation and future resiliency plans will be considered as CenterPoint Houston works to implement and later refine its Resiliency Plan.

RESILIENCY MEASURE ASSESSMENT

Q. PLEASE PROVIDE YOUR ASSESSMENT OF RESILIENCY MEASURES FOR WHICH CENTERPOINT HOUSTON SEEKS COMMISSION APPROVAL IN ITS RESILIENCY PLAN?

A. My assessment of each CenterPoint Houston technology or cybersecurity resiliency measure is presented in my responses to the following five sets of questions, in the order presented below starting with the Voice and Mobile Data Radio System Refresh resiliency

measure. For each, I address each of the evaluation categories outlined in my prior responses in this section of my testimony.

- Voice and Mobile Data Radio System Refresh
- Backhaul Microwave Communications
- Data Center Refresh
- Network Security & Vulnerability Management
- IT/OT – Cybersecurity Monitoring

Q. PLEASE DESCRIBE CENTERPOINT HOUSTON'S VOICE AND MOBILE DATA RADIO SYSTEM REFRESH RESILIENCY MEASURE.

A. CenterPoint Houston's Voice and Mobile Data Radio System Refresh resiliency measure will upgrade its current communication system to achieve increased resilience in day-to-day operations, facilitate improved 911 dispatching, and enhance field work coordination with the command center. CenterPoint currently has a disparate communication system that includes cell phones and multiple manufacturers and models of radios including handhelds and truck radios. The fleet radios are the primary method used for communication within the organization for field work. CenterPoint has had recent issues with obtaining replacement parts for outdated radio equipment. This resiliency measure will consist of an upgrade to outdated equipment that has been in service for 13+ years and considered end of life or no longer has replacement parts readily available. This phased upgrade will improve CenterPoint Houston's ability to maintain or restore communication during extreme weather events if failure of radio equipment occurs. Additionally, the resiliency measure involves connecting all CenterPoint field personnel with radios to the upgraded communication system for more universal coverage.

Q. WHAT ALTERNATIVES WERE CONSIDERED IN CENTERPOINT HOUSTON'S EVALUATION OF VOICE AND MOBILE DATA RADIO SYSTEM REFRESH RESILIENCY MEASURE REQUIREMENTS?

A. Centerpoint Houston considered a private Long Term Evolution ("LTE") communication system but determined it could not be adopted in time to meet short-term and mid-term communication needs. CenterPoint Houston determined there were no viable alternatives except the refresh initiative. Alternatives examined included a Project 25 (P25) or Digital Mobile Radio ("DMR") system in Land Mobile Radio ("LMR"), but the need from the LMR communications system is still the same, which is portability for mobile radio coverage and connectivity through a dispatch console system. Guidehouse agrees with CenterPoint Houston that the Voice and Mobile Data Radio System Refresh resiliency measure is the most feasible approach to obtain the desired communications improvements and resiliency benefits.

Q. WHAT METRICS DOES CENTERPOINT HOUSTON PROPOSE TO MEASURE AND TRACK THE EFFECTIVENESS OF THE VOICE AND MOBILE DATA RADIO SYSTEM REFRESH RESILIENCY MEASURE?

A. In the absence of quantitative data to measure the potential effectiveness of the Voice and Mobile Data Radio System Refresh, Guidehouse used qualitative metrics in a comparative analysis with the NIST CSF to determine key performance indicators ("KPIs") associated with the resiliency measure. These KPIs measure CenterPoint Houston's upgraded system's alignment with the CSF functions and specific categories that support better resiliency for IT, OT, and cyber systems. CenterPoint Houston also plans to use the

following performance metrics for tracking the effectiveness of the Voice and Mobile Data Radio System Refresh resiliency measure:

- Dispatch speed,
- Field tests completed,
- Remoteness of communications, Decrease in maintenance time,
- Annual number of End-of-life equipment replacements to:
    - Maintain continuity,
    - Avoid truck rolls, and
    - Integrate GPS tracking and text messaging.

Q. WHAT BENEFITS WILL BE REALIZED FROM CENTERPOINT HOUSTON'S VOICE AND MOBILE DATA RADIO SYSTEM REFRESH RESILIENCY MEASURE?

A. Based on a comparative analysis of the Voice and Mobile Data Radio System Refresh resiliency measure against the NISF CSF framework, Guidehouse determined that CenterPoint Houston's proposed resiliency measure offers additional features that will support the resiliency of CenterPoint Houston's electric system. All determinations below are based on CenterPoint Houston information on resiliency measure descriptions, interviews, and responses to data requests for additional resiliency measure details.

