2. **Qualitative Benefits** – The likelihood of insulator flashover is lower than other resiliency measures during most hurricanes when heavy rainfall removes salt contamination buildup. Nonetheless, pre-rain winds during hurricanes and windstorms where minimal rainfall occurs accelerate salt contamination, resulting in the increased likelihood of flashover. When combined with other outage causes during resiliency events, multiple flashovers can lead to lengthy customer interruptions in contamination zones. These events, when combined with other outage causes could result in widespread socio-economic impact to critical coastal area loads, particularly if transmission supply to major substations is interrupted. Similar to other resiliency measures, numerous concurrent flashovers with attendant load loss would lead to heightened political and community concern along coastal regions.

5.6.6.7 Resiliency Measure Assessment and Conclusion

Guidehouse concludes that CenterPoint Houston's Saltwater Contamination resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's SRP for the following reasons:

- The resiliency measure should reduce potential damage to substation equipment and distribution lines.
- Replacing at-risk insulators with polymer or fiberglass devices (and wood poles with fiberglass on distribution circuits) substantially reduces the need and expense for ongoing insulator washing.
- The potential damage and customer interruptions served from substations and distribution circuits located within CenterPoint's contamination zones support the proposed investments. The measure also produces a favorable BCA.
- The installation of flashover resilient insulators in substations and distribution circuits meets CenterPoint Houston's current design standard and equipment selection practices.
- Proactive replacement of at-risk insulators avoids lengthy interruptions to customers located within contamination zones, particularly during resiliency events.

5.6.7 Substation Fire Protection Barriers

5.6.7.1 Resiliency Measure Description

CenterPoint Houston's Substation Fire Barriers resiliency measure is designed to protect power transformers and other equipment vulnerable to damage caused by the catastrophic failure of adjacent transformers. Although substation transformer failures are low compared to other distribution equipment failures (*e.g.*, broken poles), the consequences and impact of a catastrophic failure can be severe. An enormous amount of energy is released when a transformer catastrophically fails, with the possibility of extensive damage to nearby equipment from associated fire and debris. When such an event occurs, there is a high potential for lengthy outages and costly repairs. Extinguishing the fire also presents challenges to fire department personnel.

CenterPoint Houston proposes to install concrete or metal barriers between substation transformers in locations where the impact of a catastrophic failure is high. As discussed in Section 4.2, increased variability and higher temperatures over time increase the risk of transformer failures. Substations targeted for substation fire protection barriers include locations where the magnitude of load at risk is high or those that serve critical customers or facilities (*e.g.*, those serving hospitals or other facilities providing emergency services).

5.6.7.2 Revisions from the Prior System Resiliency Plan

CenterPoint Houston proposes to increase spending on the Substation Fire Protection Barriers measure, which will increase the number of barriers installed over the 3-year Resiliency Plan. Except for the use of a higher VoLL and higher cost of installation, all other values applied to derive benefits in the Prior report remain unchanged. The criteria that will be used to identify and select substations for fire protection barriers also remain unchanged.

5.6.7.3 Resiliency Measure Targets

CenterPoint Houston's proposed SRP quantities and investments are presented below:

- Number of substation fire protection barriers targeted: **12** per year (**36** total at 21 substations)
- Total project cost: **$ 9.0 million** (**$250,000** for each barrier)

5.6.7.4 Alternatives Considered

Alternatives to the substation fire protection barriers are not applicable, as there are no viable alternative options for protecting equipment from catastrophic transformer failures.

5.6.7.5 Resiliency Measure Metrics and Effectiveness

CenterPoint Houston transitioned from an asset-centric program-based approach to a project-based approach using co-optimized sets of project types to address resiliency challenges specific to geographic regions in its service area. Using an array of best practice project type alternatives, different project types were selected in each area to enhance resiliency and structural hardening at a discrete asset level.

Substations and transmission assets mitigations were primarily structural enhancements, such as elevating substations above inundation levels or replacing existing transmission structures with designs capable of withstanding higher wind speeds. The discrete nature of these projects results in efficacy measurements that are more asset-centric.

Measurements:

1. Percent of planned asset installations completed by County
2. Percent of resilient power delivery asset failures projected to fail during a Resiliency Event
3. Percent of resilient power delivery asset failures occurring during a Resiliency Event

5.6.7.6 Benefits Analysis

Guidehouse evaluated the benefits associated with CenterPoint Houston's proposed Substation Fire Barriers resiliency measure on a quantitative and qualitative basis. The quantitative analysis adheres to the BCA methodology described in Section 5.1, with resiliency measure-specific inputs and assumptions described below.

1. **Quantitative Benefits** – Key assumptions include the probability of a transformer failure and the likelihood that the failure will cause adjacent transformers or nearby equipment to fail. For most substations, high temperatures coupled with high through-fault currents place critical equipment at risk of failure. The probability over the next 10 years that a catastrophic failure is likely to occur at one of the 21 substations is 0.2%, with 75% of such events causing damage to adjacent equipment. The average amount of load at risk at substations where fire protection barrier installations are proposed is 75 MW with restoration times averaging 18 hours.

   Benefits include reduced load loss, shorter restoration times, and the high cost of avoided repairs and crew labor required to restore service. Based on these assumptions, the Substation Fire Protection Barriers resiliency measure is projected to reduce cumulative CMIs over the 3-year Resiliency Plan by approximately 1.5 million and 0.7 annually by 2028. Guidehouse derived a composite BCA of 4.0 for the 21 substations targeted for fire protection barriers.

2. **Qualitative Benefits** – The potential for nearby equipment to fail when a power transformer fails catastrophically is high, resulting in lengthy outages to customers served by the substation. Substations serving critical loads, area industries, and businesses could experience disruption in day-to-day operations and economic harm if such an event occurred. Further, a major fire at a substation would likely draw negative media attention, with associated reduced confidence in the electric utility from its customers and the general public. Figure 5-7 presents photographs of a fire that occurred at CenterPoint Houston's Kluge Substation in 2016

Figure 5-7: 2016 Substation Fire

Source: CenterPoint Houston.

5.6.7.7 Resiliency Measure Assessment and Conclusion

Guidehouse concludes that CenterPoint Houston's Substation Fire Barriers resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's SRP for the following reasons:

- The proposed solution effectively avoids major equipment damage due to transformer failures.
- Installation of firewalls at critical substations is a responsible action given the potential consequences of a catastrophic failure.
- The proposed measure is consistent with practices deployed at other utilities based on Guidehouse experience and peer utility benchmarking survey results.
- Installation of firewalls at critical substations also avoids potentially undesirable attention and a loss of confidence in CenterPoint Houston from its customers and the general public.

5.6.8 Digital Substation

5.6.8.1 Resiliency Measure Description

CenterPoint Houston's Digital Substation resiliency measure is in the early stages of design and development. To support this resiliency measure, CenterPoint Houston is evaluating the benefits of adopting increased digitization and automation in accordance with the International Electrotechnical Committee's ("IEC") 61850 communications protocol. The 61850 standard promotes the use of digital equipment, the adoption of cybersecurity measures, and large amounts of data capture to enhance reliability and real-time monitoring of critical substation equipment.

Key features of CenterPoint Houston's Digital Substation resiliency measure include the substitution of copper wiring with less costly fiber optics for easier conversion to digital communications, enhanced situational awareness for better and faster operational decisions, adoption of compact digital protective relays allowing for a more compact substation, standardized configurations for increased speed of installation, centralized communications/data collection busses (*i.e.*, via merging units), enhanced switching via GOOSE protocols,[102] and proactive detection of equipment abnormalities and incipient failure with an overall smaller substation design footprint. These features will help drive down O&M costs, collectively enhance reliability and resiliency, and lower the cost of constructing new substations over time.[103]

[102] Generic Object Oriented Substation Events (GOOSE) protocol provides extremely fast tripping of multiple devices, thus eliminating the need for sequential switching of devices.

[103] Over time, CenterPoint Houston proposes to adopt the IEC 61850 design protocol for all new substations.

5.6.8.2 Revisions from the Prior System Resiliency Plan

CenterPoint Houston proposes to increase spending on the Digital Substation measure to those established in the Prior SRP. Except for using a higher VoLL, all other values applied to derive benefits in Guidehouse's prior report remain unchanged.

5.6.8.3 Resiliency Measure Targets

The estimated three-year cost for this resiliency measure is presented below.

- Number of substations targeted: **4-5** per year (**13** over three years)
- Total project cost: **$31.8 million** for substation equipment[7]

5.6.8.4 Alternatives Considered

In reviewing the SRP, CenterPoint Houston, in collaboration with Guidehouse, determined an alternative is to continue utilizing the analog and copper-based communication system for CenterPoint Houston's substation control houses. The continued use of an analog and copper-based communication system is less secure and more costly than a digital and fiber-based communication system. CenterPoint Houston believes that using a digital and fiber-based communication system is more cost-efficient, has additional operational benefits, and aligns with good utility practices seen within the industry.

5.6.8.5 Resiliency Measure Metrics and Effectiveness

CenterPoint Houston transitioned from an asset-centric program-based approach to a project-based approach using co-optimized sets of project types to address resiliency challenges specific to geographic regions in its service area. Using an array of best practice project type alternatives, different project types were selected in each area to enhance resiliency and structural hardening at a discrete asset level.

Distribution system mitigations are focused on areas of higher predicted damage concentration to maximize overall system restoration efficiency. When optimized at the project level, these mitigations require considering interdependencies between mitigations contemplated for the same distribution feeder/area. For example, strategic undergrounding changes the need for automation and vegetation management frequency. As a result of using the co-optimized project-based approach, CenterPoint Houston will use efficacy measures that capture the complementary nature of project-based system resiliency plans. This approach is consistent with industry best practices and measures success as a product of regional performance instead of individual asset performance.

Measurements:

1. Percent of planned asset installations completed by County
2. Percent change in predicted damage based on the event type.

3. Normalized total system restoration performance during Resiliency Events pre- and post-completion of mitigation projects based on the event type.
4. Normalized restoration performance of predicted high damage concentration area compared to Normalized total system restoration performance pre- and post-completion of mitigation projects during Resiliency Events based on the event type.

5.6.8.6 Benefits Analysis

The benefits associated with CenterPoint Houston's proposed Digital Substation resiliency measure are generally described above. However, because the resiliency measure is in the initial stages of development, quantifying benefits is premature.

1. **Quantitative Benefits** – Although CenterPoint Houston has not collected or estimated benefits related to installing substation components, it proposes to do so as described in the metrics reporting section above. In lieu of such information, benefits used by Guidehouse to calculate a BCA value are the additional time for technicians to drive to substations to obtain event data following faults, reduced outage restoration time resulting from fault locating features of new relays, and reduced relay failures. The Digital Substation resiliency measure is projected to reduce cumulative CMIs over the 3-year Resiliency Plan by approximately 1.2 million and 0.7 million annually by 2027. Using these assumptions, Guidehouse derived a BCA of 1.8.
2. **Qualitative Benefits** – CenterPoint Houston's Digital Substation resiliency measure is designed to transition CenterPoint Houston's substation through digital technology adoption and automation. Specific applications and features of this resiliency measure are highlighted above. The resiliency measure should achieve resiliency benefits by improving system performance during major storms and other extreme weather events through the use of real-time monitoring and visualization. Over the long term, a more compact design with fewer equipment components should lower the cost of new substations, particularly in urban areas with space constraints. It also provides greater flexibility to site new substations due to the smaller space needed to build a substation using digital equipment.

5.6.8.7 Resiliency Measure Assessment and Conclusion

Guidehouse concludes that CenterPoint Houston's Digital Substation resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's SRP for the following reasons:

- The introduction of grid modernization initiatives, such as those associated with digitization and automation, is consistent with leading utility practices based on Guidehouse's experience advising clients in North America and worldwide.[104]

[104] For example, Guidehouse personnel assigned to assess CenterPoint's Resiliency Plan provided detailed grid modernization recommendations, including adoption of the IEC 61850 communications protocol, to the Dubai Electric & Water Authority ("DEWA").

- As implementation proceeds, CenterPoint Houston's Digital Substation resiliency measure should enhance the reliability and resiliency of its system while lowering the footprint and cost of constructing new substations over the longer term.

5.6.9 Wildfire Mitigation

CenterPoint Houston proposes to implement a range of measures that, collectively, will reduce the potential of electric transmission and distribution facilities to provide an ignition source in areas susceptible to wildfires. Areas most susceptible to wildfires are located in the northern and southern sections of CenterPoint Houston's service territory. Most of CenterPoint Houston's transmission and distribution lines and equipment are located in areas designated by Texas A&M as moderate fire hazard zones. The two regions that CenterPoint Houston proposes to address wildfire risk are those designated as higher-risk hazard zones by the USA Wildfire Hazard Potential Risk Index map below. Guidehouse's review and application of Argonne National Laboratory's "Climate Risk and Resilience" tool indicates that the risk of wildfires is projected to increase over the next few decades, particularly during summer months. Although CenterPoint Houston's electric facilities have not been the source of wildfires in the past, the increased risk and potential impact of wildfire events on its customers and regional economy supports the measures CenterPoint Houston proposes to apply to reduce these risks.

CenterPoint Houston's Wildfire Mitigation measure comprises five separate activities, each designed to contribute to the reduction of wildfire detection, reduction in ignition potential, and damage to electric assets. Each of these five activities is described below.

5.6.9.1 Revisions from the Prior System Resiliency Plan

CenterPoint Houston has reduced the number of Wildfire Mitigation measures from 10 to 5, focusing on those expected to reduce ignition risk and minimize customers impacted during wildfire events. The current Plan includes specific quantities of assets that will be upgraded or replaced, and expenses associated with enhanced vegetation management.

5.6.9.2 Resiliency Measure Targets

The estimated three-year cost for this resiliency measure and associated expenses is presented in Table 5-9 for each measure component.

Table 5-9: Wildfire Mitigation Measures

Measure Component	Capital ($ Millions)	Expense ($ Millions)
Wildfire Advanced Analytics	$ -	$ 0.9
Wildfire Strategic Undergrounding	$ 50.0	$ -
Wildfire Vegetation Management	$ -	$ 30.0
Wildfire IGSD	$ 19.4	$ 0.3

As of December 2024, CenterPoint Houston has reduced wildfire risk via prior spending on vegetation management, asset hardening (*e.g.*, replacement of wood structures with steel or

concrete), and IGSD schemes in areas of elevated wildfire risk illustrated in Figure 6-11. CenterPoint Houston has also adjusted protective relay settings to enable operating personnel to block reclosing on circuits or circuit sections in areas where fire authorities have assigned high threat levels. Operational procedures for wildfire events, including implementation of PSPS, are outlined in CenterPoint Houston's Energy Operating Procedures. CenterPoint Houston has formalized its Wildfire Mitigation measures to focus on targeting measures to reduce wildfire risk associated with electric assets acting as an ignition source, minimize the spread of wildfires, reduce the time and expense of ground patrols, and limit the impact of wildfire events on its customers and surrounding areas.

5.6.9.3 Vegetation Management

CenterPoint Houston vegetation management plans for at-risk areas are designed to reduce ignition risk for dominant vegetation species in the northern region and grassland in the south. Mitigation focuses on identifying at-risk areas using LiDAR measurements and analytical models to prioritize trimming and tree and undergrowth removal, along with field inspections of rights-of-way with grasslands and low-lying shrubs to identify areas with higher ignition potential. It is separate from the accelerated Vegetation Management measure presented in Section 5.3.7Tree trimming and removal will target species with higher ignition potential based on informed arborist assessments. Tree removal includes expanding rights-of-way (ROW) to further reduce risk from trees with higher risk of ignition. Further, using input from arborists, CenterPoint Houston will perform bare ground clearing surrounding poles equipped with devices that can act as an ignition source due to hot expulsion fuse drops when clearing faults. CenterPoint Houston will also apply fire retardant material on critical wood poles and structures to reduce damage to utility equipment.

5.6.9.4 Fire Detection Cameras

Control center personnel will use wildfire detection cameras to rapidly detect incipient wildfires. The data obtained from cameras will also be used in conjunction with the Wildfire Modeling and Analytics measure.

5.6.9.5 Wildfire Modeling and Analytics

CenterPoint Houston's Wildfire Modeling and Analytics measure is designed to detect via analytical modeling of wildfire spread potential and conditions and locations where circuits and equipment may contribute to increased wildfire risk. The analytical model(s) will apply data obtained from LiDAR and Digital Twin technology together with inspection and equipment monitoring information to identify high-risk locations with increased granularity. Results obtained from the Wildfire Modeling and Analytics measure will be used in combination with other Wildfire Mitigation measures to determine where to target individual assets for improvement as a means to reduce wildfire risk at lowest cost.

5.6.9.6 Wildfire Strategic Undergrounding

CenterPoint Houston proposes to relocate overhead distribution lines underground in areas of elevated wildfire risk. Most overhead lines selected for undergrounding will be single phase lateral line sections, chosen based on limited accessibility and wildfire potential, along with LiDAR results and analytics. The undergrounding of overhead lines in areas of elevated wildfire risk will have attendant benefits for other resiliency events such as hurricanes. The benefits analysis presented below includes a qualitative assessment of wildfire reduction risk associated with wildfire resiliency events.

5.6.9.7 Wildfire IGSD

CenterPoint Houston proposes to install IGSD schemes to reduce wildfire risk in areas where isolation of circuit sections can reduce wildfire risk and minimize customer interruptions when distribution circuits are de-energized due to activation of Public Safety Power Shutoff (PSPS) protocols. Several of CenterPoint Houston's distribution circuits – typically, longer lines – transition from areas of lower to higher wildfire risk. For circuits where activation of PSPS is confined to specific line segments, IGSD will be installed to isolate shutoff only to high-risk line sections, thus resulting in fewer customers impacted by PSPS. The installation of IGSD schemes as Wildfire Mitigation measures are in addition to those implemented under the stand-alone IGSD measure. Similar to other Wildfire Mitigation measures, IGSD schemes installed in areas of elevated wildfire risk will have attendant benefits for other resiliency events, particularly along coastal areas where hurricane impacts are elevated.

5.6.9.8 Alternatives Considered

With wildfires beginning to be a larger issue in Texas, CenterPoint Houston decided to add wildfire measures within the SRP. The only real alternative to adding these measures is not to provide and prepare for wildfire mitigation. In recent history, there has been a significant uptick in the number of drought and heat days, lending to the higher possibility of fuel for wildfires. Considering this, the risk of wildfire is increasing within CenterPoint Houston's territory, and mitigation measures must begin. The option of not proactively preparing for wildfires was not a viable option due to the increased risk seen within the territory (drought conditions in recent years, wildfire in Brazoria County in 2024, the Smokehouse Creek fire, and most recently, the Los Angeles fires are just a few examples of the risk).

CenterPoint Houston has identified and is proposing four extreme temperature (drought) wildfire Resiliency Measures—each a recognized best practice within the utility industry—as measures most likely to be useful in mitigating the risk of wildfires in CenterPoint Houston's service area and areas outside its service area in which it operates facilities. CenterPoint Houston will consider how all or some of the measures can work in combination to address the specific service area risk confronting CenterPoint Houston most appropriately.

5.6.9.9 Resiliency Measure Metrics and Effectiveness

CenterPoint Houston transitioned from an asset-centric program-based approach to a project-based approach, using co-optimized sets of project types to address resiliency challenges specific to geographic regions in its service area. Using an array of best practice project type alternatives, different project types were selected in each area to enhance resiliency and structural hardening at a discrete asset level.

Distribution system mitigations are focused on areas of higher predicted damage concentration to maximize overall system restoration efficiency. When optimized at the project level, these mitigations require considering interdependencies between mitigations contemplated for the same distribution feeder/area. For example, strategic undergrounding changes the need for automation and vegetation management frequency. As a result of using the co-optimized project-based approach, CenterPoint Houston will use efficacy measures that capture the complementary nature of project-based system resiliency plans. This approach is consistent with industry best practices and measures success as a product of regional performance instead of individual asset performance.

Measurements:

1. Percent of planned asset installations completed by County
2. Percent change in predicted damage based on the event type.
3. Normalized total system restoration performance during Resiliency Events pre- and post-completion of mitigation projects based on the event type.
4. Normalized restoration performance of predicted high damage concentration area compared to Normalized total system restoration performance pre- and post-completion of mitigation projects during Resiliency Events based on the event type.

5.6.9.10 Benefits Analysis

Guidehouse evaluated the benefits associated with CenterPoint Houston's Wildfire Mitigation resiliency measure on a quantitative and qualitative basis. The benefits analysis differs from other resiliency measures in two ways. First, the quantitative analysis for Wildfire Mitigation was derived on a composite basis for the five measure components. Second, the quantification of benefits for wildfire mitigation is not derived as impacts are primarily collateral damage of non-electric assets, along with the economic consequences associated with a wildfire event.

While the incidence of major wildfires in CenterPoint Houston's service territory has been low or non-existent, the likelihood of major wildfires is expected to increase due to climatological conditions outlined in Section 0. The wildfire incident rate in Texas in 2022 was deemed to be among the worst over the past decade.[1] Given the increased risk, the consequences of a major wildfire on the integrity and damage to CenterPoint Houston's transmission and distribution system and interruption of customer load could be severe. It would also result in widespread socio-economic impact on the region and heightened public and media attention.

5.6.9.11 Resiliency Measure Assessment and Conclusion

Given the potential impact of wildfire events within CenterPoint Houston's service territory and the increased risk of wildfire events, Guidehouse concludes that CenterPoint Houston's Digital Substation resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's SRP. The five measures CenterPoint Houston proposes to address wildfire risk are comparable to other utilities within and outside of Texas. These measures include a combination of predictive modeling, targeted vegetation management, and asset hardening, which, taken together, will reduce the risk of CenterPoint Houston's electric assets as a source of ignition and reduce potential damage to its equipment that otherwise would be caused by a wildfire event.

5.7 Physical Attack

5.7.1 Measure Category Summary

Physical security measures include the two transmission substation security upgrades, Substation Physical Security Fencing and Security Upgrades, each of which was proposed in CenterPoint Houston's prior SRP. Measure costs are mostly unchanged from the prior Plan. Further, the substations selected for upgrades are based on the same criteria as applied in the prior Plan.

Table 5-10: Physical Attack Resiliency Measures Costs and Benefits

Resiliency Measure[105]	Resiliency Measure No. (RM)	3-Year Capital Cost ($MM)	3-Year O&M Expense ($MM)	BCA Ratio	3-Yr CMI 2026-2028 (million)	Annual CMI 2028 (million)
Physical Attack						
Substation Physical Security Fencing	RM - 26	$18.0	$0.0	21.8	17.6	8.8
Substation Security Upgrades	RM - 27	$19.4	$0.1	28.7	25.1	12.5
Group Subtotal		**$37.4**	**$0.1**	**25.4**	**42.7**	**21.3**

5.7.2 Benchmarking

Peer Utility Benchmarking Survey

The peer utility benchmarking survey, discussed in Appendix A, indicates that seven (7) of eleven (11) utilities address physical attack risks through their resiliency programs (Figure A-5), five (5) of nine (9) respondent utilities include both substation fencing and substation security upgrades in their resiliency programs (Table 5-11), and four (4) of those utilities also identified threat intelligence as a mechanism to ensure the safety of substations.

[105] This table comprises the subset of measures for which Guidehouse has performed BCA and estimated CMI savings. Other measures included within CenterPoint Houston's SRP are excluded from this table.

Table 5-11: Resiliency Survey Investment Types (Physical Attack Measures)

Type of Investment[106]	Respondent Utility Company ID								
	102	103	106	107	108	109	114	122	123
Substation fencing	✓	✓	✓				✓	✓	
Substation security upgrades	✓	✓	✓				✓	✓	
Threat intelligence and management	✓	✓					✓	✓	

Source: Guidehouse analysis, based on inputs from the First Quartile Resiliency Survey

Jurisdictional Benchmarking

The jurisdictional benchmarking report, provided as Appendix B, also indicates that the types of measures CenterPoint proposes to address physical attack risks are common measures across jurisdictions. Of the 17 states in Table B-4, four (4) include substation physical security measures within proposed investments or generally consider them within scope.

In one notable example, Hawaiian Electric's Resiliency Working Group considered several human threat magnitude thresholds in their threat scenarios, with examples such as physical substation attacks from rifles or explosives. These metrics and repair times follow a similar methodology that CenterPoint Houston has adopted in evaluating their Substation Security Upgrades resiliency measure.

In Texas, SRPs submitted by other utilities, including Oncor and TNMP, have included similar physical security measures to those CenterPoint Houston is proposing.

5.7.3 Substation Physical Security Fencing

5.7.3.1 Resiliency Measure Description

CenterPoint Houston proposes replacing chain-link fences with more resilient and less permeable wire mesh fences at critical substations to thwart unauthorized access and equipment damage from vandals (*e.g.*, stealing copper wire) or terrorist activity. Substations targeted for enhanced fencing will be chosen based on network vulnerability, load criticality, and location (*e.g.,* remote or hidden areas). Substation security in locations targeted for enhanced fencing will typically be supplemented with mobile cameras to monitor and detect intrusions.

5.7.3.2 Revisions from the Prior System Resiliency Plan

CenterPoint Houston proposes to increase spending on the Substation Security Fencing measure, which will increase the number of substations with upgraded security fences over the 3-year Resiliency Plan. Except for using a higher VoLL, all other values applied to derive benefits in Guidehouse's prior report remain unchanged. The criteria that will be used to identify and select substations for fencing upgrades also remain unchanged.

[106] This table includes only the subset of resiliency measures included in the survey that are most closely associated with the measures included by CenterPoint Houston within this risk category (Physical Attack). These were not categorized as such within the survey, and respondent utilities may categorize them differently. The full list of surveyed measures is included in Figure A-2.

5.7.3.3 Resiliency Measure Targets

The estimated three-year cost and quantities for this resiliency measure is presented below.

- Number of substations targeted: **7** per year (**21** total)
- Total project cost: **$18 million**

5.7.3.4 Alternatives Considered

In reviewing the SRP, CenterPoint Houston, in collaboration with Guidehouse, evaluated three alternatives to address substation security: First, concrete fences would aid in preventing unauthorized access equally, as well as wire mesh fencing, but at a much higher cost. CenterPoint Houston may consider concrete fencing in lieu of mesh fencing in key high-risk locations if further analysis determines that this option be recommended.

Second, mobile cameras and motion detection systems can detect intrusion but are unlikely to completely prevent access to substations equipped with chain-link fences (chain-link fencing is cut more easily than the proposed firewall fencing). As noted above, CenterPoint Houston proposes to install security cameras as an additional security measure in some substations where chain-link fences will be replaced with wire mesh.

Third, adding full-time security personnel at each site to continually monitor substations is also an option, but it is extremely expensive and deemed not feasible simply due to the number of substations requiring active 24-hour monitoring (well over 250).

5.7.3.5 Resiliency Measure Metrics and Effectiveness

CenterPoint Houston transitioned from an asset-centric program-based approach to a project-based approach, using co-optimized sets of project types to address resiliency challenges specific to geographic regions in its service area. Using an array of best practice project type alternatives, different project types were selected in each area to enhance resiliency and structural hardening at a discrete asset level.

For substations and transmission assets, these mitigations were primarily structural enhancements, such as elevating substations above inundation levels or replacing existing transmission structures with designs capable of withstanding higher wind speeds. The discrete nature of these projects results in efficacy measurements that are more asset-centric.

Measurements:

1. Percent of planned asset installations completed by County
2. Percent of resilient power delivery asset failures projected to fail during a Resiliency Event
3. Percent of resilient power delivery asset failures occurring during a Resiliency Event

5.7.3.6 Benefits Analysis

Guidehouse evaluated the benefits associated with CenterPoint Houston's proposed Substation Physical Security Fencing resiliency measure on a quantitative and qualitative basis. The quantitative analysis adheres to the BCA methodology described in Section 5.1, with resiliency measure-specific inputs and assumptions described below.

Quantitative Benefits – Key assumptions include estimates on the number of attempted intrusions and, for these, the percentage that will lead to equipment damage and interruption of load. The analysis accounts for the potential for multiple, concurrent intrusions by terrorist organizations. Accordingly, the amount of load at risk is adjusted upward to account for load loss at multiple substations. The probability that over the next 10 years, unauthorized access might occur at each of the substations where wire mesh fencing is proposed is 2% (*i.e.*, once every 50 years). The amount of load at risk is estimated at 729MW,[107] which includes concurrent equipment outages resulting from terrorist or vandal actions (*e.g.*, gunshots or release of explosive devices). The restoration interval to restore the grid is estimated at 24 hours based on concurrent interruptions at several substations. Other benefits include avoided cost of repairs and crew time required to restore service absent the presence of enhanced fencing. The Substation Physical Security Fencing resiliency measure is projected to reduce cumulative CMIs over the 3-year Resiliency Plan by approximately 17.6 million and 8.8 million annually by 2028. Guidehouse's analysis resulted in a composite BCA of 21.8 for these substation security improvements.

Qualitative Benefits – The likelihood of terrorist activity is low compared to incident rates or outages associated with other resiliency events. However, the consequences of such actions can be significant, causing lengthy outages and major load interruption across CenterPoint Houston's service territory. Such an event could result in widespread economic impacts, raise national security implications, and societal harm. Critical loads, industries, and businesses served by impacted substations could experience severe inconvenience and economic losses. Further, terrorist activity on the grid would bring forth adverse media attention along with heightened community awareness and concern.

5.7.3.7 Resiliency Measure Assessment and Conclusion

Guidehouse concludes that CenterPoint Houston's Substation Physical Security Fencing resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's SRP for the following reasons:

- The resiliency measure should reduce damage to substation equipment and avoid widespread outages and concerns that terrorist actions would bring to the region.

[107] Tier 1 NERC first level load at risk.

- While the likelihood of unauthorized substation access and major damage is low, the modest cost of wire mesh fencing supports the proposed investment. Despite the low probability of a major event, the resiliency measure produces a favorable BCA.
- Wire mesh fencing proposed at existing substations meets CenterPoint Houston's current design standard for new substations.
- Implementation of security measures avoids potential highly undesirable economic and societal impacts associated with widespread, lengthy interruptions of service.

5.7.4 Substation Security Upgrades

5.7.4.1 Resiliency Measure Description

CenterPoint Houston proposes to upgrade security monitoring systems at critical transmission substations to detect unauthorized access from individuals seeking to commit vandalism or terroristic actions. Substation security upgrades include unauthorized entry detection systems, video surveillance cameras, and associated communications that link to CenterPoint Houston's control center. These systems will enable operating center staff to rapidly notify law enforcement of an attempted or active intrusion. Rapid response of law enforcement reduces potential equipment damage and customer interruptions caused by vandals or individuals with terroristic intentions.[108] Substations targeted for security will be chosen based on network vulnerability, load criticality, and location (*e.g.*, remote or hidden areas). Enhanced security in some substations will also include upgraded perimeter fencing, as described in Section 5.7.3.

5.7.4.2 Revisions from the Prior System Resiliency Plan

CenterPoint Houston proposes to retain prior spending levels on the Substation Security measure, with no changes in the number of substations that will be equipped with enhanced security systems over the 3-year Resiliency Plan. Except for using a higher VoLL, all other values applied to derive benefits in Guidehouse's prior report also remain unchanged. The criteria that will be used to identify and select substations for security upgrades also remain unchanged.

5.7.4.3 Resiliency Measure Targets

The estimated three-year cost for this resiliency measure and investment amounts are presented below.

- Number of substations targeted: **10** per year (**30** total)
- Total project cost: **$19.5 million**
- Total operation and maintenance expense: **$100,000**

[108] Substation security upgrades may be performed in conjunction with substation fencing upgrades described in Section 5.7.3.

5.7.4.4 Alternatives Considered

The only potentially viable alternative is to add security personnel to continuously monitor substations. This alternative would substantially increase labor expenses and is deemed not feasible due to the large number of substations that would need to be monitored (*i.e.*, over 300).

5.7.4.5 Resiliency Measure Metrics and Effectiveness

CenterPoint Houston transitioned from an asset-centric program-based approach to a project-based approach using co-optimized sets of project types to address resiliency challenges specific to geographic regions in its service area. Using an array of best practice project type alternatives, different project types were selected in each area to enhance resiliency and structural hardening at a discrete asset level.

For substations and transmission assets, these mitigations were primarily structural enhancements, such as elevating substations above inundation levels or replacing existing transmission structures with designs capable of withstanding higher wind speeds. The discrete nature of these projects results in efficacy measurements that are more asset-centric.

Measurements:

1. Percent of planned asset installations completed by County
2. Percent of resilient power delivery asset failures projected to fail during a Resiliency Event
3. Percent of resilient power delivery asset failures occurring during a Resiliency Event

5.7.4.6 Benefits Analysis

Guidehouse evaluated the benefits associated with CenterPoint Houston's Substation Security Upgrades resiliency measure on a quantitative and qualitative basis. The quantitative analysis adheres to the BCA methodology described in Section 5.1 with resiliency measure-specific inputs and assumptions described below.

1. **Quantitative Benefits** – Key assumptions include estimates on the number of attempted intrusions and, for these, the percentage that will lead to equipment damage and interruption of load. The analysis accounts for the potential for multiple concurrent intrusions by individuals acting in coordination or in conjunction with or in support of terrorist organizations, with the amount of load risk being adjusted upward to account for load loss at multiple substations. The probability over the next 10 years that unauthorized access will cause damage with load loss at each of the 36 substations proposed for security systems is 2% (*i.e.*, once every 50 years). The amount of load at risk is estimated at 729 MVW which includes potential concurrent outages resulting from terrorist actions. Restoration time is estimated at 24 hours, which includes repairs on multiple substations for those involving terrorist action. Other benefits include the avoided cost of repairs and crew time required to restore service absent the presence of upgraded security systems. The Substation Security Upgrades resiliency measure is

projected to reduce cumulative CMIs over the 3-year Resiliency Plan by approximately 25.1 million and 12.5 million annually by 2028. From these assumptions, Guidehouse derived a BCA of 28.7.

2. **Qualitative Benefits** – The likelihood of vandal or terrorist activity is low compared to incident rates or number of outages associated with other resiliency measures.[109] However, the consequences of such actions can be significant, with lengthy outages and major customer load interruption across CenterPoint Houston's service territory. Such an event could result in widespread socio-economic impact, raise national security implications, and create societal harm. If only single substations were impacted, there could be severe impacts to critical customers, industries, and businesses. If several substations fed by the transmission network were to fail, it would result in even greater inconvenience and economic harm. Further, terrorist or vandal activity would invariably bring forth adverse media attention, public safety exposure, and heightened community concern. It should be expected that local, state, and federal law enforcement agencies would be engaged, given the severity of terrorist activity or vandalism on critical grid infrastructure.

5.7.4.7 Resiliency Measure Assessment and Conclusion

Guidehouse concludes that CenterPoint Houston's Substation Security resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's SRP for the following reasons:

- The resiliency measure should reduce potential damage to substation equipment, address public safety implications, and avoid widespread concern that terrorist actions or major vandalism would bring to the region, state, and nation.
- While the likelihood of unauthorized substation access and major damage is low, the cost of upgraded security systems supports the proposed investments. Despite the low probability of a major event, the project also produces a favorable BCA.
- The installation of security measures at existing transmission substations meets CenterPoint Houston's current practice for new substations.
- Implementation of security measures avoids highly undesirable potential national security, economic, and societal impacts associated with widespread interruption of service.

[109] The Department of Energy ("DOE") tracks and issues reports on critical infrastructure attacks. In 2023, there were 90 instances of reported attacks, including substation attacks that attracted nationwide media attention.

5.8 Technology & Cybersecurity

5.8.1 Measure Category Summary

Table 5-12: Technology & Cybersecurity Measures

Resiliency Measure	RM Number	3-Year Capital Cost ($MM)	3-Year O&M Expense ($MM)	BCA Ratio	3-Yr CMI 2026-2028 (million)	Annual CMI 2028 (million)
Technology & Cybersecurity						
Spectrum Acquisition		$42.0	$-			
Data Center Modernization		$12.7	$1.3			
Network Security & Vulnerability Management		$7.5	$2.0			
IT/OT Cybersecurity Monitoring		$13.4	$4.2			
Cloud Security, Product Security & Risk Management		$4.0	$6.0			
Group Subtotal		**$361.5**	**$12.4**	--	--	--

Technology & Cybersecurity measures mostly align with those outlined in CenterPoint Houston's prior SRP with three key exceptions:

1. The current SRP proposes to acquire spectrum for a broadband communications network (Spectrum Acquisition resiliency measure) to supplement and ultimately replace several existing broadband spectrums and mesh networks used for operations technology systems, each of which provides essential functionality during resiliency events.
2. The current SRP proposes to add a comprehensive Cloud Security, Product Security & Risk Management resiliency measure to enhance current cybersecurity measures and provide additional resiliency to CEHE cyber systems and associated cyber devices being introduced to support other key operational resiliency measures
3. The Smart Grid Data Resiliency initiative was added to the current Data Center Modernization resiliency measure to improve redundancy and resiliency for electrical distribution operations by adding an Advanced Distribution Management System (ADMS) and a SCADA communications link at the CEHE backup control center (AOC).