The analysis identified the following categories and results where the category and associated subcategory(ies) have a high correlation:

- **Risk Assessment (ID.RA)**: CenterPoint Houston plans to upgrade its communication system to address a key identified vulnerability that some equipment will no longer be supported. Without the upgrade, field personnel may

have to perform their duties without communication devices, which would adversely impact power operation responses, especially during extreme weather events.

- **Risk Management Strategy (ID.RM)**: CenterPoint Houston identified a risk of failure to radio components that are end of life, which would disable communication or reduce communication coverage size, causing a failure in communication in some locations. This would, in turn, negatively impact system restoration efforts. Therefore, this resiliency measure will help address and mitigate potential risk to system operations and restoration.
- **Access Control (PR.AC)**: CenterPoint Houston has leased sites that are more susceptible to physical security issues, especially where a telecommunications shelter is involved. The resiliency measure upgrades would potentially remove the need for those leased sites and introduce vendors and capabilities for better coverage.
- **Data Security (PR.DS)**: CenterPoint Houston plans to strengthen integrity verification and availability, including adequate communication capacity, based on information provided from each vendor in the Request for Proposal process. CenterPoint Houston requires potential vendors to be able to maintain coverage, at a minimum, and, if possible, reduce base station sites to reduce the physical footprint for the mobility coverage area.
- **Information Protection Processes and Procedures (PR.IP):** CenterPoint Houston plans to implement improved capabilities for managing the baseline configurations when resetting radios that have been changed (e.g., system crash).

This resiliency measure includes this additional functionality while also potentially re-signing co-channeling agreements with third parties to address frequency usage.

- **Protected Technology (PR.PT):** CenterPoint Houston plans to perform periodic checks of equipment and grounding testing to ensure the devices are functioning correctly as part of this resiliency measure. Additionally, there will be improved communication load balancing and backup systems used in instances of device/equipment failures.
- **Communications (RS.CO)**: CenterPoint Houston plans to continue to use the radio system for communications specific to incident investigations and field coordination for responding to impacts from extreme weather events. Radio is also the method used to report incidents.
- **Communications (RS.CO):** CenterPoint Houston plans to continue to use the radio system for communication and coordination activities specific to recovery and system restoration activities and will have third-party agreements in place for equipment warranties, maintenance, and support.

Q. PLEASE PROVIDE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S PROPOSED VOICE AND MOBILE DATA RADIO SYSTEM REFRESH RESILIENCY MEASURE.

A. The Guidehouse team concluded that CenterPoint Houston's Voice and Mobile Data Radio System Refresh resiliency measure has a high level of correlation with system and business resilience and system restoration. This resiliency measure represents the most feasible approach to obtain the desired communications improvements in support of resiliency of CenterPoint Houston's electric system during normal and emergency operations The Voice

and Mobile Data Radio Refresh Resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's Resiliency Plan, as the resiliency measure supports a stronger and more resilient electric transmission and distribution system by providing:

- Better mobile radio coverage across CenterPoint Houston's service area,
- Improved risk management by replacing outdated and end-of-life communications equipment with newer vendor-supported technology,
- Better data security, integrity, and availability across CenterPoint Houston communication channels
- Consistent communications between CenterPoint Houston control centers and field personnel, which will expedite and facilitate timely customer outage restorations
- Redundant and backup power sources for communication facilities during emergency operations

In addition, we find that CenterPoint Houston's proposed Voice and Mobile Data Radio Refresh resiliency measure is consistent with resiliency practices deployed at other utilities, based on Guidehouse experience and peer utility benchmarking survey results described in Section VI.

Q. PLEASE DESCRIBE CENTERPOINT HOUSTON'S BACKHAUL MICROWAVE COMMUNICATIONS RESILIENCY MEASURE.

A. CenterPoint Houston's Backhaul Microwave Communication resiliency measure will replace end-of-life microwave equipment used for large data transfer with standardized units, the goal of which is to facilitate improved maintenance, repair, and replacement

procedures, and includes the communication for dispatching crews for blue sky and weather events. This initiative will streamline operations by minimizing the need for personnel to carry multiple pieces of technology and maintain multiple system platforms. The implementation will also enable CenterPoint to deploy firmware updates from a central location. Backhaul support will extend to CenterPoint's transmission and distribution operations and service centers as a primary or secondary method of data communication between facilities. Additionally, the Backhaul Microwave Communication system will support the transfer of information from substations to CenterPoint personnel. The microwave system is a backup system for monitoring and controlling field devices where there is fiber optic control and as a primary system at sites that are not fiber compatible. In addition, resiliency measures for protecting the microwave sites from flooding and other extreme weather events are included in the Operations resiliency measures addressed in Mr. Shlatz's testimony.