5.8.2 Benchmarking

Peer Utility Benchmarking Survey

The peer utility benchmarking survey, discussed in Appendix A, indicates that seven (7) of eleven (11) respondent utilities address cybersecurity risks through their resiliency programs (Figure A-5). Furthermore, as indicated in Table 5-13, the specific measures significantly align with the technology resiliency measures proposed by CenterPoint Houston. Of nine (9)

respondent utilities, seven (7) included at least one of the surveyed technology resiliency measures, and four (4) utilities included at least nine (9) of the ten (10) surveyed technology resiliency measures included in Table 5-13.

Table 5-13: Resiliency Survey Investment Types (Technology & Cybersecurity Resiliency Measures)

Type of Investment[110]	Respondent Utility Company ID								
	102	103	106	107	108	109	114	122	123
Threat intelligence and management	✓	✓					✓	✓	
Data Center Facilities upgrades	✓	✓					✓	✓	
Data storage and handling	✓	✓				✓	✓	✓	
Smart grid data modifications	✓	✓					✓	✓	
Operational data resiliency	✓	✓				✓	✓	✓	
Cyber Security	✓	✓	✓				✓	✓	✓
Cloud based data handling improvements	✓	✓					✓	✓	
Application security							✓	✓	
Telecommunication infrastructure	✓	✓					✓	✓	
Network security	✓	✓					✓	✓	

Source: Guidehouse analysis, based on inputs from the First Quartile Resiliency Survey

Additionally, some peer utilities responded that they have regulatory obligations to require system monitoring and logging at minimum, with an additional risk-based approach for establishing and implementing additional controls to ensure the core controls are being implemented and managed as necessary to protect the bulk electric systems ("BES") and associated BES Cyber Systems.

Lastly, some peer utilities also indicate that some states are supporting cybersecurity resiliency planning as part of state resilience plans, planning reports, or approvals of plans for electric distribution grid transformation projects.

Jurisdictional Benchmarking

The jurisdictional benchmarking report, provided as Appendix B, also indicates that the types of measures CenterPoint proposes to address technology resiliency are common measures across jurisdictions. Of the 17 states in Table B-4, at least six (6) include cybersecurity measures within proposed investments or generally consider them to be within scope. Some specific examples include:

- Some utilities are considering the benefits of implementing a Private Long-Term Evolution (PLTE) network to mitigate reliance on commercial providers and enhance their ability to manage recovery efforts independently during extreme weather events or

[110] This table includes only the subset of resiliency measures included in the survey that are most closely associated with the measures included by CenterPoint Houston within this risk category (Technology & Cybersecurity). These were not categorized as such within the survey, and respondent utilities may categorize them differently. The full list of surveyed measures is included in Figure A-2.

system outages.[111] Utilities that have implemented or pursued PLTEs include Southern Company, San Diego Gas & Electric, Southern California Edison, Tampa Electric Company, Evergy, Xcel Energy, and Ameren.

- Green Mountain Power has a goal of keeping its data centers reliable and efficient. Green Mountain Power's investment requirements include projects for failover systems, providing enhanced levels of redundancy and resiliency to key operational systems that could more easily succumb to extreme weather-related impacts in their current configuration.[112]
- Duke Energy North Carolina's multi-year rate plan includes cybersecurity monitoring as a key requirement in resiliency investments to increase protection against attacks.
- Related to Southern California Edison's application for approval of its Grid Safety and Resiliency Program, small business advocates expressed concerns about privacy with publicly available weather information and an interest in greater cybersecurity protections.
- Ameren Illinois recognizes that 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. Given this, it was determined that there is a need for reliance on monitoring their state and potentially controlling their performance to maintain reliability and resilient grid conditions.[113]

In Texas, SRPs submitted by other utilities, including Oncor and TNMP, have included similar measures to CenterPoint Houston's Technology & Cybersecurity measures, including Oncor's Private Broadband Communications Deployment Program, which aligns with CenterPoint Houston's Spectrum Acquisition measure.

5.8.3 Spectrum Acquisition

5.8.3.1 Resiliency Measure Description

CenterPoint Houston Electric (CEHE) currently employs a highly redundant and resilient Smart Grid field area network (FAN) that leverages redundant backhaul communications to data centers. CEHE leverages mobile carriers such as FirstNet, AT&T, and Verizon, as well as a privately owned transport FAN that uses a private 700 MHz A block radio spectrum band. To maintain future levels of reliability and resiliency and accommodate new communication demands on the electrical power grid, an additional spectrum needs to be acquired.

The spectrum acquisition is the long-term solution to support the multitude of utility use cases to satisfy the T&D systems and functions. This is based on global standards with an active

[111] Khalid, S., Hotovec, S. and Clancy, J. (2023), Utilities' Need for Advanced Telecommunications. Climate and Energy, 39: 1-10. **https://doi.org/10.1002/gas.22323**

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

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

ecosystem and well-aligned with long-term trends in communications technology. Current modeling predicts that additional spectrum is needed to support future capacity needs. The future holds a more complex and dynamic power grid and more end points that will deliver information. The investment needed to secure a resilient future is the ownership of radio spectrum that will meet future needs and technologies.

Spectrum refers to the frequency ranges that are divided into different bands that are used for wireless communications. Wider spectrum (broadband) is needed to support smart communicating devices that requires lower latencies, higher bandwidths and increased reliability. The future need for additional system automation, advanced protection schemes and system visibility to increase reliability / resiliency of the system is driving the need for expanding telecommunication capabilities and in turn additional spectrum. No transmission system outage is required for the Spectrum Acquisition resiliency measure.

Due to increasing climate-related challenges; growing demand for real-time visibility, automation, and better operational control; and anticipated additions to smart communication devices required to meet these challenges and demand, CenterPoint is currently evaluating a set of spectrum options to augment and replace its current set of disparate purpose-built telecommunication networks that are reaching capacity or nearing end-of-life. The proposed Spectrum Acquisition resiliency measure meets the requirement to develop an improved telecommunication network that can deliver lower latencies, higher bandwidth, increased reliability, and other benefits that cannot be obtained by CEHE's current telecommunication network solutions. The Spectrum Acquisition resiliency measure is supported by use cases that identify categories of smart communications devices and a benchmark survey that identified other utilities that have proposed and implemented similar spectrum projects to meet similar needs.

Current 700MHz narrowband telecommunications networks are a blend of leased third-party cellular services and the CEHE narrowband FAN. CEHE currently uses its FAN as a primary network with failover capability to the leased third-party network in the event problems occur on the primary FAN. The proposed Spectrum Acquisition resiliency measure can support 5G broadband services and will support CEHE's Greater Houston Resiliency Initiative (GHRI), which includes the installation of approximately 5,000 automation and Intelligent Grid Switching Devices (IGSD), and other devices to build a self-healing and more resilient electrical grid. CEHE has implemented Direct Transfer Trip (DTT) schemes to manage renewable generation installations across existing fiber networks. However, the Spectrum Acquisition resiliency measure allows CEHE to increase the pace of renewable generation installations by avoiding costly and time-consuming fiber installations. Augmenting and, in some cases, replacing multiple disparate telecommunication networks with the Spectrum network will reduce reliance on public carriers and support better cost management.

It is important to realize that telecommunications bandwidth is a finite resource. Thus, spectrum bandwidth purchase and lease options may be available for a limited time only. Therefore, it is

critical to the success of the Spectrum Acquisition resiliency measure to move forward as soon as possible to acquire the necessary bandwidth while it is available.

5.8.3.2 Revisions from the Prior System Resiliency Plan

None. This measure was not included in CEHE's prior 2024 SRP.

5.8.3.3 Resiliency Measure Targets

The estimated three-year cost for this resiliency measure and investment amounts are presented below.

- Total project cost: **$42.0 million**
- Total operation and maintenance expense: **$0.0**

Utilities require communication capabilities to support devices used for operational control and system visibility. As the need for reliability and resiliency increases, so does the dependence on a robust communication network. CEHE currently owns a 700 MHz spectrum FAN and also leases a third-party commercial cellular spectrum that provides resiliency in the environment for communications. CEHE has a history of delivering communications reliably, despite infrastructure damage which increases situational awareness during critical times of grid restoration.

With future needs to deploy next-generation meters, additional distribution automation, two-way communications capacitor bank deployment, sensors, etc., the sector capacity planning limit is anticipated to be reached in 2030.

There are many things that can adversely impact third-party cellular carriers. These include, but are not limited to:

- Power Outages
- Physical Damages
- Terrorist Attacks
- Cyber Attack
- Natural Disaster

A privately owned network, in combination with leased third-party commercial cellular services, increases network reliability and resiliency, which is crucial during emergency scenarios. The likelihood of private and third-party communication services both being unavailable is low. However, in the event such an event occurs, CEHE can prioritize the restoration of the private network for critical areas.

5.8.3.4 Alternatives Considered

The Greater Houston area currently operates on 700MHz narrowband networks, but capacity constraints must be remedied in the near term (5-10 years) while capabilities must be offered to support long-term (10-20 years) use cases and business needs.

The various Spectrum Acquisition options indicate there is an initial expenditure for the spectrum with some ongoing costs depending on the chosen option. The spectrum lease options incur initial lease expenditures with no fixed costs or guarantee of usage after the contract term expires. While maintaining the 700 MHz in the near term, CEHE has identified multiple alternatives, including three spectrum options that are considered potential best-fit options for the CEHE service territory:

- Commercial cellular, which has no control over restoration and priorities.
- Augment 700 MHz networks with 850 MHz purchase option, which offers a larger 7x7 Frequency Division Duplex (FDD) channel that allows 5G capability.
- Augment 700 MHz networks with 900 MHz that are offered only as a lease option, operate on a 3x3 Frequency Division Duplex (FDD) channel, and are not currently 5GG capable.
- Augment 700 MHz networks with 1.6 GHz lease or purchase options using Time Division Duplex (TDD) for higher spectral efficiency as an early adopter compared to other options with a pathway to spectrum ownership that is 5G capable.

5.8.3.5 Resiliency Measure Metrics and Effectiveness

In reviewing the SRP, CenterPoint Houston, in collaboration with Guidehouse, determined the following performance metrics will be tracked:

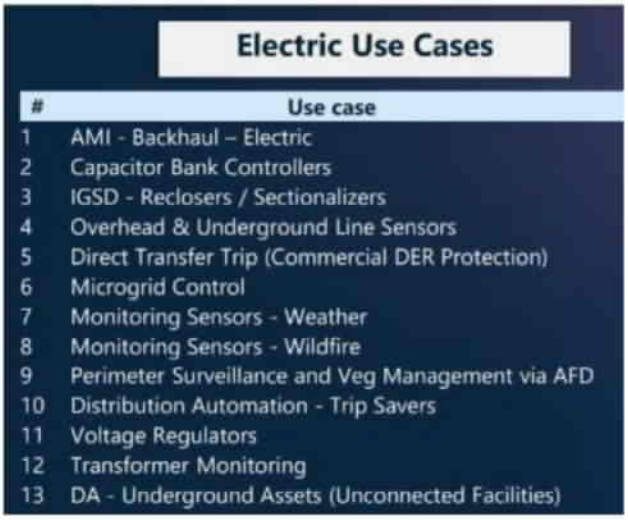
- Downlink latency
- Link utilization
- Throughput.

5.8.3.6 Benefits Analysis

Developing a new spectrum network has indirect resiliency benefits as effective telecommunication capability enables resiliency measures across the current CEHE filing similar to the benefits identified by the Backhaul Microwave Communication and IT/OT Cybersecurity Monitoring resiliency measures. Through collaboration with a third party, West Monroe, CenterPoint identified several electric use cases that require telecommunication network upgrades (Figure 5-8) to support the higher data demands described as "upwards of 50MB/day/device". Although the Spectrum Acquisition resiliency measure addresses the acquisition of broadband and does not directly contain specific cyber systems, Guidehouse applied a NIST Cybersecurity Framework (CSF) comparative analysis, as applicable to the spectrum features, and identified a strong correlation with NIST subcategory PR.DS-02 for higher security for data in transit over private networks as compared to weaker security measures for data transferred over public networks. Guidehouse identified higher data security features including dedicated infrastructure, enhanced encryption capability, secure authentication measures, the ability to segment networks as needed, and stronger security

monitoring and management practices. Guidehouse also identified a high correlation with the NIST CSF subcategory PR.IS-04, as the Spectrum Acquisition resiliency measure is intended to acquire and maintain adequate resource capacity to meet CEHE data communication needs in the near term and extend out to 20 years as a long-term solution.

Figure 5-8: Electric Use Cases



Guidehouse further prepared a qualitative benefit analysis that includes an analysis of the use cases and reviewed regulatory precedence information provided by comparable utilities across multiple regulatory jurisdictions.

Network needs are driven by several proposed measures that support the Greater Houston Resiliency Initiative (GHRI) including an electric Advanced Metering Infrastructure (AMI 2.0) refresh, electrical operations sensor upgrades and replacements, and a need for automation, protection, and system visibility. These components require a robust telecommunications network with higher bandwidth with lower latencies.

Table 5-14 identifies the number of planned additional and replaced cyber systems in the Greater Houston area that would be supported by the spectrum network. Many of the cited cyber systems are included in other proposed CEHE resiliency measures, Table 5-14 is intended to identify the resiliency enabling characteristics of the Spectrum Acquisition resiliency measure and does not imply additional support for other resiliency measures included in the 2025 CEHE System Resiliency Plan.

Table 5-14: Anticipated Number of Replacement & New Devices

CEHE Greater Houston Electric Use Cases- Device Counts		
Device Type	Replacements	New
AMI – Backhaul – Electric	6,000	
Capacitor Bank Controllers	7,000	
IGSD – Reclosers/Sectionalizers		5,000
Overhead/Underground Line Sensors		3,000

Direct Transfer Trip (DER Protection)		200
Microgrid Control		5
Weather Monitoring Systems		100
Wildfire Monitoring Systems		25
Perimeter Surveillance & Veg Management	10	
Trip Savers – Distribution Automation	25,000	
Voltage Regulators		100
Transformer Monitoring Sensors		100,000
DA – Underground Assets	1,000	
Totals	**39,010**	**108,430**

CEHE's current 700 MHz narrowband spectrum current supports its AMI v1.0 access points for backhaul connectivity, in addition, CEHE plans to upgrade its current inventory of 7000 capacitor bank controllers from one-way pagers to two-way communications devices, which will require higher bandwidth with lower latency rates to be effective. There are approximately 14 current sites that have the potential to overload associated radio sectors in the future due to 700MHz capacity constraints caused by an anticipated transition to a GenX mesh network and higher AMI 2.0 capabilities. While there are some near-term mitigating measures, *e.g.*, optimizing modulation rates and supplementing the current network with other narrowband spectrum or public cellular service, that can extend the life of the current 700MHz narrowband network, such efforts may be insufficient to adequately support the need for higher bandwidth, lower latency, and increasing requirements for the identified electric use cases over the next 10-20 years. Potential problems were also identified with narrowband telecommunications vendors, including vendors moving to higher bandwidth service offerings and abandoning the support for 700 MHz communications equipment.

As cited above, CEHE may be able to remediate 700 MHz capacity concerns with stopgap mitigating measures in the near term (5-10 years), but that solution does not meet long-term use case requirements. A 5G capable broadband spectrum solution, which is currently available but may not be available in 5-10 years, is recommended as a long-term approach that will supply the higher bandwidth and lower latency requirements for CEHE's identified long-term use cases and business needs out to 20 years. Development of a broadband spectrum solution is the most cost-effective compared to other purchase or lease options. This solution allows CEHE to keep its current 700 MHz narrowband network, augment it with purchased broadband frequencies, and expand the network over time. This solution is 5G capable and meets the long-term use case requirements for higher bandwidth and lower latency rates.

Other utilities have filed similar proposed plans for grid modernization and resiliency measures, including several utilities/companies across the North American electrical grid that implemented or have proposed spectrum projects to support long-term resiliency projects, similar to the use cases and other resiliency measures proposed by CEHE. One utility made a direct purchase of spectrum bandwidth, five utilities purchased spectrum broadband at FCC auction, while one company in the survey developed a private Access Point Name (APN) network that allows devices to connect to the Internet through a cellular network and supports a Virtual Private Network (VPN) to provide secure communications over the Internet as part of its Distributed

Asset (DA) strategy. Additionally, four utilities negotiated spectrum bandwidth leases to implement their broadband projects, while three utilities have filed grid modernization plans to implement spectrum projects, which have not been ruled upon by the associated regulatory bodies as of January 2025.

5.8.3.7 Resiliency Measure Assessment and Conclusions

Based on information provided by CEHE, Guidehouse gained a reasonable assurance the Spectrum Acquisition resiliency measure is needed to support grid modernization projects and determined CEHE can obtain significant benefits in a cost-effective manner through the implementation of the Spectrum Acquisition resiliency measure. Guidehouse further concluded that CenterPoint's Spectrum Acquisition resiliency measure is justified with regard to a demonstrated need for higher bandwidth and lower latency rates to support grid modernization and other proposed resiliency measures. The Spectrum Acquisition resiliency measure is also supported by similar utility spectrum projects, which have been approved or are in the review process by various regulatory jurisdictions.

5.8.4 Data Center Modernization

5.8.4.1 Resiliency Measure Description

CenterPoint Houston's Data Center Modernization resiliency measure addresses the following aspects to support the 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 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.
- Installing a redundant Advanced Distribution Management System (ADMS) and SCADA communication link at the CEHE backup control center (AOC) to enhance resiliency in electrical system operations (new Smart Grid Data Resiliency component).

The infrastructure will be implemented to support replacement technology to perform transmission and distribution operations functions and will include key performance indicators

("KPIs") and additional metrics to monitor key attributes to assess measure effectiveness and reliability. The combination of aspects of this resiliency measure, which in most cases begins implementation in 2024, including planning, offers a more sustainable infrastructure. The resiliency measure addresses issues and concerns with outdated and end-of-life systems, applications, and equipment, while also streamlining processes. The implementation will last three years, with automated failover being the immediate component, taking one year. All implementation components are 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 which is aimed at enhancing grid resiliency through improved response and recovery capabilities, ultimately minimizing risks related to service interruptions. A data center is a physical facility utilized by organizations to house critical applications and data through a network of computing and storage resources, facilitating the delivery of shared applications and data. Key components include routers, switches, firewalls, storage systems, servers, and application delivery controllers.[114]

Currently, CEHE's distribution smart grid SCADA communication is only configured at CEHE's primary control center (ECDC). There is no redundant distribution SCADA communication link configured at CEHE's backup control center (AOC). If CEHE's distribution smart grid SCADA communication link at ECDC becomes unavailable, CEHE will lose the capability to monitor and control CEHE's distribution SCADA devices. This initiative is to set up a redundant smart grid SCADA communication link at AOC so Distribution Control has the resilient capability to monitor/control smart grid devices in CEHE's distribution network at AOC if the ECDC link is unavailable. The Smart Grid Data Resiliency initiative will also implement a fully redundant Advanced Distribution Management System (ADMS) at both control centers.