Q. WHAT ALTERNATIVES WERE CONSIDERED IN CENTERPOINT HOUSTON'S EVALUATION OF BACKHAUL MICROWAVE COMMUNICATIONS RESILIENCY MEASURE REQUIREMENTS?

A. Mr. Bahr stated CenterPoint Houston's communications system was designed to have two communication paths to support redundancy and reliability, both of which support resiliency. CenterPoint Houston considered multiple communication alternatives when evaluating this resiliency measure. The primary alternative would be use of fiber optics at all facilities and assets. While a desirable alternative, CenterPoint determined this option is not feasible due to cost and difficulty of creating fiber optics connections to remote locations and assets. CenterPoint, however, does have fiber to many of its locations and, in

those locations, it is the primary communication method used. For facilities that are not fiber compatible, CenterPoint currently has in place older microwave communication equipment. For these facilities, CenterPoint considered simply maintaining the existing equipment. CenterPoint determined that it needs to acquire updated equipment because of lack of support due to end-of-life status, reducing the need to maintain multiple equipment platforms, and utilizing features that currently cannot be used due to technological incompatibilities between the different platforms.

After considering these alternatives, CenterPoint concluded that purchasing a modern backhaul microware system for communication needs at its locations and assets was the most resilient and efficient communication option for the organization and provided redundancy for the fiber control network in critical locations. The use of such modern equipment would eliminate the end-of-life issues related to CenterPoint's existing equipment that are not fiber compatible.

Q. WHAT METRICS DOES CENTERPOINT HOUSTON PROPOSE TO MEASURE AND TRACK THE EFFECTIVENESS OF THE BACKHAUL MICROWAVE COMMUNICATIONS RESILIENCY MEASURE?

A. Guidehouse reviewed CenterPoint Houston's Backhaul Microwave Resiliency measure using a qualitative comparative analysis. A quantitative analysis was not conducted due to data limitations and lack of metrics to benchmark against. Guidehouse evaluated the benefits and features associated with CenterPoint's proposed Backhaul Microwave resiliency measure on a qualitative basis with resiliency measure-specific inputs and assumptions. This analysis compared CenterPoint's resiliency measure with the NIST CSF to identify levels of correlation between the five CSF Functions (Identify, Detect, Protect,

Respond, and Recover), and the proposed system in terms of developing resilient systems. Guidehouse determined whether the resiliency measure had high, medium, or low correlations to the individual subcategories of the CSF. For this report, Guidehouse is only reporting on features, applications, or business processes with a high or, in some instances, medium correlation to subcategories of the NIST CSF.

The subcategories selected for reporting from the medium correlations were selected based on Guidehouse's professional judgment and conclusion that the resiliency measure had a partial or indirect correlation, along with Guidehouse's professional judgment that the resiliency measure was sufficiently implementing the intent of the subcategory from a resiliency perspective. The system features that were mapping to low correlation were considered to be relatively ineffective at improving resiliency, although depending on the context of the proposed resiliency measure, they may still have value in pursuing from reliability or policy perspectives.

CenterPoint Houston also plans to use the following performance metrics for tracking the effectiveness of the Backhaul Microwave Communications resiliency measure:

- Amount of end-of-life equipment replaced by modern vendor-supported systems,
- Decrease in maintenance time, and
- Increased collection of data points.

Q. WHAT BENEFITS WILL BE REALIZED FROM CENTERPOINT HOUSTON'S BACKHAUL MICROWAVE COMMUNICATIONS RESILIENCY MEASURE?

A. Guidehouse evaluated the benefits associated with CenterPoint Houston's proposed Network Security and Vulnerability Management Resiliency measure Guidehouse's

analysis indicates that the resiliency measure will provide a high level of effectiveness for detecting of threats to the system. Based on the results of a comparative analysis, Guidehouse determined that the resiliency measure offers resiliency benefits. All determinations below are based on CenterPoint Houston information on resiliency measure descriptions, interviews, and responses to data requests for additional resiliency measure details.

The analysis identified the following CSF categories and results where the category and associated subcategories have a high and medium correlation to the Backhaul Microwave Communications resiliency measure:

- **Asset Management (ID.AM)**: Guidehouse determined CenterPoint Houston will replace end-of-life microwave equipment to create a standard microwave system. This will inherently require identifying all end-of-life equipment as well as new replacement equipment. This practice should lead to a better repair and maintenance resiliency measure, improving resiliency. Replacing end-of-life radios with new equipment offers several key benefits to CenterPoint Houston. Enhancing reliability by providing improved performance and reducing the frequency of equipment failures, while minimizing disruptions to CenterPoint Houston. Investing in new radio equipment will strengthen the communication infrastructure while enhancing resiliency through redundant communication paths to critical locations.
- **Business Environment (ID.BE)**: Guidehouse determined the microwave system is used for (a) data communication into the SCADA system, (b) assisting with supporting meters for industrial business, (c) improving security by providing video

feeds from some substation locations, and (d) improving system health by sending traveling wave data, data from digital fault recorders, and monitoring capacitor banks in the field. As part of the Backhaul Microwave Communications refresh, CenterPoint will be deploying a microwave management system that focuses on the health of the microwave system and allows for maintaining consistency on the latest firmware released by the vendor, adding additional support for delivering critical services and enhancing resiliency for the CenterPoint Houston electrical delivery system.

- **Risk Assessment (ID.RA)**: Guidehouse determined CenterPoint Houston will perform risk assessment of the vendor and the product, prior to introducing the new equipment into production. The evaluation includes a technical assessment of vulnerabilities to be performed in the test environment. This assessment will verify whether there are any components that are communicating outside of the desired parameters and will also include a vulnerability assessment to determine if there are any potential weaknesses that could impact their performance. Additionally, the evaluation plays a crucial role in enhancing resilience by identifying potential risks that could adversely impact CenterPoint Houston operations. Leveraging evaluation findings enables proactive measures to mitigate risk, enhancing robust systems, and ensuring continuity of operations. Overall, integrating evaluation processes into resiliency strategies will empower CenterPoint to better understand existing vulnerabilities and threat vectors.
- **Supply Chain Risk Management (ID.SC)**: Guidehouse determined CenterPoint Houston stated they would not only evaluate or assess the product prior to bringing

it to production, but also assess vendor supply chain risk. This is a vital step to supply chain quality and security and adds an additional layer of resiliency to their overall system as the microwave technology plays an important role in data communication.

- **Access Control (PR.AC)**: Guidehouse determined CenterPoint Houston will place all new equipment inside physical barriers with additional controls such as a substation fence, cyber keys, login access requirements, and individual key assignments that only allow privileged users access to the equipment. Additionally, the system upgrades will improve remote access management as it will include a universal platform that will standardize the microwave system and introduce advanced capabilities such as remote control, monitoring, and troubleshooting. Older equipment that will be removed does not have these capabilities. These improved access controls will protect the system and increase system capabilities that further improve resiliency.
- **Data Security (PR.DS)**: Guidehouse determined the Backhaul Microwave Communications system will have the ability to encrypt data that moves through it using the Internet Protocol Security ("IPSec") suite. By replacing incompatible microwave technology that currently exists, CenterPoint Houston will have the ability to leverage the stronger data security technology to avoid interception and possible modification of critical operational data. Additionally, the new equipment will replace end-of-life equipment and provide for a more resilient communication pathway ensuring the availability of data transfers. CenterPoint Houston will also

be testing the new equipment in their test environment to ensure the systems are as secure as possible prior to introducing them to production.

- **Information Protection Processes and Procedures (PR.IP)**: Guidehouse determined CenterPoint Houston's efforts to enhance protection processes are under consideration, with plans to incorporate IPSec encryption into new equipment. IPSec encryption for backhaul microwave networks requires system compatibility to encrypt data packets and transmit them securely over the wireless links. While the full implementation of encryption capabilities is contingent upon further evaluation, a significant portion of vendor-selected systems is expected to support IPsec tunnel encryption. The potential utilization of microwave encryption with the new system presents an opportunity for further resiliency, with plans to standardize and improve microwave encryption capabilities in the future by strengthening bulk encryption measures.
- **Maintenance (PR.MA)**: Guidehouse determined CenterPoint Houston will execute the maintenance and repair interventions whenever issues arise. It is noteworthy to mention that there is a predetermined resiliency measure specifically dedicated to managing maintenance and repairs for radio links. An approval process is in place for maintenance and repair tasks.
- **Protective Technology (PR.PT)**: Guidehouse determined integration of recloser devices with remote operation capabilities will impact CenterPoint Houston's Advanced Distribution Maintenance System ("ADMS"). This integration has the potential to necessitate an increase in communication system capacity, a factor that flows beyond the current scope of operations. It is imperative to consider the

relationship between the backhaul microwave system and remote operations. The remote operation functionality predominantly serves purposes relating to the remote control within the intelligent grid switching device system. The backhaul microwave system plays a crucial role in facilitating remote operations by providing the necessary communication infrastructure for transmitting control signals between the intelligent grid switching device and the ADMS. Any enhancement or modifications to the backhaul microwave system directly impacts the ability to perform remote operations effectively. Enhancing communications redundancy is one of the key objectives of this resiliency measure, aligning with CenterPoint Houston's overall goal of improving system reliability and resiliency.