5.8.4.2 Revisions from the Prior System Resiliency Plan

The Smart Grid Data Resiliency component is an addition to the Data Center Modernization resiliency measure initially submitted with the 2024 filing. The other components of the Data Center Modernization resiliency measure were unchanged from the 2024 filing.

5.8.4.3 Resiliency Measure Targets

The estimated three-year cost for this resiliency measure and investment amounts are presented below.

- Total project cost: **$13.9 million ($12.7 capital/$1.3 O&M)**
- Total operation and maintenance expense: **$1.3 million**

CEHE will establish a separate smart grid communication link at AOC to maintain resilient visibility and controllability of CEHE's distribution network in the event of loss of ECDC smart grid communication. Adding smart grid telecommunications infrastructure is the first priority.

[114] Cisco (2024)

CEHE will also install network security appliances such as firewalls to ensure the confidentiality, integrity, and availability of operational data transferred across CEHE's distribution SCADA communication links. Implementing redundant ADMS also is required at the two control centers to ensure resilient communications with CEHE's smart grid devices through the redundant distribution SCADA link at AOC.

5.8.4.4 Alternatives Considered

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 with the hybrid cloud and the personnel's skill set. CenterPoint Houston is looking to transition its IBM-HP equipment into Intel-based systems to increase system agility. It is also looking into a modern system that can become hybridized with the cloud or transition into a full cloud. Alternatives will depend on the vendors and the products being offered.

CenterPoint Houston will migrate many of its legacy applications into a cloud environment, leveraging cloud solutions to improve its ability to recover them. Some software cannot simply be moved to the cloud, and as they decide what could be moved to the cloud, they will need alternative recovery options. The alternatives are to keep systems on-premises and leverage replication or move to a hybrid environment and solution.

CEHE has two control centers: ECDC and AOC. There are no other alternatives to consider for the Smart Grid Data Resiliency component of the Data Center Modernization resiliency measure.

5.8.4.5 Resiliency Measure Metrics and Effectiveness

Guidehouse evaluated the benefits and features associated with CenterPoint Houston's proposed Data Center Modernization resiliency measure on a qualitative basis with measure-specific inputs and assumptions. This analysis compared CenterPoint Houston's resiliency measure with the NIST CSF Categories, to determine the levels of correlation between the six CSF Functions (Govern, 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.

CenterPoint Houston also plans to use the following performance metrics for tracking the effectiveness of the Data Center Modernization 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
- Field tests using the AOC Smart Grid Data Resiliency SCADA communication link to monitor and control smart grid devices.
- Periodic activation and testing of the AOC ADMS and SCADA communication links to ensure availability when needed.

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 measure was sufficiently implementing the intent of the subcategory from a resiliency perspective. The system features that were mapped to low correlation were considered to be relatively ineffective in improving resiliency. However, depending on the context of the proposed measure, pursuing it may still have value from reliability or policy perspectives. For a detailed explanation of the methodology used, refer to Section 5.1.4.

Table 5-15 lists CSF Functions and associated categories with high and/or medium correlations to the resiliency measure:

Table 5-15: Data Center Modernization Analysis Results

Function	Categories
Govern	• Operational Context ("OC") • Risk Management Strategy ("RM")
Identify	• Asset Management ("AM") • Risk Assessment ("RA")
Protect	• Identity Management, Authentication, and Access Control ("AA") • Data Security ("DS") • Platform Security ("PS") • Technology infrastructure Resilience ("IR")
Recover	• Incident Recovery Communication ("CO")
Please note: Guidehouse did not include the "Respond" and "Detect" functions in these analysis results as they did not have high or medium correlations.	

5.8.4.6 Benefits Analysis

Guidehouse evaluated the benefits associated with CenterPoint Houston's proposed resiliency measure and determined that the measure will provide a high level of effectiveness. Based on the results of its analysis, Guidehouse determined that the measure offers resiliency benefits.

All determinations below are based on CenterPoint Houston information on measure descriptions, interviews, and responses to data requests for additional resiliency measure details.

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

Operational Context ("GV.OC") *The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood.*	
Analysis Results Description:	CenterPoint Houston highlights the comprehensive understanding and prioritization of its critical system and their dependencies and critical functions by improving their failover, recovery, and redundancy capabilities 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 platform where a full cloud solution is not possible.

Risk Management Strategy ("GV.RM") *The organization's priorities, constraints, risk tolerance, appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.*	
Analysis Results Description:	CenterPoint Houston will leverage third-party services as part of the design, procurement, integration, and implementation of its resiliency measure. It is important that partners understand their roles and responsibilities from a cybersecurity perspective. CenterPoint Houston highlighted cybersecurity roles and responsibilities for both internal personnel and external partners. They also 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.

Asset Management ("ID.AM") *The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.*	
Analysis Results Description:	Asset management is a vital part of resiliency. Strategies for addressing supply chain and warehousing operations will be devised to identify and implement upgrades that will phase out aging and end-of-life equipment. CenterPoint Houston will inventory the associated data center hardware and software to successfully implement the resiliency measure. CenterPoint Houston plans to move existing on-premises services to cloud-based applications through a SaaS deployment or directly into a cloud space such as Azure for clients and personnel. It plans to continue on-premises as needed until it can transition to a hybrid platform, then possibly a fully cloud model. Additionally, data flows will be improved by implementing new Cisco switches aimed at automatic failure prevention. CenterPoint Houston plans to transition from their aging and end-of-life 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 service life of these assets typically spans six years, though in some cases, it extends to seven years.

Risk Assessment ("ID.RA") *The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.*	
Analysis Results Description:	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 is prioritizing setting up an automated method for failover between data centers, demonstrating a proactive approach to mitigating risks.

Identity Management, Authentication, and Access Control ("PR.AA") *Access to physical and logical assets and associated facilities is limited to authorized users, processes, or devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.*	
Analysis Results Description:	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") *Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.*	
Analysis Results Description:	CenterPoint Houston's information management and security strategy aligns with its risk strategy, emphasizing the protection of data confidentiality, integrity, and availability. To safeguard data at rest, CenterPoint Houston implements Self-Encrypting Drives ("SEDs") in resiliency measure aspects like the SAN Fabric, complemented by a software layer for monitoring traffic within the SAP environment. CenterPoint Houston's in-transit data is mostly internal traffic that leverages network segmentation to ensure traffic is seen by the appropriate parties. 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 sanitize the data. Furthermore, they are increasing system availability by upgrading to an automated failover architecture 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.

Platform Security ("PR.PS") *The hardware, software (e.g., firmware, operating systems, applications), and physical and virtual platform services are managed consistently with the organization's risk strategy to protect their confidentiality, integrity, and availability.*	
Analysis Results Description:	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. CenterPoint Houston establishes baseline configurations for its information technology and industrial control systems, incorporating security principles and concepts like least functionality. Least functionality ensures 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 levels 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. Network security and cybersecurity teams at CenterPoint Houston are responsible for managing the protection of network devices involved in these measures, ensuring robust safeguards are in place. Additionally, the primary objective of the Cisco upgrade is to improve failover capabilities, particularly for the automatic failover program, demonstrating CenterPoint Houston's dedication to maintaining 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.

Incident Recovery Communication ("RC.CO") *Restoration activities are coordinated with internal and external parties.*	
Analysis Results Description:	Through this resiliency measure, CenterPoint Houston intends to improve its ability to recover its applications in Business Continuity and Disaster Recovery ("BCDR") situations. CenterPoint Houston intends to move to a cloud solution where it is possible for many of its applications. On-premises replication and recovery are currently in place with the next steps to move toward the development of a Hybrid Cloud (Cloud and On-Premises) BCDR strategy, with eventual intentions of full cloud migration. The data center automated failover program incorporating the redundant ADMS and SCADA communication link will also improve the recovery strategy when 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, which is estimated to take around three hours. The automated recovery will further improve system availability, making their system more resilient.

Technology Infrastructure Resilience ("PR.IR") *Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, availability, and organizational resilience.*	
Analysis Results Description:	CenterPoint Houston will improve its ability to recover its applications in Business Continuity and Disaster Recovery ("BCDR") situations with the implementation of the proposed addition of the SCADA resiliency component to the Data Center Modernization resiliency measure. CenterPoint Houston proposes implementing redundant ADMS and SCADA communication links located at geographically discrete control centers, which offer significant resiliency benefits and ensure continued operations by minimizing operational disruptions in the event of failure or disruption in one or more control centers.

Key benefits of the Smart Grid Data Resiliency initiative and other components of the Data Center Modernization resiliency measure include the following areas:

Enhanced Operational Continuity
Redundant control centers with associated redundant ADMS and SCADA communication links ensure that if the primary control center experiences a failure or an outage, the backup control center can take over operations seamlessly, which can prevent or mitigate service disruptions in CEHE's distribution operations by ensuring a continuous supply of operational services, minimizing downtime, and reducing potential damage. While backup control centers are not currently required in distribution operations[1], it is an operational best practice in electrical systems operations, and it is currently mandated by NERC Reliability Standard EOP-008-2 for Reliability Coordinators, Transmission Operators, and Balancing Authorities. Implementing the SCADA resiliency measure also supports a strong correlation with the NIST CSF Technology Infrastructure Resilience (***PR.IR***) category, as described below.

Increased Reliability and Availability
Redundant control centers and ADMS mitigate single points of failure, creating more reliable and available system control capability. In cases such as power failure, equipment malfunctions, or natural disasters, the redundant systems can maintain continuous operations. The increased reliability inherent in redundant systems is crucial for the electrical sector, where continuous operations are essential.

Reduced Risk of System Failures
Redundant systems reduce the risk of system downtime, failures, disruptions, and minimize the length of potential consumer outages and associated costs. By providing backup systems, redundant control centers, and associated ADMS and SCADA communication links can minimize the impact of potential failures and ensure the continued functioning of critical electrical system infrastructure. This function and the Increased Reliability and Availability function discussed above strongly correlate with NIST CSF subcategory ***PR.IR-04***, which requires CEHE to implement and maintain adequate resource capacity to ensure availability.

Improved Security and Protective Measures
Redundant control centers and their associated cyber systems and communication links can enhance security by offering backup systems in case of cyberattacks or other security threats. Redundancy can also prevent data loss and maintain the integrity of sensitive operational information. Redundant and segmented control systems can also help to protect against malicious attacks that could disrupt operations. This function strongly correlates with NIST CSF subcategories ***PR-IR-01***, which requires networks and environments to be protected from unauthorized logical access and usage, and ***PR.IR-03***, which requires mechanisms to be implemented to achieve resiliency requirements in normal and adverse situations.

Enhanced Disaster Recovery Capability
Redundant control centers and their associated cyber systems and communication links are crucial components of disaster recovery plans. Implementing the SCADA resiliency measure should allow CEHE to recover from major disruptions quickly. In the event of a natural disaster or other catastrophic event, redundant systems can ensure that CEHE distribution system operations can continue from a different location, ensure business continuity, and minimize the

impact of disasters across the CEHE electrical distribution service territory. This function provides a strong correlation with NIST CSF subcategory PR.IR-02, which requires CEHE's technology assets to be protected from environmental threats. This function also correlates with NIST CSF subcategory RC.RP-04, which considers critical mission functions and cybersecurity risk management to establish post-incident operational norms.

5.8.4.7 Resiliency Measure Assessment and Conclusions

Guidehouse concludes there is a high correlation between system and business resilience and system restoration with CenterPoint Houston's Data Center Modernization resiliency measure. This was based on the high level of correlation the measure has with the NIST CSF functions. Particular areas in which this resiliency measure supports a strong and resilient electric transmission and distribution system include:

- Governance
- Access Control
- Data Security
- Protective Technology
- Technology Infrastructure Resilience

Upgrading the outdated equipment and implementing solutions that improve system availability through enhanced recovery solutions was the intent of many aspects of this resiliency measure. Ensuring that 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 move forward with upgrading to the latest technology. Moving to an on-premises solution for replication, then a hybrid system, with goals to fully implement in the cloud environment leveraging cloud solutions will provide CenterPoint Houston with the ability to recover quickly from a natural disaster or a cybersecurity event using the latest recovery methods these solutions provide.

Based on the information provided by CEHE and professional judgment, Guidehouse gained a reasonable assurance that the addition of the Data Center Modernization resiliency measure is needed to support higher operational service levels and improved resiliency for electrical system operations and determined CEHE can cost-effectively obtain significant benefits through the implementation of the Smart Grid Data Resiliency initiative included in the Data Center Modernization resiliency measure. Guidehouse concluded that the components of the Data Center Modernization resiliency measure are generally supported by distribution system operations best practices that align with mandated activities required under EOP-008-2 for the transmission sector of the North American electrical grid and support compliance with the NIST CSF (v2.0) Technology Infrastructure Resilience category.

5.8.5 Network Security & Vulnerability Management

5.8.5.1 Resiliency Measure Description

CenterPoint Houston's Network Security and Vulnerability Management resiliency measure is focused on proactive procedures 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. Its 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 security equipment allows CenterPoint Houston to have the latest in-service and manufacturer-supported equipment.

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, mitigating, and reporting software and network vulnerabilities. Identifying, monitoring, and responding to urgent and complex issues are essential components of vulnerability management and cybersecurity. In another measure, CenterPoint Houston will be upgrading to a Governance, Reliability, and Compliance ("GRC") tool to automate its processes and replace its manual processes of using spreadsheets, which will reduce potential data input errors. CenterPoint Houston also plans to deploy a vulnerability assessment tool to support the vulnerability management process.

Additionally, as part of this measure, CenterPoint Houston also plans to refresh the hardware for over 200 appliances, firewalls, and hardware for critical software such as Palo Alto, QRadar, and Cyber Ark, which is currently being used for firewall protection (Palo Alto), threat detection (QRadar) and as a password vault (Cyber Vault) for housing important privileged 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.

5.8.5.2 Revisions from the Prior System Resiliency Plan

None, the Network Security and Vulnerability Management resiliency measure is unchanged from the 2024 SRP.

5.8.5.3 Resiliency Measure Targets

The estimated three-year cost for this resiliency measure and investment amounts are presented below.

- Total project cost: **$9.5 million**
- Total operation and maintenance expense: **$2.0 million**

The Network Security & Vulnerability Management Resiliency Measure is known in CenterPoint Houston's experience and within the industry to protect digital assets including, but not limited to, network, network equipment, client computers, and control systems. Without a Network Security & Vulnerability Management Measure, CenterPoint Houston's digital assets and data would be at risk of vulnerabilities that may allow unauthorized access or attacks by threat actors.

While the three elements of this resiliency measure are not dependent on one another, they are complementary and together are more effective in increasing the resiliency of CenterPoint Houston's system.

5.8.5.4 Alternatives Considered

CenterPoint Houston is determining the solutions and tools that will continue to be implemented to address vulnerability management and GRC procedures. It currently uses Rapid7 and is doing its due diligence to consider other vendors and solutions as potential replacements.

5.8.5.5 Resiliency Measure Metrics and Effectiveness

Guidehouse qualitatively evaluated the benefits and features associated with CenterPoint Houston's proposed Network Security and Vulnerability Management resiliency measure with measure-specific inputs and assumptions. This analysis compared CenterPoint Houston's resiliency measure with the NIST CSF Categories 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 by identifying 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.

CenterPoint Houston also plans to use the following performance metrics for tracking the effectiveness of the Network Security & Vulnerability Management resiliency measure:

- Number of applications in scope having gone through their Secure Software Development Lifecycle ("SSDLC") process,
- Amount of peer reviews, code reviews, code scans,
- Number of application security vulnerabilities detected/remediated,
- Number of network segments ingested daily,
- Number of suspicious/malicious alerts,
- Number of packets stopped at firewalls,
- Number of packets inspected, and
- Net number of rules moved from layer 4 to layer 7.

The subcategories selected for reporting from the medium correlations were selected based on Guidehouse's professional judgment 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 mapped to low correlation were considered to be relatively ineffective in improving resiliency. However, depending on the context of the proposed resiliency measure, it may still have value in pursuing from reliability or policy perspectives. For a detailed explanation of the methodology used, refer to Section 5.1.4.

Table 5-16 lists the CSF Functions and associated categories with high and/or medium correlations to the measure:

Table 5-16: Network Security and Vulnerability Management Analysis Results

Function	Category
Identify	• Asset Management ("AM") • Business Environment ("BE") • Governance ("GV") • Risk Assessment ("RA") • Supply Chain Risk Management ("SC")
Detect	• Anomalies and Events ("AE") • Security Continuous Monitoring ("CM") • Detection Processes ("DP")
Protect	• Access Control ("AC") • Awareness and Training ("AT") • Data Security ("DS") • Information Protection Processes and Procedures ("IP") • Protective Technology ("PT")
Please note: Guidehouse did not include the "Respond" and "Recover" functions in these analysis results as they did not have high or medium correlations.	

Guidehouse concludes that there is a high level of correlation between resiliency and CenterPoint Houston's Network Security and Vulnerability Management resiliency measure. This was based on the measure's high level of correlation with the NIST CSF functions.

The areas in which these measures support a strong and resilient electric transmission and distribution system include:

- Risk Assessment
- Access Control
- Information Protection Processes and Procedures
- Protective Technology
- Security Continuous Monitoring

Through continuous monitoring and proactive risk controls, CenterPoint Houston will fortify its defenses against potential cyber threats, thereby minimizing the risk of cyber-related disruptions to critical grid operations. Guidehouse concludes that CenterPoint Houston's Network Security and Vulnerability Management resiliency measure supports grid resiliency by ensuring the stability and integrity of its infrastructure.

5.8.5.6 Benefits Analysis

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 threats to the system, as well as resiliency benefits. All determinations below are based on CenterPoint Houston's information on measure descriptions, interviews, and responses to data requests for additional measure details.

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

Asset Management ("ID.AM") *The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.*	
Analysis Results Description:	CenterPoint Houston is upgrading and refreshing technology that needs to be updated. This resiliency measure helps ensure CenterPoint Houston has network and security tools that meet industry standards to ensure the resiliency of the services it provides. CenterPoint Houston listed the hardware and software it will upgrade and refresh, prioritizing criticality and business needs. Network devices approaching end-of-life are being prioritized as part of this resiliency measure. Having the latest network security hardware available will ensure the manufacturer updates the network and has the latest security features installed to ensure a robust and resilient network.

Business Environment ("ID.BE") *The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.*	
Analysis Results Description:	Establishing critical functions assists with ensuring resiliency in the services being provided. CenterPoint Houston plans to improve resilience by upgrading its ability to failover or switch from its primary and/or backup control center. It is important that CenterPoint Houston implement the network refresh to ensure a successful failover. Additionally, CenterPoint Houston will include a GRC tool that will assist with ensuring a strong process flow is in place for critical steps toward security and resiliency activities. Dependencies for critical functions must be established to improve overall resilience.