- **Security Continuous Monitoring (DE.CM)**: Guidehouse determined CenterPoint Houston's scrutiny extends to the physical environment, where security cameras are integrated with the backhaul microwave system and play a crucial role in detecting potential cybersecurity threats. Having access to the video feeds allows CenterPoint Houston personnel to respond to a potential threat. The Backhaul Microwave Resiliency measure will enhance video feeds by improving communication throughput and provide a redundant communication line that assist with ensuring critical security video feeds are available for surveillance.

Q. PLEASE PROVIDE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S PROPOSED BACKHAUL MICROWAVE COMMUNICATIONS RESILIENCY MEASURE.

A. Guidehouse concludes that CenterPoint's IT – Backhaul Microwave Communication Resiliency measure provides resiliency benefits. I concur with this determination that

CenterPoint Houston's Backhaul Microwave Communications resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's Resiliency Plan for the following reasons:

- Primarily, the resiliency measure is aimed at reducing communication loss and control for critical electrical systems.
- Redundancy is one of the primary methods for ensuring a resilient electric delivery service. The goal of the Backhaul Microwave Communications resiliency measure is to implement a robust secondary method of communication available under system duress caused by extreme weather or cybersecurity events, which will reduce the risk of losing critical data and control from remote locations if the fiber control network fails.
- System recovery will also improve as the redundancy that the microwave system provides would allow for business continuity and a clearer view of communications link failures.
- The proposed resiliency measure is consistent with resiliency practices deployed at other utilities, based on Guidehouse experience and peer utility benchmarking survey results described in Section VI.

Q. PLEASE DESCRIBE CENTERPOINT HOUSTON'S DATA CENTER REFRESH RESILIENCY MEASURE.

A. CenterPoint Houston's Data Center Refresh resiliency measure addresses the following aspects to support resiliency of its transmission and distribution systems:

- Updating existing processes from manual connection and router adjustment between centers to an automatic turnover system to increase the resilience of cloud-based data centers.
- Improving application recovery and introducing a comprehensive cloud-based tool for recovery plan management.
- Transitioning to newer Intel-based server hardware, specifically Gen 11, increasing availability and reducing failure susceptibility.
- A comprehensive redesign of the complex Storage Area Network ("SAN") Fabric Storage network across the fiber network. The current setup involves various vendors and isolated storage pockets and unnecessary fabrics. The resiliency measure will eliminate isolated storage packets, enhancing the system's efficiency.
- Developing a single storage platform that will allow for multi-protocol usage as well as cloud native capabilities of replication, tiering, and archiving.

The infrastructure will be implemented to support replacement technology to perform transmission and distribution operations functions and will include KPIs and additional metrics to monitor key attributes to assess resiliency measure effectiveness and reliability. The combination of aspects of this resiliency measure, which in most cases begins implementation 2024, even if some of it is just planning, offers a more sustainable infrastructure. The resiliency measure addresses issues and concerns with outdated systems, applications, and equipment, while also streamlining processes to provide efficiency. The implementation will last three years, with automated failover being the fastest component, taking one year, all aligned with the broader objective of enhancing grid resilience.

CenterPoint Houston plans to shift from an on-premises data center model to a hybrid model that will enhance grid resiliency through improved response and recovery capabilities, ultimately minimizing risks related to service interruptions.

Q. WHAT ALTERNATIVES WERE CONSIDERED IN CENTERPOINT HOUSTON'S EVALUATION OF DATA CENTER REFRESH RESILIENCY MEASURE REQUIREMENTS?

A. CenterPoint Houston considered various alternatives from three vendors - Dell, HP, and IBM - to address the introduction of new Cisco switches. They aimed to enable automatic failover to replace the current equipment lacking this capability and to ensure uninterrupted operations. The determining factors were compatibility for hybrid cloud and the skill set within the personnel.

CenterPoint Houston will migrate their IBM-HP equipment into Intel-based systems to increase system agility. This resiliency measure will allow CenterPoint Houston to implement a modern system that can become a hybrid with the cloud and have the capability to transition into full cloud. Feasible alternatives depended on the vendors and the products that are being offered.

CenterPoint Houston will also migrate many of their legacy applications into a cloud solution to improve the ability to recover them. Some legacy software cannot simply be moved to the cloud and will need alternative options for recovery, while CenterPoint Houston determines what can and cannot be moved to the cloud. The alternatives are to keep on premises replication or move to a hybrid solution.

Q. WHAT METRICS DOES CENTERPOINT HOUSTON PROPOSE TO MEASURE AND TRACK THE EFFECTIVENESS OF THE DATA CENTER REFRESH RESILIENCY MEASURE?

A. Guidehouse evaluated the benefits and features associated with CenterPoint Houston's proposed Data Center Refresh resiliency measure on a qualitative basis with resiliency measure-specific inputs and assumptions. This analysis compared CenterPoint Houston's resiliency measure with the NIST CSF to identify levels of correlation between the five CSF Functions (Identify, Detect, Protect, Respond, and Recover) and the proposed system in terms of developing resilient systems. Guidehouse performed the analysis and identified whether the resiliency measure had high, medium, or low correlations to the individual subcategories of the CSF. For the purpose of this report, Guidehouse is only reporting on features, applications, or business processes with a high or, in some instances, medium correlation to subcategories of the NIST CSF.

The subcategories selected for reporting from the medium correlations were selected based on Guidehouse's professional judgment and conclusion that the resiliency measure had a partial or indirect correlation, along with Guidehouse's professional judgment that the resiliency measure was sufficiently implementing the intent of the subcategory from a resiliency perspective. The system features that were mapping to low correlation were considered to be relatively ineffective in improving resiliency, although depending on the context of the proposed resiliency measure, they may still have value in pursuing from reliability or policy perspectives.

CenterPoint Houston also plans to use the following performance metrics for tracking the effectiveness of the Data Center Refresh resiliency measure in moving from an on-premises model to a cloud-based model:

- Number of replaced systems,
- Number of manual processes replaced by automation,
- Decreased storage footprint (on premises) vs. Increased resource management/storage efficiency improvements (cloud-based system)
- Decreased data compression rates, and
- Decreased application recovery time

Q. WHAT BENEFITS WILL BE REALIZED FROM CENTERPOINT HOUSTON'S DATA CENTER REFRESH RESILIENCY MEASURE?

A. Guidehouse evaluated the benefits associated with CenterPoint Houston's proposed Data Center Refresh resiliency measure and determined that the resiliency measure will provide a high level of effectiveness. Based on the results of a comparative analysis, Guidehouse determined that the resiliency measure offers resiliency benefits. All determinations below are based on CenterPoint Houston information on resiliency measure descriptions, interviews, and responses to data requests for additional details.

The analysis identified the following categories and results where the category and associated subcategory(ies) have a high correlation to the resiliency measure:

- **Asset Management (ID.AM)**: Guidehouse determined CenterPoint Houston plans to move existing on premises services to cloud-based applications in a SaaS application or directly into a cloud space such as Azure for clients and personnel. It plans to continue on-premises as needed until they can transition to a fully cloud

model, if possible, or continue in a hybrid platform. Additionally, data flows will be improved through the implementation of new Cisco switches aimed at automatic failure prevention. CenterPoint Houston plans to transition from their aging IBM HP hardware to a more modern Intel-based server hardware that can add security features and provide for a hybrid (on premises and cloud) environment showing their prioritization for critical systems. The useful life of these assets typically spans six years, though in some cases, it extends to seven years.

- **Business Environment (ID.BE)**: Guidehouse determined CenterPoint Houston highlights the comprehensive understanding and prioritization of its critical system and their dependencies and critical functions by improving their failover capabilities and recovery and redundancy for some of their software services through this resiliency measure. Specifically, the Cisco upgrade aspect of this resiliency measure emphasizes the importance of enhancing the availability of their data centers and transitioning to an automatic failover solution from the primary to their backup center. CenterPoint Houston's focus on increasing resilience includes improving software application availability by migrating to the cloud or a hybrid solution where a full cloud solution is not possible.
- **Governance (ID.GV)**: Guidehouse determined CenterPoint Houston highlighted cybersecurity roles and responsibilities for both internal personnel and external partners and provided assurance of defined and controlled access processes during implementation, including formal request and approval procedures. CenterPoint Houston has an access provisioning system that would be leveraged and a physical

escorting process that would ensure only those approved will have electronic or physical access to the systems included in this resiliency measure.