Governance ("ID.GV") *The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.*	
Analysis Results Description:	Implementing an automated solution will improve managing NIST CSF alignment and compliance efforts. CenterPoint Houston plans to implement a GRC tool that will assist with the transition from a manual process to an automated solution. This provides a more straightforward method for approval and compliance efforts by including a taxonomy for risk indicators, catalog control, and stakeholder notification. CenterPoint Houston also intends to mature the GRC process by implementing a risk tolerance program using residual risk data. This will also improve upper management's view on actions that need approval to move forward with risks. CenterPoint Houston intends to mitigate or remediate, further improving the system's resilience. The GRC tool will also improve the prioritization of remediation efforts with a sign-off process, further improving its resiliency posture.

Risk Assessment ("ID.RA") *The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.*	
Analysis Results Description:	Implementing a tool to scan for vulnerabilities will improve the view of potential weaknesses or gaps in a system, further reducing the risk of impact on the system. CenterPoint Houston plans to use the Vulnerability Assessment tool Rapid7 to scan individual machines and assess potential security risks. The refresh will ensure CenterPoint Houston has the latest version and threat intelligence libraries for assessing any potential security gaps. Awareness of these gaps allows CenterPoint Houston to mitigate them.

Supply Chain Risk Management ("ID.SC") *The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.*	
Analysis Results Description:	Utilizing support services, including third parties, to help implement the latest technology for refreshing network equipment can ensure equipment functions as expected. CenterPoint Houston has a resident Palo Alto representative to assist with implementing its network security refresh for Palo Alto network devices. Additionally, it has a team of engineers to assist around the clock with any implementation and ongoing maintenance issues. Having these third-party service providers support CenterPoint Houston through implementation greatly improves its ability to ensure its network is fully functioning and resilient.

Anomalies and Events ("DE.AE") *Anomalous activity is detected, and the potential impact of events is understood.*	
Analysis Results Description:	The capability to detect anomalous activity and vulnerabilities is critical to identifying and mitigating weaknesses to improve cybersecurity resiliency. CenterPoint Houston plans to implement security measures that detect potential security gaps in its network and associated systems. CenterPoint Houston stated that it has architecture diagrams that allow it to be aware of the data flows of communication in its network. This is a good initial step to detecting anomalous activity.

Security Continuous Monitoring ("DE.CM") *The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.*	
Analysis Results Description:	As part of its ongoing system security program, CenterPoint Houston uses monitoring features from the hardware and software it will be refreshing to including monitoring of the system's network, users, and vulnerabilities. CenterPoint Houston plans to implement malicious communication detection as part of the refreshed network equipment to monitor the network for unwanted communication. CenterPoint Houston will also monitor for gaps or vulnerabilities within the system using a refreshed vulnerability scanner, Rapid 7.

Detection Processes ("DE.DP") *Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.*	
Analysis Results Description:	Detecting system anomalies helps ensure awareness of cybersecurity events and prepare for quick remediation or mitigation actions. CenterPoint Houston plans to refresh the systems that assist with threat detections in its network and on its system endpoints. CenterPoint Houston plans to improve its detection efficiency by replacing its QRadar system with cloud-based software that will assist with streamlining and alerting. CenterPoint Houston will continue to use network security features such as sandboxing and threat signature technologies with the network refresh it will implement.

Access Control ("PR.AC") *Access to physical and logical assets and associated facilities is limited to authorized users, processes, or devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.*	
Analysis Results Description:	Managing and controlling who can access critical systems is vital for a more secure and resilient system. CenterPoint Houston has access control for remote users and protects its systems by limiting the users that can access its system remotely. CenterPoint Houston is including an update on hardware for the Cyber Ark, which is used as a vault for passwords, and also plans to limit remote access to the system to only a privileged team that requires request, approval, and provisioning of access. This includes the vulnerability servers and network security appliances that are part of the resiliency measure. CenterPoint Houston has physical protection to prevent unauthorized access, further improving its resiliency posture.

Awareness and Training ("PR.AT") *The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.*	
Analysis Results Description:	Cybersecurity awareness and training assist personnel with understanding their key role and quickly identifying, prioritizing, approving, and executing solutions to address cybersecurity issues. CenterPoint Houston plans to include awareness and training for the GRC tool at all user levels. This will include understanding the policies and procedures related to this tool and ensuring that all critical personnel understand their roles and responsibilities.

Data Security ("PR.DS") *Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.*	
Analysis Results Description:	Protecting an organization's data is key to maintaining data integrity and confidentiality. CenterPoint Houston plans to implement several data protection controls to ensure the new hardware and software are secure. CenterPoint Houston will implement encryption and secure communication protocols such as Hypertext Transfer Protocol Secure ("HTTPS"). CenterPoint Houston will forward network log information to a log aggregator for some hardware. This information will be sent using encryption methods. For data that resides within the hardware itself, CenterPoint Houston plans to physically destroy hard drives via shredding rather than send them back to the manufacturer to prevent retrieval of critical data.

Information Protection Processes and Procedures ("PR.IP") *Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.*	
Analysis Results Description:	Information protection techniques are necessary to maintain confidentiality and secure critical information. CenterPoint Houston includes information protection techniques such as hard drive shredding in this resiliency measure. CenterPoint Houston plans to mature its information protection methodologies to further increase resiliency by creating business case documentation of existing vulnerabilities identified by its vulnerability assessment tool. CenterPoint Houston currently scans its network environment with endpoint and system security scanning tools to mitigate potential environmental vulnerabilities. It also performs web inspection and penetration testing.

Protective Technology ("PR.PT") *Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.*	
Analysis Results Description:	Protecting assets using security solutions that ensure networks are protected and are available can ensure a functional and resilient communication infrastructure. CenterPoint Houston plans to upgrade its network equipment with the latest firewalls, routers, and switches to protect its communication and control networks. To ensure high network availability, CenterPoint Houston will include system redundancy and have multiple scanners for its vulnerability assessment scanning tool. CenterPoint Houston also plans for the GRC tool to be on premises for redundancy purposes. Lastly, some of the software is being transitioned into the cloud, allowing for increased availability capacity to enable a more resilient system.

5.8.5.7 Resiliency Measure Assessment and Conclusions

Guidehouse concluded that there is a high level of correlation between resiliency and CEHE's Network Security and Vulnerability Management resiliency measure. This was based on the measure's high level of correlation with the NIST CSF functions.

The areas in which these measures support a strong and resilient electric transmission and distribution system include:

- Risk Assessment
- Access Control
- Information Protection Processes and Procedures
- Protective Technology
- Security Continuous Monitoring

Through continuous monitoring and proactive risk controls, CEHE will fortify its defenses against potential cyber threats, thereby minimizing the risk of cyber-related disruptions to critical grid operations. Guidehouse concludes that CEHE's Network Security and Vulnerability Management resiliency measure supports grid resiliency by ensuring the stability and integrity of its infrastructure.

5.8.6 IT/OT Cybersecurity Monitoring

5.8.6.1 Resiliency Measure Description

The IT/OT Cybersecurity Monitoring Resiliency Measure is a comprehensive program that will deploy advanced firewalls, passive network sensors, and other cyber technologies to over 400 sites. CenterPoint Houston proposes building a sustainable cybersecurity resiliency measure that provides enhanced monitoring for greater visibility, analytics, integration of data sources, better protections, and detections for responding to cybersecurity threats. Specifically, the proposed OT tool set will provide visibility into the operational environments that were not previously available. It shows network traffic detection and OT asset visibility and provides alerts for abnormal or malicious behavior. The resiliency measure allows for 24x7 monitoring of operational assets based on industry best practices (*e.g.*, NIST SP 800-82r3). The resiliency measure will fill gaps in segmentation, monitoring, and OT asset management.

CenterPoint Houston will use Splunk as their logging system as well as for Key Performance Indicator ("KPI") visibility, Palo Alto for segmentation, and Nozomi for internal network monitoring threat detection and response. This resiliency measure will introduce automation capabilities to learn CenterPoint Houston's operating baseline and tune it to identify anomalous activity that could lead to a cybersecurity incident. CenterPoint Houston will include, as part of the measure, a testing center that will assist with onboarding all IT, OT, and physical security system data sources. Training will be provided to Security Operations Center ("SOC") personnel to understand the alerts and take appropriate action against any attempts at intrusion or successful intrusions by attackers.

Resiliency Measure Details:

- Scope includes ~300 transmission and distribution sites, standardizing the security monitoring architecture for all sites.
- This resiliency measure covers CenterPoint Houston's Transmission & Distribution systems.
- Tentative schedule - begin in 2024, continue into 2025, and complete by end of 2025.

5.8.6.2 Revisions from the Prior System Resiliency Plan

None. The IT/OT Cybersecurity Monitoring resiliency measure is unchanged from the 2024 CEHE SRP.

5.8.6.3 Resiliency Measure Targets

The estimated three-year cost for this resiliency measure and investment amounts are presented below.

- Total project cost: **$17.6 million**
- Total operation and maintenance expense: **$4.2 million**

Threat and intelligence data and scanning systems data employed by CEHE indicate that the IT/OT environment has a continuous target of threat actors. The proposed features and functions of the IT/OT Cybersecurity Monitoring resiliency measure are known best practices within the industry to protect all digital assets, including the IT network, network equipment, client computers, and control systems.

5.8.6.4 Alternatives Considered

Other technology platforms were considered and evaluated via an objective process that aligns business requirements, company and product features, and other important factors such as fiscal and support considerations. The Guidehouse analysis team determined that this resiliency measure is directly related to monitoring for cybersecurity breaches and addresses other cybersecurity threats and vulnerabilities; therefore, it did not evaluate other methods.

5.8.6.5 Resiliency Measure Metrics and Effectiveness

A cybersecurity threat targets computer networks, systems, and user data. These threats can come in the form of malware, phishing, and other malicious activity. Cybersecurity monitoring is crucial in enhancing organizational resilience by analyzing network traffic patterns to identify, mitigate, and prevent potential cyber threats. This approach allows for early detection, isolation, neutralization, and response to potential threats. Most monitoring will analyze network traffic, allowing organizations to identify and respond to malicious activities. By monitoring network traffic patterns, malicious traffic patterns, and unauthorized access attempts, organizations can quickly isolate and neutralize potential threats.

CenterPoint Houston also plans to use the following performance metrics for tracking the effectiveness of the IT/OT-Cybersecurity resiliency measure:

- Number of alerts,
- Number of systems being monitored (system transparency),
- Incident response time,
- System information ingestion rates,
- Volume of recorded malicious behavior,
- Volume of data inspected,
- Number of Data sources migrated to SOC, and
- Number of SOC rules, use cases, and SOC playbooks developed.

Guidehouse evaluated the benefits and features of CenterPoint Houston's proposed OT-Cybersecurity Monitoring resiliency measure qualitatively with measure-specific inputs and assumptions. This analysis compared CenterPoint Houston's resiliency measure with the NIST CSF Categories 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 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 measure was sufficiently implementing the intent of the subcategory from a resiliency perspective. The system features mapped 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. For a detailed explanation of the methodology used, refer to Section 5.1.4.

Table 5-17 lists the Functions and associated categories with high and/or medium correlations to the resiliency measure:

Table 5-17: IT/OT-Cybersecurity Monitoring Analysis Results

Function	Category
Identify	• Risk Assessment ("RA")
Detect	• Anomalies and Events ("AE") • Security Continuous Monitoring ("CM") • Detection Processes ("DP")
Protect	• Protective Technology ("PT") • Data Security ("DS") • Information Protection Processes and Procedures ("IP")
Respond	• Analysis ("AN")
Please note: Guidehouse did not include the "Recover" function in these analysis results as it did not have high or medium correlations.	

Guidehouse can conclude that CenterPoint Houston's IT/OT-Cybersecurity Monitoring resiliency measure has resiliency benefits, including reduced potential cyber-attacks and improved detection and response times to cybersecurity threats. Implementation of security measures also avoids potentially high undesirable economic and societal impacts associated with widespread, lengthy outages.

This resiliency measure focuses on receiving cyber threat intelligence and potential risks from information-sharing sources by leveraging indicators of compromise that the cyber threat and response software will use to identify a potential cybersecurity threat. This information is internally documented by the cyber threat and response software and compared to the sharing sources to determine if threats exist. It will then alert CenterPoint Houston SOC personnel with the necessary information to respond. The cyber threat and response software will also use machine learning to tune the system to reduce system noise by learning potential threats and prioritizing by risk level.

Guidehouse has determined that the measure has several areas that support strong resiliency by providing network baselining, detections of anomalous activities, cybersecurity event identification, impact determination, communication, process improvement, and maintaining threat details that would feed into event responses. These capabilities, when combined, collectively provide the support needed to maintain a resilient system and network.

Overall, Guidehouse has found a significant correlation between detective controls for system protection from malicious events and potential intrusions to support the inclusion of CenterPoint Houston's IT/OT-Cybersecurity Monitoring resiliency measure in their SRP. This measure will provide CenterPoint Houston with a cyber monitoring system that will provide real-time insight into network traffic, alert for potential threats, and support quicker responses to attempted intrusions. These controls will reduce cyber risk for CenterPoint Houston by enabling a quicker response to malicious events and attempts at intrusion, enhancing overall organizational resilience.

5.8.6.6 Benefits Analysis

CenterPoint Houston also stated that the IT/OT-Cybersecurity Monitoring Resiliency Measure is a comprehensive program that will include deploying advanced firewalls, passive network sensors, and other cyber technologies to over 400 sites. Guidehouse evaluated the benefits of CenterPoint Houston's proposed IT/OT Cybersecurity Monitoring resiliency measure. Guidehouse's analysis indicates that the resiliency measure will provide a high level of effectiveness for detecting threats to the system. Based on the results of its analysis, Guidehouse determined that the measure offers resiliency benefits. All determinations below are based on CenterPoint Houston's information on resiliency measure descriptions, interviews, and responses to data requests for additional measure details.

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

Risk Assessment ("ID.RA") *The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.*	
Analysis Results Description:	CenterPoint Houston will deploy a cybersecurity monitoring system that will identify vulnerabilities that are possibly present within devices. Once the vulnerabilities have been identified, they will be documented within and aggregated with the logging solutions threat intelligence engine for indications of compromise. This information is then leveraged against security research data sources that provide information on responding to potential threats. The monitoring system will inherently document the identified threats for processing. Identifying these threats and vulnerabilities will provide CenterPoint Houston with the necessary information to perform assessments that identify business impact likelihoods and determine their risk. The monitoring system will aggregate data to correlate against potential risks, providing cybersecurity subject matter experts ("SMEs") with critical information to make informed decisions on necessary actions to respond to a cybersecurity threat. The monitoring system will use automation to reduce system noise (*i.e.*, false or minor threats) and prioritize alerts for potential threats.

Asset Management ("ID.AM") *The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.*	
Analysis Results Description:	To ensure the successful implementation of CenterPoint Houston's cybersecurity monitoring system, all cyber-related assets and their software/applications will need to be accounted for and also maintained on an annual basis to ensure the accuracy of the inventory, which CenterPoint Houston plans to do. This ensures that all cyber systems and associated software are identified and tracked for monitoring. The data flows from each cyber system will be included as part pf the monitoring measure to ensure all system-related information is aggregated for monitoring. All resources that provide vital data into the monitoring system will need to be prioritized and managed based on their criticality to sustaining a resilient power system.

Anomalies and Events ("DE.AE") *Anomalous activity is detected, and the potential impact of events is understood.*	
Analysis Results Description:	An effective cybersecurity monitoring system should have a baseline of network operations and expected data flows to detect anomalies from users and systems. CenterPoint Houston's proposed cybersecurity monitoring system aims to provide better network visibility, analytics, and protections. The system will have machine learning capabilities that allow for a better understanding of the targets and attack methods being used. Machine learning would also constantly update the threshold for incident alerts and escalation. CenterPoint Houston will deploy Nozomi, which will analyze and catalog attack data and allow for impact evaluation for potential attacks. These two systems will allow CenterPoint Houston to better detect and evaluate the potential impacts of events.

Security Continuous Monitoring ("DE.CM") *The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.*	
Analysis Results Description:	Network monitoring is a key element for detecting cybersecurity events. It offers awareness and is a detective control that provides information to support appropriate, necessary, and timely responses to events. CenterPoint Houston's cybersecurity monitoring system will include monitoring activity for malicious code. An effective cybersecurity monitoring system should be capable of monitoring external service provider activity to detect potential cybersecurity threats. CenterPoint Houston's resiliency measure includes monitoring of the network, and better visibility and analytics that will be used for response, including internal and external traffic, personnel, connections, devices, and software. Nozomi will provide common vulnerability and exposure ("CVE") lookups based on the model and firmware of the device in a "passive scan" instead of an "active scan." A passive scan sifts through traffic, whereas an active scan sends test packets through the network.[115]

Detection Processes ("DE.DP") *Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.*	
Analysis Results Description:	Robust cybersecurity monitoring systems maintain and test detection processes and procedures to ensure awareness of anomalous events. To ensure accountability, roles and responsibilities associated with these processes and procedures should be well defined. CenterPoint Houston's deployment of the resiliency measure will have detection requirements that will allow the system to learn and tune to such detections, thereby only alerting when there is a potential threat. A primary focus of the resiliency measure will include improving the detection process, which increases system awareness for appropriate, necessary, and timely responses to events. Additionally, an effective cybersecurity monitoring system encompasses security event detection, including information communication to System Operation Control ("SOC") personnel via alerts. CenterPoint Houston indicated that SOC personnel will receive alerts through this new system and take action in response to a detected event.

Data Security ("PR.DS") *Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.*	
Analysis Results Description:	System visibility, availability, and integrity are necessary to provide a secure and resilient system. The IT/OT-Cybersecurity Monitoring resiliency measure will assist in availability by using RAID technology for backing up data stores. System resource planning has been defined and finalized for storage with defined active and non-active timeframes. Maintenance programs have been developed and finalized, with plans to be implemented as part of this resiliency measure. With this resiliency measure, CenterPoint Houston plans to actively monitor data 24x7, not just for alerts but also to ensure only authorized users access the information. OT data will be kept on premises with a "defense-in-depth" approach behind multiple firewalls. Splunk and Nozomi support industry-standard encryption for data at rest and in transit.

Information Protection Processes and Procedures ("PR.IP") *Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.*	
Analysis Results Description:	CenterPoint Houston's proposed cybersecurity monitoring system with a baseline configuration of all monitored systems necessary to identify if a bad actor is manipulating a system. This is an inherent requirement for identifying potential threats. Through interviews and data requests, Guidehouse determined that CenterPoint Houston will implement a system development lifecycle process for the resiliency measure. Additionally, a change control process will be monitored through the monitoring system, and any changes within the environment must first be approved by compliance personnel as required by NERC CIP reliability standards requirement CIP-010. A focus of this resiliency measure is to provide better protection to the enterprise system, which includes generation facilities, transmission facilities, distribution facilities, and the command center. OT monitoring will be incorporated into the SOC and incident response ("IR") and business continuity ("BC") plans. Nozomi will be used to identify vulnerabilities within the OT environment and provide vendor recommendations, integrated into CenterPoint Houston's current vendor management plan.

Protective Technology ("PR.PT") *Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.*	
Analysis Results Description:	Effective cybersecurity monitoring systems include logging systems that document and allow for a review of system logs to determine if a cybersecurity response action is warranted. CenterPoint Houston stated that Splunk would be deployed as part of their central logging system. From the interviews conducted by Guidehouse, we have concluded that CenterPoint Houston has implemented firewalls and follows network architecture best practices to protect the CenterPoint Houston environment, which will be vital for successfully implementing the CenterPoint Houston's cybersecurity monitoring system resiliency measure. Nozomi provides system-level broadcasts for detecting removable media to ensure appropriate levels of protection and restrictions are in place. Additionally, CenterPoint Houston will design alert use cases for Nozomi to process.

Awareness and Training ("PR.AT") *The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.*	
Analysis Results Description:	To ensure the efficient functioning of essential cyber monitoring systems, personnel with a role in the use and execution of the related monitoring systems will need to undergo training. The training should equip the necessary SOC personnel with the knowledge to ensure readiness to respond appropriately. CenterPoint Houston has emphasized the necessity of cybersecurity to their architects and SMEs.

Analysis ("RS.AN") *Analysis is conducted to ensure effective response and support recovery activities.*	
Analysis Results Description:	CenterPoint Houston's IT/OT Cybersecurity Monitoring system will provide a greater understanding of cyber incidents using network analysis capabilities and historical monitoring. This will improve analysis capability for both proactive and reactive threats. Monitoring occurs on OT environments 24/7, which will provide additional analysis to support response and recovery efforts. The resiliency measure will provide enhancements to alerting that can provide notifications to guide response type and potentially reduce response time.

5.8.6.7 Resiliency Measure Assessment and Conclusions

Based on information provided by CEHE, Guidehouse concluded that CEHE's IT/OT-Cybersecurity Monitoring resiliency measure has resiliency benefits, including a reduction in potential cyber-attacks, and improved detection and response times to cybersecurity threats. Implementation of security measures also avoids potentially high undesirable economic and societal impacts associated with widespread, lengthy outages.
This resiliency measure focuses on receiving cyber threat intelligence and potential risks from information-sharing sources by leveraging indicators of compromise that the cyber threat and response software will use to identify a potential cybersecurity threat. This information is internally documented by the cyber threat and response software and compared to the sharing sources to determine if threats exist. It will then alert CEHE SOC personnel with the necessary information to respond. The cyber threat and response software will also use machine learning to tune the system to reduce system noise by learning potential threats and prioritizing by risk level.

Guidehouse determined that the measure has several areas that support strong resiliency by providing network baseline, detection of anomalous activities, cybersecurity event identification, impact determination, communication, process improvement, and maintaining threat details that would feed into event responses. These capabilities, when combined, collectively provide the support needed to maintain a resilient system and network.

Overall, Guidehouse found a significant correlation between detective controls for system protection from malicious events and potential intrusions to support the inclusion of CEHE's IT/OT Cybersecurity Monitoring resiliency measure in their SRP. This measure will provide CEHE with a cyber monitoring system that will provide real-time insight into network traffic, alert

for potential threats, and support quicker responses to attempted intrusions. These controls will reduce CEHE cyber risks by enabling a quicker response to malicious events and attempts at intrusion, enhancing overall organizational resilience.

5.8.7 Cloud Security, Product Security & Risk Management

5.8.7.1 Resiliency Measure Description

CenterPoint Houston's Cloud Security, Product Security & Risk Management (CSPSRM) resiliency measure focuses on tools and processes to proactively enhance its cybersecurity posture and align with industry standards and best practices through implementations of three components:

Cloud Security is required to provide visibility, assessment, and response/recovery of cloud data systems to protect data flow to and from the cloud. CEHE currently hosts enterprise Information Technology (IT) applications with two Cloud Services Providers (CSP) for redundancy. Due to restrictions for electrical OT systems (*e.g.*, the NERC CIP reliability standards), CEHE does not have a large cloud presence for Operational Technology (OT) systems. CEHE proposes to develop security and risk management in cloud services to improve resiliency before regulatory requirements (*e.g.,* the NARUC Cybersecurity Baselines) come into effect for electrical distribution systems and ahead of the anticipated reduction in cloud restrictions on NERC OT cyber systems. The resiliency benefits of improved Cloud Security include real-time visibility into the data, continuous control monitoring of the cloud environments, alerts and findings being identified, and an improved ability to detect, respond, and recover in near real-time from cyber-attacks.

Product Security is required to protect the grid and consumers through the protection of the products in the field and of the data captured from those products. This component requires the capability to remotely update/repair/respond and recover devices that may become out of compliance due to a newly exposed vulnerability while in the field. CEHE uses the MITRE ATT&CK framework to assess attack vectors, plan around potential attack impacts, perform scenario planning, and dictate response times based on severity levels. CEHE measures cybersecurity maturity levels and performs product analysis using the NIST Cybersecurity Framework (v2.0). CEHE also implemented the CISA Secure by Design framework to build resiliency in the development phase of internal software, ties the Secure by Design framework into threat modeling and risk scenario development, and uses the framework for security and architecture risk assessments and reviews. CEHE currently has a NERC CIP-013 Supply Chain Risk Management (SCRM) measure, and this component is designed to extend and augment the SCRM measure for electrical distribution cyber systems to further manage cybersecurity risks from suppliers and their products or services used in CEHE cyber systems.

Risk Management is required to manage product and cloud security and ensure consistent application and governance of tooling, policies, and programs that support continuous

technology risk management and monitoring. By serving as a wrapper for Cloud Security and Product Security, a robust Risk Management measure will enhance CEHE's ability to identify and measure risks, assess identified risks, prioritize and mitigate risks, and align risks with appropriate protective measures and controls. CEHE stated a need to ensure the Risk Management measure has the appropriate information to identify risks up front, continuously monitor for realized risks, and take necessary actions, as applicable.

CEHE proposes a three-year plan to develop a stronger foundation for Cloud Security and Product Security (mission, goals, visions) and identify necessary activities to upgrade CEHE's current Risk Management measure in year 1. The plan for year 1 also includes analyzing the efficacy of each proposed tool and process, procuring identified tools, and developing processes and procedures, prioritizing tool and process implementations for the greatest impact. The year 2 plan consists of implementing the tools and processes and developing baseline data, while year 3 targets stabilizing and improving from the year 2 baselines to ensure CEHE has the right processes in place and is achieving the goals of this proposed resiliency measure. Moving onward from the three-year plan, CEHE plans to implement continuous monitoring and improvement processes.

Implementing these three components with the proposed three-year plan should reduce initial risks during the cyber system procurement phase, reduce risks to cyber systems once installed in the field, and ensure the cyber systems are protected from attack and available during resiliency events.

5.8.7.2 Revisions from the Prior System Resiliency Plan

None. The Cloud Security, Product Security & Risk Management resiliency measure was not included in CEHE's prior 2024 SRP.

5.8.7.3 Resiliency Measure Targets

The estimated three-year cost for this resiliency measure and investment amounts are presented below.

- Total project cost: **$10.0 million**
- Total operation and maintenance expense: **$6.0 million**

The CSPSRM resiliency measure targets increased data visibility, identification of reduced or eliminated risks in the design phase, implementation of effective protective measures and controls, and baselining CEHE's understanding of alerts and findings across the cyber system lifecycle.

5.8.7.4 Alternatives Considered

Alternatives to this resiliency measure include doing nothing and maintaining the status quo of cyber systems and associated applications physically located within CEHE facilities. Doing

nothing is not a viable option, as cyber-attacks are expected to increase in volume and severity, as identified in this report's Cyber Risk Profile section. Maintaining the status quo also reduces CEHE's ability to respond to and recover from cyber-attacks rapidly. It prevents CEHE from leveraging cloud-based cyber systems in a more resilient manner.

5.8.7.5 Resiliency Measure Metrics and Effectiveness

CEHE provided the following metrics to monitor the effectiveness of the CSPSRM resiliency measure:

- The number of identified risks,
- The number of implemented protective measures and controls,
- The number of developed baselines,
- The number of alerts and findings received by monitoring systems, and
- Reduced response and recovery times in the event of cyber-attacks.

5.8.7.6 Benefits Analysis

During discussions with CEHE, Guidehouse identified a list of products and services that will be required to fully implement the CEHE three-year plan, which includes the following task summary:

Year 1: Discovery, Scoping, Visibility, Baselining, and Beginning implementation of prioritized tools/processes;
Year 2: Accelerating Deployment of tools and deploying additional tools as needed, Tuning Policies and controls, baselining and handling of findings; and
Year 3: Stabilizing, Governance, Continuous Improvement, and Automation where applicable.

Guidehouse reviewed the proposed products and services to evaluate inherent security functions against specific NIST CSF (v2.0) Core Function Subcategories that exhibited a strong correlation. Since cybersecurity tools and processes often work together to form a defense-in-depth or defense-in-diversity posture, Guidehouse considered two scenarios during the NIST correlation process for the tools and processes in Table 5-18:

1. Where the cybersecurity function or capability was available when integrated with other tools, the correlating NIST CSF 2.0 subcategory was included.
2. Where the cybersecurity function or capability only provided information to feed another tool or process, the function or capability was considered an indirect correlation and not included.

Guidehouse included all NIST CSF Subcategories that strongly correlate to the reviewed product or service.

Table 5-18: NIST CSF V2.0 Correlations with CEHE CSPSRM Tools

Category	Tools and Processes	Correlates to NIST CSF (v2.0) Subcategories
Cloud Security	Software-as-a-Service (SaaS) Security Posture Management (SSPM)	PR.AA-01, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, DE.CM-03, DE-AE-01, RS.MA-02, GV.SC-07,
	Cloud Security Posture Management (CSPM)	ID.AM-01, ID.AM-04, ID.RA-01, PR.AA-01, PR.AA-05, PR.DS-01, PR.DS-10, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, RS.MI-01, RC.RP-01, GV.SC-06
	Cloud Workload Protection Platform (CWPP)	ID.AM-01, ID.RA-01, ID.RA-06, GV.SC-06, PR.AA-01, PR.AA-05, PR.DS-01, PR.DS-02. PR.PS-01, ID.AM-08, DE.CM-01, DE.CM-03, DE.CM-06, RS.MI-01, RC.RP-01
	Cloud Access Security Broker (CASB)	PR.AA-01; PR.AA-02; PR.AA-03; PR.AA-04, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, DE.CM-01, DE.CM-03, RS.MI-01
	Cloud Native Application Protection Platform (CNAPP)	ID.AM-01, ID.AM-05, ID.RA-01, ID.RA-06, GV.SC-06, PR.AA-01, PR.AA-05, PR.DS-02, PR.PS-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.AE-01, RS.MI-01, RC.RP-01
	Cloud Key Management Principles (CKMP)	ID.AM-01, ID.AM-05, ID.RA-01, ID.RA-06, PR.AA-01, PR.AA-05. PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, ID.RA-07, PR.PS-02, PR.IR-01, DE.CM-01, DE.CM-03, DE.AE-01, RS.MI-01,
	Third-Party Cloud Security Products under Consideration	
	CheckPoint Harmony SaaS	ID.AM-01, ID.AM-05, ID.RA-01, ID.RA-06, PR.AA-01, PR.AA-05, PR.DS-01, , PR.DS-02, PR.DS-02, PR.DS-10, PR.IR-04, PR.PS-04, DE.CM-01, DE.SC-03, DE.AE-01, DE.CM-01, DE.CM-03, RS.MA-01, RS.MA-02, RS.MI-01, RC.RP-01, ID.IM-03
	AppOmni Data Breach monitoring	ID.AM-01, ID.AM-05, ID.RA-01, ID.RA-06, ID.RA-07, PR.AA-01, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, DE.CM-01, DE.CM-03, DE.AE-01, RS.MA-01, RS.MA-02, RS.MI-01, RC.RP-01, ID.IM-03,
	Nudge Security for SaaS	ID.AM-01, ID.AM-05, ID.RA-01, ID.RA-06, ID.RA-07, PR.AA-01, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, DE.CM-01, DE.CM-03, DE.AE-01, DE.CM-01, DE.CM-03, RC.RP-01, RS.MA-02, RS.MI-01, RC.RP-01
	Data Dog (CSPM)	ID.AM-01, ID.AM-05, ID.RA-01, ID.RA-06, PR.AA-01, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-04, DE.CM-01, DE.CM-03, DE.AE-01, RC.RP-01, RS.MA-02, RS.MI-01

Product Security	**Third-Party Product Security tools under consideration**	
	MS STRIDE Threat Modeling Tool	ID.RA-01, ID.RA-02, GV.RR-04, ID.AM-08, PR.PS-02, DE.CM-01, DE.CM-09, RS.MA-01. RS.MA-02
	Fuzz Testing	ID.RA-01, ID.RA-02, PR.PS-01, DE.AE-01, RS.MA-02, RS.MI-01
	Automotive Cybersecurity & Data Management (energy version)	ID.AM-01, ID.AM-04, PR.AA-01, PR.AA-05, PR.DS-01, PR.DS-02, PR.DS-10, ID.RA-07, PR.PS-01, ID.AM-08, PR.PS-04, DE.CM-01, DE.CM-03, RS.MA-02, RC.RP-01
Risk Management	**Third-Party Risk Management Tools under consideration**	
	CycloneDX Tool Center	ID.AM-01, GV.OC-04, GV.OC-05, PR.PS-01, ID.RA-07, GV.RR-04, PR.DS-01, DE.AE-01, RS.MA-02,
	Code42 Data Behavior monitoring	ID.AM-01, ID.RA-01, ID.RA-04, PR.DS-01, PR.DS-02, DE.CM-01, DE.CM-03. GV.RR-02, RS.MA-02,
	ServiceNow SecOps	ID.AM-01, ID.AM-03, ID.RA-01, ID.IM-01, GV.PO-01, GV.PO-02, PR.PS-01, ID.AM-08, DE.CM-01, RS.MA-01, RS.MA-02, RS.MI-01, RS.CO-02,

Based on the Guidehouse NIST comparative analysis process, Guidehouse gained reasonable assurance that the tools currently in use at CEHE and the tools proposed for implementation through the three-year CSPSRM project plan provide strong correlations with relevant NIST CSF (v2.0) subcategories and offer significant resiliency benefits for cyber systems associated with the CEHE electrical distribution system.

As cited in the Project Description section above, CEHE also reported the use of various cybersecurity processes and frameworks (see Table 5-19) to perform Threat Modeling, Risk Assessments, and other Risk Management practices. Guidehouse concurred with using these frameworks and processes to manage current and future risks, as they have been vetted and are commonly used across the electrical sector. Guidehouse did not further evaluate these practices against the NIST CSF v2.0 Core Function categories or subcategories.

Table 5-19: CEHE Risk Management Approach, Cybersecurity Frameworks, and Processes

Cybersecurity Frameworks and Processes	Description
Threat Modeling	CEHE applies threat modeling to systematically analyze systems and applications to identify potential vulnerabilities and threats by simulating various attack scenarios. This allows security teams to understand how attackers might exploit weaknesses and proactively implement mitigation strategies to minimize risk. CEHE implements threat modeling as a proactive approach to security planning by visualizing potential attacks on a system to identify areas for improvement.

Cybersecurity Frameworks and Processes	Description
Cybersecurity Risk Assessments	CEHE performs cybersecurity risk assessments to evaluate its cyber defenses against cyber threats. This helps CEHE identify and quantify threats and determine the likelihood and impact of each threat. The result is a prioritized list of risks that CEHE SMEs can address to prevent data breaches and application downtime, avoid long-term costs and reputational damage, and keep CEHE's risk profile current.
Cybersecurity Vulnerability Assessments	CEHE performs cybersecurity vulnerability assessments to identify, evaluate, and address vulnerabilities in its identified cyber systems, processes, and operations. CEHE includes vulnerability scans, assessments, prioritization, and remediation of identified vulnerabilities, as well as continuous vulnerability management to manage risks associated with identified vulnerabilities.
Threat Assessment and Remediation Analysis (TARA)	CEHE applies TARA to identify, evaluate, and prioritize potential cyber threats, then develop and implement plans to mitigate those risks by addressing vulnerabilities and taking corrective actions. CEHE also uses TARA to actively work to mitigate weaknesses that could be exploited.
MITRE ATT&CK Framework	CEHE applies the MITRE ATT&CK framework to understand and respond to cyber threats by documenting common behaviors of cyber attackers or adversaries, anticipating attacker moves, mitigating risks, developing better defenses and incident response plans, and prioritizing network defenses.
NIST Cybersecurity Framework (CSF, v2.0)	CEHE measures cybersecurity maturity levels on the NIST CSF (v2.0) to track maturity across its service offerings and applies the CSF to perform product analysis during procurement processes.
Container Security	CEHE implemented Cloud container security using NIST SP 800-190 & NIST SP 800-53r5 protective measures and controls.
API Security (best practices)	CEHE implemented an application security program to test code and services and evaluate vulnerabilities and risks in its continuous development pipeline.
CISA Secure by Design	CEHE implements CISA Secure by Design as a framework for building in resiliency up front in the development phase. This framework is tied to threat modeling and risk scenario development. CEHE applies this tool for security risk assessments and architecture risk assessments and reviews.
Supply Chain Risk Management (SCRM)	CEHE reported the use of common SCRM processes to implement best SCRM practices in the lifecycle management of products or services for CEHE cyber systems, including:
Design of Experiments – Supply Chain Principles (DOE-SCP)	CEHE implements DOE-SCP to systematically identify and optimize key variables within the supply chain process to improve overall efficiency and performance to achieve cost reduction and targeted improvements across the CEHE supply chain through experimentation and data analysis.
Supply Chain Cybersecurity Principles (SCCP)	CEHE implements SCCP as best practices for cybersecurity throughout the supply chain that support and secure CEHE cyber systems and technologies before they are exploited by cyber actors seeking to cause destruction or disruption to critical CEHE infrastructure.
Hardware Bill of Materials (HBOM)	CEHE is implementing a third-party risk management process to manage the risk of the supplier, which is currently in place, and manage the risks of the suppliers' products and services, using HBOM and SBOM, which will be implemented in this resiliency measure. The HBOM framework provides a standardized way to name and identify components and offers guidance on what information to include in an HBOM. It also helps organizations communicate about hardware components in the supply chain and allows CEHE to make decisions about a product's origins or security risks.
Software Bill of Materials (SBOM)	As a key component of an overall SCRM measure, the SBOM provides a detailed list of all software application components, including open-source and third-party

Cybersecurity Frameworks and Processes	Description
	components, licenses, versions, and patch status. The SBOM also allows CEHE to identify and manage risks, track vulnerabilities, ensure compliance, and improve transparency.
NERC SCRM Practices	CEHE has a current NERC CIP-013 SCRM program for applicable transmission cyber systems. CEHE plans to augment and adapt that program to develop an SCRM measure for its distribution cyber systems. As a resiliency measure, CEHE envisions applying the augmented SCRM measure to reduce initial procurement risks and lifecycle risks when cyber systems are installed in the field. The distribution SCRM measure is expected to provide better visibility to the data, design out some risks up front, and reduce response times in the event of cyber-attacks.