- **Risk Assessment (ID.RA)**: Guidehouse determined CenterPoint Houston demonstrates an understanding of cybersecurity risks pertaining to its operational functions and asset protection. Threats are identified, documented, and prioritized for risk response using the vulnerability assessment tool prior to introducing new hardware into production. CenterPoint Houston also identified manual failover mechanisms between data centers as a risk due to reduced recovery capacity and increased downtime. CenterPoint Houston prioritized an automated method for failing over between data centers, which demonstrates a proactive approach to mitigating risks.
- **Access Control (PR.AC)**: Guidehouse determined CenterPoint Houston employs robust access control measures to manage both physical and logical asset access, ensuring that only authorized users, processes, or devices are granted entry, aligning with assessed risks of unauthorized access. Remote access is limited to company storage personnel and relevant management teams, with some least privilege principles applied, to ensure individuals have the least number of privileges necessary to perform their tasks. Third-party access follows a formal account creation and approval process, with regular recertification and manual removal capabilities. Network segmentation is implemented across the enterprise and is continually considered for enhancement. Overall, CenterPoint Houston maintains effective access management practices, prioritizing security and risk mitigation.

- **Data Security (PR.DS)**: Guidehouse determined CenterPoint Houston's information management and security strategy aligns with its risk strategy, emphasizing the protection of data confidentiality, integrity, and availability. CenterPoint Houston implements Self Encrypting Drives ("SEDs") in program aspects like the SAN Fabric to safeguard data-at-rest, complemented by a software layer for monitoring traffic within the SAP environment.

CenterPoint Houston in-transit data is mostly internal traffic that is secured through network segmentation. A subset of their system employs encryption tools such as PGP with a global key manager. Additionally, they encrypt the traffic from the firewalls to the logs servers that aggregate network logs. CenterPoint Houston includes proper disposal procedures like shredding drives prior to disposal to protect the data. Furthermore, CenterPoint Houston is increasing system availability by upgrading to an automated failover for data centers, transitioning software into a cloud or hybrid solution as well as increasing storage capacity with the SAN fabric upgrade. CenterPoint Houston utilizes a test environment for testing new equipment and making vendor updates when applicable before deployment into production.

- **Information Protection Processes and Procedures (PR.IP)**: Guidehouse determined CenterPoint Houston establishes baseline configuration for its IT and industrial control systems, incorporating security principles like the concept of least functionality which provides only essential capabilities and prohibits or restricts the use of non-essential functions, though it lacks ongoing maintenance and historical tracking within programs.

CenterPoint Houston leverages data lifecycle techniques, such as change management, backup and retention procedures, and data destruction techniques. For change management processes, baselines are established before implementation begins, but will be adjusted as needed during the upgrade. Backups are made at the application and file level and are included in the disaster recovery process. For retention, copies of application/file information are triplicated and follow CenterPoint Houston's data retention policy. CenterPoint Houston plans to enhance data protection by shredding drives upon equipment and hardware decommissioning, collapsing storage SAN fabrics, and integrating virtual SAN fabrics into other devices within the SAN fabric program to lessen the attack radius of external threats.

- **Protective Technology (PR.PT)**: Guidehouse determined CenterPoint Houston prioritizes the protection of its communications and control networks by implementing a range of security measures, including electronic and physical access controls such as authentication, encryption, and other security features.

Network security and cybersecurity teams at CenterPoint Houston are responsible for managing the protection of network devices involved in these programs, ensuring robust safeguards are in place. Additionally, the primary objective of the Cisco upgrade is to improve fail-over capabilities, particularly for the automatic failover program, demonstrating CenterPoint Houston's dedication to maintain network resilience and continuity in the face of potential disruptions. CenterPoint Houston also leverages the use of authentication mechanisms for physical and logical access, as well as encryption for data management, and will continue to do so.

- **Improvements (RC.IM)**: Guidehouse determined CenterPoint Houston will improve its ability to recover its applications in Business Continuity and Disaster Recovery ("BCDR") situations through this program. CenterPoint Houston intends to move to a cloud solution where it is possible for many of its applications. On premises replication and recovery is currently in place and moving towards development of a Hybrid Cloud (Cloud and On-Premises) BCDR strategy, with intentions of full cloud migration. The data center automated failover program will also improve the recovery strategy in a case where one of CenterPoint Houston's data centers becomes unavailable. The current manual processes involve identifying the issue and manually contacting someone to perform the necessary steps, estimated to take around three hours. The automated recovery will greatly improve system availability, further making the CenterPoint Houston system more resilient.