Based on an understanding of CEHE's use of the various cybersecurity frameworks and processes in Table 5-19, Guidehouse gained reasonable assurance that the CSPSRM project will provide significant cybersecurity protective measures and controls in the event of a cyber-attack and will support higher resiliency as an enabling factor for cyber systems associated with the CEHE electrical distribution system and other proposed resiliency measures.

5.8.7.7 Resiliency Measure Assessment and Conclusions

Guidehouse concludes that the proposed Product Security, Cloud Security, & Risk Management resiliency measure is justified with respect to strong correlations for proposed tools with various NIST CSF (v2.0) Core function subcategories (see Table 5-18) Guidehouse also confirmed CEHE has established a strong cybersecurity foundation by applying existing frameworks, processes, and other risk management approaches (see Table 5-19). Guidehouse further determined CEHE has a feasible three-year plan to expand cybersecurity protective measures and controls to enhance cybersecurity as an enabling factor and provide better resiliency to the CEHE cyber systems and associated electrical distribution system services and facilities. Guidehouse gained a reasonable assurance that the CSPSRM resiliency measure is needed to support higher operational service levels and improved resiliency for electrical system operations and determined CEHE can cost-effectively obtain significant benefits through the implementation of this resiliency measure.

5.9 Situational Awareness

5.9.1 Measure Category Summary

Situational awareness measures, presented in Table 5-20 include several measures that overlap with resiliency event categories listed earlier in this report. Foremost among these are proposed enhancements to the Advanced Aerial Imagery/Digital Twin measure that CenterPoint Houston has and will continue to apply to identify and mitigate assets at risk of failure or impacts during resiliency events. It also includes cameras and weather stations to detect incipient wildfire conditions or events, and that will provide critical input to advanced analytical models that CenterPoint Houston is proposing under the Extreme Weather (Drought) event category.

Additionally, situational awareness measures proposed in CenterPoint Houston's prior SRP include upgrades to the existing Backhaul Microwave Communication system and Voice & the Mobile Data Radio System.

Table 5-20: Situational Awareness Resiliency Measures Costs and Benefits

Resiliency Measure	RM Number	3-Year Capital Cost ($MM)	3-Year O&M Expense ($MM)	BCA Ratio	3-Yr CMI 2026-2028 (million)	Annual CMI 2028 (million)
Situational Awareness						
Advanced Aerial Imagery	RM - 33	$18.4	$2.0	4.8	10.8	5.1
Group Subtotal		**$18.4**	**$2.0**	**4.8**	**10.8**	**5.1**

5.9.2 Benchmarking

Peer Utility Benchmarking Survey

The peer utility benchmarking survey, discussed in Appendix A, indicates that five (5) of eleven (11) respondent utilities address communications systems in their resiliency programs (Figure A-3). Furthermore, Table 5-21 indicates that seven (7) of nine (9) respondent utilities include at least one of the surveyed situational awareness measures included in Table 5-21 within their resiliency programs, and three (3) utilities include all of these measures.

Table 5-21: Resiliency Survey Investment Types (Situational Awareness Measures)

Type of Investment[116]	Respondent Utility Company ID								
	102	103	106	107	108	109	114	122	123
Monitoring of assets	✓	✓				✓	✓	✓	
Microwave communications	✓	✓					✓	✓	
Voice and mobile data enhancements	✓	✓					✓	✓	
Use of monitoring cameras, communications	✓	✓	✓				✓	✓	
Changes to emergency response plans		✓		✓			✓	✓	

Source: Guidehouse analysis, based on inputs from the First Quartile Resiliency Survey

Jurisdictional Benchmarking

The jurisdictional benchmarking report, provided as Appendix B, also indicates that the types of situational awareness measures proposed by CenterPoint are common across jurisdictions. Some specific examples include:

[116] This table includes only the subset of resiliency measures included in the survey that are most closely associated with the measures included by CenterPoint Houston within this risk category (Situational Awareness). These were not categorized as such within the survey, and respondent utilities may categorize them differently. The full list of surveyed measures is included in Figure A-2.

- Green Mountain Power is making a concerted effort to invest in measures that ensure reliable and resilient grid operations. The utility stated that programs will be concentrated in three key areas, including enhancements to their communications technology.[117]
- Dominion Energy Virginia received approval of a Plan for Electric Distribution Grid Transformation Projects that included telecommunications and physical security enhancements.[118]

Within Texas, SRPs submitted by other utilities—including Oncor and TNMP—have included situational awareness measures similar to those proposed by CenterPoint Houston.

5.9.3 Advanced Aerial Imagery/Digital Twin

5.9.3.1 Resiliency Measure Description

CenterPoint Houston's Advanced Aerial Imagery Platform / Digital Twin resiliency measure is designed to improve and enhance the visibility of the overall transmission, substation, and distribution systems managed by CenterPoint Houston by digitizing a replication of the physical equipment installed. This will allow for an overlay of imagery to determine vegetation management risk and analyze potential improvements to equipment to improve performance during extreme weather event conditions. Improvements made would be based on good engineering design standards before incurring the expense of installing equipment upgrades. This allows for a more streamlined approach, including a reduction in engineering design time, improvements in installation expediency and placement of equipment, increased resiliency, and customer benefits.

Over time, CenterPoint Houston proposes to leverage this software in tandem with other software to "rank" projects based on their value-add to customers. Utilizing this software will help reduce costs over time by focusing on improvements with the greatest resiliency benefits. CenterPoint Houston will leverage the digital model to review and determine optimal placement of projects, maximizing potential benefits for future resiliency efforts as well as identifying other resiliency measures or projects that could offer higher benefits. This software is also capable of "learning" and leveraging prior analyses to improve future projects. It can also be used to review different scenarios and model the performance of these improvements in different extreme weather event scenarios, as well as leveraging the imagery to determine encroachments from vegetation (or other sources) and identify broken/leaning equipment to address.

CenterPoint Houston intends to initially prioritize this software to determine how existing projects are performing from a resiliency basis and use this to determine if/how these projects could provide improved resiliency (*e.g.*, better location, greater number per circuit, and potential

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

[118] 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).

weather risks are a few examples of how this will be leveraged). The estimated three-year cost for this resiliency measure and investment amounts are presented below.

- Back-casting analysis targeted for the entire system was completed in 2024. Leveraging the software to produce a detailed analysis on a per device/circuit is estimated to reduce the amount of study time for manual processes (from days to hours)
- Forecasting analysis for existing initiatives targeted for the entire system began in late 2024 and will continue, without interruption, to support enhancements/modifications to plans. This will allow for more granular circuit-level analysis.

5.9.3.2 Revisions from the Prior System Resiliency Plan

The total cost of the Digital Twin measure increased from $9.0 million to $20.4 million, which includes O&M of $2.04 million. The increased cost is associated with accelerated deployment, as well as the addition of new functional capabilities including a vegetation model incorporating encroachment and fall-in risk, increased LiDAR resolution, and hyperspectral imagery to predict vegetation growth.

5.9.3.3 Resiliency Measure Targets

Total estimated project cost: **$20.4 million** over the 3-year Plan, including **$2 million** in IT support providing centralized data products to digital technologies and analytics applications to enable real-time decision-making. Doing so involves developing a reusable data foundation to support grid resiliency. This foundation will use cloud-native technologies to improve agility, resiliency, performance, and ease of use. This data foundation will be leveraged for data analysis, machine learning and AI, and digital technologies. As of January 2024, CenterPoint Houston has shared data with the software vendor in a test environment (after starting the overall vendor selection process in September 2023) and is now working to transition to the production environment. Once the transition to the production environment is complete, CenterPoint Houston will begin analyzing circuits for its initial backcast analysis. The three-year operation and maintenance expense is **$2.0 million**.

5.9.3.4 Alternatives Considered

CenterPoint Houston evaluated it proposed improved Advanced Aerial Imagery Platform / Digital Twin resiliency measure in comparison to its existing methodology and was able to identify significant improvements through this new software, including reduced analysis time and a progression of improvements in design and project location achieved by AI "learning." CenterPoint Houston reviewed and analyzed the qualifications of many different vendors and determined the best solution to meet its needs. One alternative considered is described below.

1. **Build Internal Software Applications**—Building in-house software applications to perform similar functions would likely take much more time, estimated at approximately 24-36 months. CenterPoint Houston rejected this option because it seeks a more immediate solution than this option provides.

5.9.3.5 Resiliency Measure Metrics and Effectiveness

In collaboration with Guidehouse, CenterPoint Houston proposes to perform an analysis of events to determine the correctness of the algorithms for the digital twin models.

CenterPoint Houston will track and report to the PUCT annually the percentage of programmatic decisions made using the digital twin. Adjustments may need to be made, but CenterPoint Houston believes that improvements in the resiliency of CenterPoint Houston's transmission and distribution system should be seen.

5.9.3.6 Benefits Analysis

Guidehouse evaluated the benefits associated with CenterPoint Houston's proposed Advanced Aerial Imagery Platform / Digital Twin resiliency measure on a quantitative and qualitative basis. The quantitative analysis adheres to the BCA methodology described in Section 5.1, with resiliency measure-specific inputs and assumptions described below.

1. **Quantitative Benefits** – Key assumptions include estimates of the average number of sustained interruptions avoided on circuits targeted for improvements during storms, the average number of customers or load at risk, and the estimated time to restore service. The reduction in failure rate where analysis is performed is approximated at 10% for an estimated 100 distribution projects (based on other utility results). The estimated average load at risk generally varies by resiliency measure. It depends on the review but is estimated to be a minimum of 15 MW (and likely much greater) with a minimum restoration time of 4 to 8 hours. The estimated time to repair the damage is 5 days during extreme weather conditions. Other benefits include reduced costs for truck rolls and crew labor to restore service without damage; it also provides design efficiency benefits and better selection for locating new equipment. The annual maintenance expense for software support is $20,000. The Advanced Aerial Imagery Platform / Digital Twin resiliency measure is expected to reduce cumulative CMIs by 0.8 million over the 3-year Plan and 0.3 million annually by 2027. From these assumptions, Guidehouse derived a BCA of 3.4.

   Qualitative Benefits – The potential to improve engineering designs with greater visibility into the grid is significant, particularly for extreme weather events. When leveraged with all other resiliency measures, this advanced aerial imagery platform coupled with the software analysis materially reduces the cost of engineering design, enhances vegetation management and improves IGSD schemes, assists in targeting transmission tower/pole and distribution pole resiliency, and flooding event mitigation, among other potential applications.

5.9.3.7 Resiliency Measure Assessment and Conclusions

Guidehouse concludes that CenterPoint Houston's Advanced Imagery Platform/Digital Twin resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's SRP for the following reasons:

- The addition of the imagery platform and Digital Twin will enhance the functionality of CenterPoint Houston's transmission and distribution system by analyzing and mitigating the risks of line failures, enhancing the grid's resiliency during extreme weather events.
- CenterPoint Houston will leverage the proposed software to improve the design of its transmission, substation, and distribution systems while providing greater withstand capabilities during extreme weather events. It will also provide guidance for the optimal location of equipment to mitigate outages and provide greater customer benefit.
- Guidehouse's analysis of CenterPoint Houston's Advanced Aerial Imagery Platform / Digital Twin resiliency measure produced a BCA that confirms the measure's cost-effectiveness.
- The use of advanced aerial imagery as an input to a Digital Twin system is consistent with trends in utility industry best practices deployed at other utilities based on prior Guidehouse experience.
- The resiliency measure contributes to CenterPoint Houston's overarching objective of increasing the resiliency of the electric grid.

5.9.4 Weather Stations

5.9.4.1 Resiliency Measure Description

Control center personnel will use weather station data as one measure to detect incipient wildfires rapidly. Data obtained from weather stations will also be used in conjunction with the Wildfire Modeling and Analytics measure.

5.9.4.2 Revisions from the Prior System Resiliency Plan

The amount CenterPoint Houston proposes to spend on weather stations has not materially changed from the prior SRP. Weather station real-time data will be used in a manner similar to the prior SRP, with increased emphasis on integrating TechnoSylva applications for detecting at-risk areas.

5.9.4.3 Resiliency Measure Targets

Targets for weather stations are for ongoing enhancements to weather data collection and application for use in associated analytical models, including those used to proactively identify conditions when wildfire exposure is high, assets that may active as an ignition source, and for predictive modeling of wildfire spread.

5.9.4.4 Alternatives Considered

There are very few options for gathering the granularity of weather data necessary to feed the various models to ascertain reliable results. One such option was to leverage only outside data, but the granularity of data was not enough to model to the level of accuracy necessary to

provide sustainable results for the preparation and deployment of resources, and this was not a viable option. The only other option was not to maintain these stations, but this could lead to weather stations being down and not delivering the necessary data to feed models and ascertain the granular results needed. This, too, was not a viable option.

Weather stations are essential for detecting wildfire events and accurately supporting predictive analytical tools CenterPoint Houston is proposing related measures.

5.9.4.5 Resiliency Measure Metrics and Effectiveness

CenterPoint Houston transitioned from an asset-centric program-based approach to a project-based approach using co-optimized sets of project types to address resiliency challenges specific to geographic regions in its service area. Using an array of best practice project type alternatives, different project types were selected in each area to enhance resiliency and structural hardening at a discrete asset level.

Distribution system mitigations are focused on areas of higher predicted damage concentration to maximize overall system restoration efficiency. When optimized at the project level, these mitigations require considering interdependencies between mitigations contemplated for the same distribution feeder/area. For example, strategic undergrounding changes the need for automation and vegetation management frequency. As a result of using the co-optimized project-based approach, CenterPoint Houston will use efficacy measures that capture the complementary nature of project-based system resiliency plans. This approach is consistent with industry best practices and measures success as a product of regional performance instead of individual asset performance.

Measurements:

1. Percent of planned asset installations completed by County
2. Percent change in predicted damage based on the event type.
3. Normalized total system restoration performance during Resiliency Events pre- and post-completion of mitigation projects based on the event type.
4. Normalized restoration performance of predicted high damage concentration area compared to Normalized total system restoration performance pre- and post-completion of mitigation projects during Resiliency Events based on the event type.

5.9.4.6 Benefits Analysis

Weather stations provide real-time weather data necessary to support CenterPoint Houston's wildfire monitoring and detection functions. The data obtained from weather stations allows CenterPoint Houston to detect wildfire events proactively. Data from weather stations is a key input to an adjunct analytical model that will be used to predict wildfire spread potential, ignition risk and identify areas susceptible to wildfires.

5.9.4.7 Resiliency Measure Assessment and Conclusions

The relatively low cost of weather stations versus the value provided by real-time weather data strongly supports CenterPoint Houston's request for PUCT approval of this measure. Weather stations are an essential component of comprehensive wildlife mitigation programs and will enhance CenterPoint's Houston's ability to proactively detect incipient wildfire events and provide data for identifying areas susceptible to wildfires.

5.9.5 Wildfire Cameras

5.9.5.1 Resiliency Measure Description

Control center personnel will use Wildfire Detection Cameras to detect incipient wildfires rapidly. Data obtained from cameras will also be used with the Wildfire Modeling and Analytics measure.

5.9.5.2 Revisions from the Prior System Resiliency Plan

CenterPoint Houston proposes to decrease spending on wildfire cameras from the prior SRP, with total spending below $1 million.

5.9.5.3 Resiliency Measure Targets

Similar to weather stations, targets for cameras are for ongoing enhancements to data collection and application for use in associated analytical models, including those used to proactively identify incipient wildfires, locate assets that may active as an ignition source, and potential for wildfire spread.

5.9.5.4 Alternatives Considered

With wildfires becoming a larger issue in Texas, CenterPoint Houston decided to add wildfire measures within the SRP. The only real alternative to adding these measures is not to provide and prepare for wildfire mitigation. In recent history, there has been a significant uptick in the number of drought and heat days, lending to the higher possibility of fuel for wildfires. Considering this, the risk of wildfire is increasing within CenterPoint Houston's territory, and mitigation measures must begin. The option of not proactively preparing for wildfires was not a viable option due to the increased risk seen within the territory (drought conditions in recent years, wildfire in Brazoria County in 2024, the Smokehouse Creek fire, and most recently, the Los Angeles fires are just a few examples of the risk).

CenterPoint Houston has identified and is proposing four extreme temperature (drought) wildfire Resiliency Measures—each a recognized best practice within the utility industry—as measures most likely to help mitigate the risk of wildfires in CenterPoint Houston's service area and areas outside its service area in which it operates facilities. CenterPoint Houston will consider how all or some of the measures can work in combination to address the specific service area risk

confronting CenterPoint Houston most appropriately. Wildfire cameras are essential accurately to detect wildfire events and support predictive analytical tools CenterPoint Houston is proposing in related measures.

5.9.5.5 Resiliency Measure Metrics and Effectiveness

CenterPoint Houston transitioned from an asset-centric program-based approach to a project-based approach using co-optimized sets of project types to address resiliency challenges specific to geographic regions in its service area. Using an array of best practice project type alternatives, different project types were selected in each area to enhance resiliency and structural hardening at a discrete asset level.

Distribution system mitigations are focused on areas of higher predicted damage concentration to maximize overall system restoration efficiency. When optimized at the project level, these mitigations require considering interdependencies between mitigations contemplated for the same distribution feeder/area. For example, strategic undergrounding changes the need for automation and vegetation management frequency. As a result of using the co-optimized project-based approach, CenterPoint Houston will use efficacy measures that capture the complementary nature of project-based system resiliency plans. This approach is consistent with industry best practices and measures success as a product of regional performance instead of individual asset performance.

Measurements:

1. Percent of planned asset installations complete by County
2. Percent change in predicted damage based on the event type.
3. Normalized total system restoration performance during Resiliency Events pre and post-completion of mitigation projects based on the event type.
4. Normalized restoration performance of predicted high damage concentration area compared to Normalized total system restoration performance pre and post-completion of mitigation projects during Resiliency Events based on the event type.

5.9.5.6 Benefits Analysis

Cameras provide real-time visualization of rights-of-way and circuits needed to support CenterPoint Houston's operations staff for wildfire monitoring and detection. They also provide CenterPoint Houston with real-time visual status and notification to proactively detect wildfire events.