Q. PLEASE PROVIDE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S PROPOSED DATA CENTER REFRESH RESILIENCY MEASURE.

A. Guidehouse concludes there is a high level of correlation with critical CSF system and business resilience and system restoration practices with CenterPoint Houston's Data Center Refresh resiliency measure. I concur with this determination. Particular areas in which this resiliency measure supports a strong and resilient electric transmission and distribution system include enhancements in the following practice areas:

- Business Environment
- Governance
- Access Control

- Data Security
- Protective Technology
- Improvements

- I concur upgrading outdated equipment and implementing solutions that improve system availability through enhanced recovery solutions represent stronger resiliency efforts that will be provided by the Data Center Refresh resiliency measure. These practices will ensure CenterPoint Houston maintains a resilient business environment that provides critical services needed for normal operations as well as during system duress or recovery states. Through access control and data security, CenterPoint Houston will continue to protect their system as they upgrade to the latest technology. Moving to a on-premises solution for replication, a hybrid system, or full cloud solution for specific component systems, as applicable, will provide CenterPoint Houston with the ability to recover quickly from a natural disaster or a cybersecurity event using the latest methods of recovery that these solutions provide.
- The proposed Data Center Refresh resiliency measure is consistent with resiliency practices deployed at other utilities, based on Guidehouse experience and peer utility benchmarking survey results described in Section VI.

Q. PLEASE DESCRIBE CENTERPOINT HOUSTON'S NETWORK SECURITY & VULNERABILITY MANAGEMENT RESILIENCY.

A. CenterPoint Houston's Network Security and Vulnerability Management resiliency measure is focused on proactive measures to enhance its cybersecurity posture and align with industry standards and best practices. Through systemic threat detection and

vulnerability scanning processes, CenterPoint Houston identifies and addresses potential weaknesses across endpoint and system environments. CenterPoint Houston's ongoing evaluation of cybersecurity risk includes comprehensive penetration testing to assess the resilience of its infrastructure, ensuring that it stays ahead of emerging threats. Additionally, replacing the end-of-life network equipment allows for CenterPoint Houston to have the latest equipment that is being maintained through updates by the manufacturer.

Application Security: This project will develop and operationalize tools and processes to ensure all application development is completed securely with control of the point of origin/subcomponents of every in-house developed software product. The implementation process consists of assessing the current development environment; understanding gaps in current processes; working with development teams and leadership to evaluate products in the market that facilitate a consistent, measurable, auditable development process that includes software vulnerability scanning during the development process; implementing the chosen cybersecurity application development tool; and implementing process changes to ensure Company objectives are met.

Vulnerability management is a continuous cybersecurity process that includes identifying, evaluating, treating, and reporting software and network vulnerabilities. Properly monitoring and responding to both urgent and complex issues are essential components of vulnerability management and information security. CenterPoint Houston plans to deploy a vulnerability assessment tool to accomplish this. In another resiliency measure, CenterPoint Houston will be upgrading to a Governance, Reliability, and Compliance (GRC) tool to automate its processes and replace its manual compliance processes of using spreadsheets, which will reduce potential data input errors.

Additionally, as part of this resiliency measure, CenterPoint Houston also plans to refresh the hardware for over 200 appliances, firewalls and hardware for critical software such as QRadar and Cyber Ark which are used for threat detection (QRadar) and as a password vault (Cyber Vault) for housing important access management information. Through these hardware refreshes, CenterPoint Houston aims to bolster its resilience against cyber threats, aligning with the broader objective of enhancing grid resilience in an increasingly digital landscape.

Q. WHAT ALTERNATIVES WERE CONSIDERED IN CENTERPOINT HOUSTON'S EVALUATION OF NETWORK SECURITY & VULNERABILITY MANAGEMENT RESILIENCY MEASURE REQUIREMENTS?

A. CenterPoint Houston is in the process of determining the solutions and tools that will be implemented to address vulnerability management and GRC procedures. CenterPoint Houston uses Rapid7, which recently reached its first renewal cycle. CenterPoint Houston is doing its due diligence to consider other vendors and solutions as potential options for replacement for the current application.

Q. WHAT METRICS DOES CENTERPOINT HOUSTON PROPOSE TO MEASURE AND TRACK THE EFFECTIVENESS OF THE NETWORK SECURITY & VULNERABILITY MANAGEMENT RESILIENCY MEASURE?

A. Guidehouse evaluated the benefits and features associated with CenterPoint Houston's proposed Network Security and Vulnerability Management resiliency measure on a qualitative basis with resiliency measure-specific inputs and assumptions. This analysis compared CenterPoint Houston's resiliency measure with the NIST CSF to identify levels