5.9.5.7 Resiliency Measure Assessment and Conclusions

The relatively low cost of cameras and visualization and notification features strongly support CenterPoint Houston's request for PUCT approval of this measure. Cameras are an essential component of comprehensive wildlife mitigation programs and will enhance CenterPoint's Houston's ability to proactively detect incipient wildfire events.

5.9.6 Voice & Mobile Data Radio System

5.9.6.1 Resiliency Measure Description

CenterPoint Houston's Voice & Mobile Data Radio System resiliency measure will apply a phased approach by service area and 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 Houston currently has a disparate communication system that includes cell phones and multiple manufacturers and models of radios including handhelds and truck radios. The radios are the primary communication method used within the organization for fieldwork. However, CenterPoint Houston has had recent issues with obtaining replacement parts for radio equipment that has become outdated. These measures will consist of upgrading outdated equipment that has been in service for 13+ years and is considered end-of-life or no longer has replacement parts readily available. This upgrade will improve CenterPoint Houston's ability to maintain or restore communication during extreme weather events if radio equipment fails. Additionally, the resiliency measure involves connecting all CenterPoint Houston field personnel with radios to the upgraded communication system for more universal coverage.

The estimated 3-year cost for this measure is $15.6 million.

5.9.6.2 Revisions from the Prior System Resiliency Plan

None. The Voice & Mobile Data Radio System resiliency measure is unchanged from the 2024 CEHE SRP.

5.9.6.3 Resiliency Measure Targets

The estimated three-year cost for this resiliency measure and investment amounts is presented below.

- Total project cost: **$20.9 million**
- Total operation and maintenance expense: **$0.0**

In CEHE's experience, the voice and mobile data radio system has been critical to the safety of personnel and safe operations. During restoration events, areas regularly do not have adequate cell coverage, and the system has been the only means for field personnel to communicate with management and other team members. The ability to communicate with other individuals in the organization about status and issues is important to the restoration activities, in addition to standard operating procedures.

CEHE has also found radio communications to be efficient for notifying all crews in a given area, which is critical to the safety of personnel and safe operations. Cellular communications are inherently inefficient when trying to communicate in a "one-to-many" scenario. Situational awareness is key when multiple crews, including contractors, are involved in circuit operations.

A single radio call can inform multiple groups without requiring individual names and phone numbers.

CEHE expects upgraded voice and mobile communications capabilities to support better overall resiliency of CEHE's electrical distribution system and enhanced customer service.

5.9.6.4 Alternatives Considered

CenterPoint Houston considered a private LTE communication system but determined it could not be adopted in time to meet short-term and mid-term communication needs. There are no viable alternatives, leaving refresh as the only option. Utilization of a Project 25 ("P25") or Digital Mobile Radio ("DMR") system in Land Mobile Radio ("LMR") is possible. However, the need from the LMR is still the same: portability, mobile radio coverage, and connectivity through a dispatch console system. It was determined this would be the most feasible approach.

5.9.6.5 Resiliency Measure Metrics and Effectiveness

Guidehouse used a qualitative comparative analysis approach to evaluate this measure. A quantitative analysis was not conducted due to data limitations and a lack of metrics against which to benchmark. Rather, Guidehouse evaluated the benefits and features of this proposed resiliency measure qualitatively with measure-specific inputs and assumptions.

CenterPoint Houston plans to use the following performance metrics for tracking the effectiveness of the Voice & Mobile Data Radio System 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.

This analysis compared CenterPoint Houston's resiliency measure with the NIST CSF Categories, to identify levels of correlation between the five CSF Functions and the proposed system in terms of developing resilient systems. Guidehouse's analysis determined whether the resiliency measure had high, medium, or low correlations to the individual subcategories of the 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 measure was sufficiently implementing the intent of the subcategory from a resiliency perspective. The system features mapped to low correlation were considered relatively ineffective in improving resiliency. However, depending on the context of the proposed resiliency measure, they may still have

value in pursuing from reliability or policy perspectives. For a detailed explanation of the methodology used, refer to Section 5.1.4.

Table 5-22 lists Functions and associated categories with high and/or medium correlations to the resiliency measure:

Table 5-22: Voice & Mobile Data Radio System Analysis Results

Function	Categories
Identify	• Risk Assessment ("RA") • Risk Management Strategy ("RM")
Protect	• Access Control ("AC") • Data Security ("DS") • Information Protect Processes and Procedures ("IP") • Protective Technology ("PT")
Respond	• Communications ("CO")
Recover	• Communications ("CO")
Please note: Guidehouse did not include the "Detect" function in these analysis results as it did not have high or medium correlations.	

5.9.6.6 Benefits Analysis

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

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

Risk Assessment ("ID.RA") *The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.*	
Analysis Results Description:	Identifying risks, including vulnerabilities, potential impacts, and threats, supports resiliency by being one of the first steps for risk management as a core element for mitigating impact on power operations. 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, impacting power operation responses, especially during extreme weather events.

Risk Management Strategy ("ID.RM") *The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.*	
Analysis Results Description:	Risk management strategies support resilience by ensuring risk tolerances are understood so mitigation efforts can be established and implemented. CenterPoint Houston identified a risk of failure to end-of-life radio components, 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 risks to system operations and restoration.

Access Control ("PR.AC") *Access to physical and logical assets and associated facilities is limited to authorized users, processes, or devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.*	
Analysis Results Description:	Limiting access to devices for individuals who need access supports resilience by ensuring that only those who require access to a device can attain it and dissuades those who do not from manipulating it. 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") *Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.*	
Analysis Results Description:	From a risk strategy perspective, hardware integrity verification and availability are important to ensure communications are available, authentic, complete, and tamperproof. CenterPoint Houston plans to strengthen integrity verification and availability, including adequate communication capacity, based on information provided by each vendor in the Request for Proposal process. For this refresh, CenterPoint Houston requires potential vendors 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") *Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.*	
Analysis Results Description:	Establishing agreements as necessary and defining details for equipment assists with the resilience of the power system by ensuring the devices are being used on the appropriate frequencies and any agreements with third parties are in place so there are agreed-upon terms of usage and support. 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 potentially re-signing co-channeling agreements with third parties to address frequency usage.

Protective Technology ("PR.PT") *Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.*	
Analysis Results Description:	Protected communication networks and mechanisms, such as failsafe, load balancing, etc., are needed to ensure the communication system is available in both normal and adverse situations, which supports the resilience of power system operations. 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, improved communication load balancing and backup systems will be used in instances of device/equipment failures.

Communications ("RS.CO") *Response activities are coordinated with internal and external stakeholders, (e.g., external support from law enforcement agencies).*	
Analysis Results Description:	Incident response activities are key in supporting system and operations resiliency. CenterPoint Houston plans to continue using the radio system for communications specific to incident investigations and field coordination to respond to impacts from extreme weather events. Radio is also the method used to report incidents.

Communications ("RC.CO") *Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).*	
Analysis Results Description:	Communication of recovery activities and third-party agreements is necessary to provide a time-sensitive response for system recovery and restoration. CenterPoint Houston plans to continue using the radio system for communication and coordination activities specific to recovery and system restoration and will have third-party agreements in place for equipment warranties, maintenance, and support.

5.9.6.7 Resiliency Measure Assessment and Conclusions

Guidehouse concludes there is a high correlation between system and business resilience and system restoration with CenterPoint Houston's Voice & Mobile Data Radio System resiliency measure. This was based on the high level of correlation the measure has to the NIST CSF functions. Particular areas in which this resiliency measure supports a strong and resilient electric transmission and distribution system include:

- Risk Management regarding updating equipment that no longer has replacement parts available.

Traditional communication methods such as landlines or cellular networks can be less reliable during emergencies or natural events than radio communications. The benefits that will be realized with this measure are listed below:

- Consistent communication for CenterPoint Houston personnel extends to field personnel. Having access to radio communications will provide greater communication coverage, ensuring quicker responses to outages or other impacts on system operations.
- Ability to have redundancy and backup power sources to minimize impacts on communications during emergencies.

Guidehouse determined that the Voice & Mobile Data Radio System resiliency measure is necessary for CenterPoint to strengthen the resiliency of its electric transmission and distribution system through dependable and universally used communication methods.

5.9.7 Backhaul Microwave Communication

5.9.7.1 Resiliency Measure Description

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 aims to

streamline operations by minimizing personnel needing to carry multiple pieces of technology and maintain multiple system platforms. Upgrading and modernizing with standardized field devices will allow CenterPoint Houston to move into technologies and implementations such as field transparency, metrification of field data, mitigation of concurrency misalignments, and dashboarding at a level that was not possible previously. Converging to a single centralized system will also provide CenterPoint Houston with the possibility of new automation and availability options that were not previously available. Backhaul support will extend to CenterPoint Houston's transmission and distribution operations and service centers as a primary or secondary data communication method between facilities.

Additionally, the microwave system will support the transfer of information from substations to CenterPoint Houston personnel. The microwave system is a backup system for monitoring and controlling field devices where there is fiber optic control and is a primary system at sites that are not fiber-compatible.

The estimated 3-year cost for this resiliency measure is $12.1 million.

5.9.7.2 Revisions from the Prior System Resiliency Plan

None. The Backhaul Microwave Communication resiliency measure is unchanged from the 2024 CEHE SRP.

5.9.7.3 Resiliency Measure Targets

The estimated three-year cost for this resiliency measure and investment amounts is presented below.

- Total project cost: **$12.1 million**
- Total operation and maintenance expense: **$0.0**

Redundancy is one of the primary methods for ensuring a resilient electric delivery service. Having a secondary method of communication available during extreme weather or cybersecurity events has helped reduce the risk of critical data loss. Additionally, enhancements to the microwave system directly impact CenterPoint Houston's ability to perform remote operations effectively.

CEHE expects upgraded microwave communications capabilities to support better overall resiliency of CEHE's electrical distribution system and enhanced customer service.

5.9.7.4 Alternatives Considered

CenterPoint Houston considered multiple communication alternatives when evaluating this resiliency measure. The primary alternative would be using fiber optics at all facilities and assets. While a desirable alternative, CenterPoint Houston determined this is not feasible due to the cost and difficulty of creating fiber optics connections to remote locations and assets.

CenterPoint Houston, however, does have fiber to many of its locations, and, in those locations, it is the primary communication method used. CenterPoint Houston currently has older microwave communication equipment for facilities that are not fiber-compatible. For these facilities, CenterPoint Houston considered simply maintaining the existing equipment. CenterPoint Houston determined that it needs to acquire updated equipment due to the lack of support end-of-life equipment inherits, 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 Houston concluded that purchasing a modern backhaul microwave system for communication needs at its locations and assets was the most resilient and efficient communication option for the organization. Such modern equipment would eliminate the end-of-life issues related to CenterPoint Houston's existing equipment that is not fiber-compatible.

5.9.7.5 Resiliency Measure Metrics and Effectiveness

Guidehouse reviewed CenterPoint Houston's Backhaul Microwave resiliency measures using a qualitative comparative analysis. A quantitative analysis was not conducted due to data limitations and a lack of metrics against which to benchmark.

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.

Guidehouse evaluated the benefits and features associated with CenterPoint Houston's proposed Backhaul Microwave resiliency measure qualitatively with measure-specific inputs and assumptions. This analysis compared CenterPoint Houston's resiliency measure with the NIST CSF Categories 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 measure was sufficiently implementing the intent of the subcategory from a resiliency perspective. The system features mapped to low correlation were considered relatively ineffective at improving resiliency. However, depending on the context of the proposed measure, they may still have value in

pursuing from reliability or policy perspectives. For a detailed explanation of the methodology used, refer to Section 5.1.4.

Table 5-23 lists Functions and associated categories with high and/or medium correlations to the resiliency measure:

Table 5-23: Backhaul Microwave Communication Analysis Results

Function	Categories
Identify	• Asset Management ("AM") • Business Environment ("BE") • Risk Assessment ("RA") • Supply Chain Risk Management ("SC")
Protect	• Access Control ("AC") • Data Security ("DS") • Information Protection Processes and Procedures ("IP") • Maintenance ("MA") • Protective Technology ("PT")
Detect	• Security Continuous Monitoring ("CM")

5.9.7.6 Benefits Analysis

Guidehouse evaluated the benefits associated with CenterPoint Houston's proposed Network Security and Vulnerability Management resiliency measure Guidehouse's analysis indicates that the measure will provide a high level of effectiveness for detecting threats to the system. Based on the results of its analysis, Guidehouse determined that the 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 measure details.

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

Asset Management ("ID.AM") *The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.*	
Analysis Results Description:	Asset management is a vital part of resiliency. Identifying the hardware for upgrades or expansion helps manage, protect, and ensure system availability. CenterPoint Houston will inventory the associated microwave hardware to successfully implement the resiliency measure. CenterPoint Houston will replace end-of-life equipment to create a standard microwave system. This will require identifying all end-of-life equipment and new replacement equipment, leading to a better repair and maintenance program and thereby 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 is the penultimate goal of the resiliency measure. Investing in new radio equipment will strengthen CenterPoint Houston's communication infrastructure while enhancing resiliency.

Business Environment ("ID.BE") *The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.*	
Analysis Results Description:	Understanding the dependencies that need to be prioritized to ensure CenterPoint Houston meets its objectives is a critical part of resiliency. The Backhaul Microwave Communication resiliency measure will improve communication for multiple platforms that depend on it as a primary or secondary method for data communication. The microwave system is used for data communication into the SCADA system, assisting with supporting meters for industrial business, improving security by providing video feeds from some substation locations, and improving system health by sending traveling wave data, data from digital fault recorders, and monitoring capacitor banks in the field. As part of the microwave refresh, CenterPoint Houston 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.

Risk Assessment ("ID.RA") *The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.*	
Analysis Results Description:	Identifying the risks to the system is critical to resilience because it improves CenterPoint Houston's situational awareness of weaknesses that could be exploited. The Backhaul Microwave Communication resiliency measure will include various risk assessment activities that will help CenterPoint Houston understand where additional controls need to be implemented. Before deploying and implementing the new equipment into production, CenterPoint Houston will evaluate the vendor and the product. The evaluation is scoped to be a technical assessment of vulnerabilities within the product, which would 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 vulnerabilities that could turn into risks, which could impact CenterPoint Houston. Leveraging evaluation findings enables proactive measures to mitigate risk, enhancing robust systems, and ensuring continuity of operations. Overall, integrating evaluation processes into resilient strategies will empower CenterPoint Houston.

Supply Chain Risk Management ("ID.SC") *The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.*	
Analysis Results Description:	Identifying whether a vendor provides high-quality products and is reputable is an important part of resiliency. As part of the Backhaul Microwave Communication resiliency measure, CenterPoint Houston plans to assess the vendor before procuring its products or services. During interviews, CenterPoint Houston stated that they would evaluate or assess the product and the vendor prior to bringing it to production. This is a vital step to supply chain quality and security and adds an additional layer of resiliency to their overall system, as microwave technology plays an important role in data communication.

Access Control ("PR.AC") *Access to physical and logical assets and associated facilities is limited to authorized users, processes, or devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.*	
Analysis Results Description:	Controlling access to any system is an important part of protecting it from bad actors, reducing system downtime, and, therefore, improving resiliency. As part of the Backhaul Microwave resiliency measure, CenterPoint Houston intends to continue physically protecting the equipment necessary for functionality. All new equipment will be placed 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 by including 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 not only protect the system but also increase system capabilities to further improve resiliency.

Data Security ("PR.DS") *Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.*	
Analysis Results Description:	Securing the data that will flow through the microwave system and ensuring that it is available are important aspects of resiliency. As part of this resiliency measure, CenterPoint Houston plans to add a layer of protection while data is in transit, improving the redundancy channels with the equipment upgrades. The new microwave system will have the ability to encrypt data-in-transit via the IPsec protocol for encryption. By reducing the incompatible microwave technology that currently exists and replacing the older equipment, CenterPoint Houston will have the ability to leverage more current technologies. 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 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") *Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.*	
Analysis Results Description:	Security policies such as baseline configuration maintenance are rigorously upheld at CenterPoint Houston. Efforts are underway to establish and maintain baseline configurations as part of the backhaul microwave system's ongoing maturity process. CenterPoint Houston's efforts to enhance protection processes are under consideration, with plans to incorporate Internet Protocol Security ("IPsec") encryption into new equipment. IPsec encryption for backhaul microwave networks requires system compatibility to encrypt data packets and transmit them securely over wireless access points. 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") *Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.*	
Analysis Results Description:	Maintenance and repair function with established policies and procedures, which CenterPoint Houston can leverage to improve system availability and further enhance resiliency. During interviews, CenterPoint Houston stated it executes the maintenance and repair processes whenever issues arise. A predetermined program specifically dedicated to managing maintenance and repairs for radio links is in place, as is an approval process for maintenance and repair tasks.

Protective Technology ("PR.PT") *Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.*	
Analysis Results Description:	CenterPoint Houston has implemented capabilities that provide the extent of condition and validation, contributing to the overall health and effectiveness of the system that is leveraging the microwave system to transmit this type of data to the ADMS. It is important to address the resiliency risk associated with older microwave radios, which tend to fail more frequently and possess fewer capabilities. Implementing redundant systems for all substations mitigates the risk of communication loss or prolonged outages in case of failure, especially for older systems with limited capabilities. Integrating recloser devices with remote operation capabilities will impact CenterPoint Houston's ADMS. This integration has the potential to necessitate an increase in 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. 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 impact the ability to perform remote operations effectively. Enhancing redundancy is one of the key objectives of this resiliency measure, aligning with the extensive goal of improving system reliability and resilience.

Security Continuous Monitoring ("DE.CM") *The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.*	
Analysis Results Description:	CenterPoint Houston's information system and assets undergo continuous monitoring to detect cybersecurity events and validate the efficiency of protective measures. CenterPoint Houston's scrutiny extends to the physical environment, where security cameras are integrated with the backhaul microwave system, playing a crucial role in detecting potential cybersecurity threats. Access to the video feeds allows CenterPoint Houston personnel to respond to a potential threat. The Backhaul Microwave Communication resiliency measure will enhance video feeds by improving communication throughput and providing a redundant communication line that assists with ensuring critical security video feeds are available for surveillance.

5.9.7.7 Resiliency Measure Assessment and Conclusions

Guidehouse concludes that CenterPoint Houston's Backhaul Microwave Communication resiliency measure provides resiliency benefits. Primarily, the measure aims to reduce

communication loss and control for critical electrical systems. In addition, the goal of the backhaul microwave installation is to have a secondary method of communication available under system duress caused by extreme weather or cybersecurity events, helping reduce the risk of losing critical data and controls from remote locations as a primary form of communication. Redundancy is one of the primary methods for ensuring a resilient electric delivery service. System recovery will also improve as the microwave system's redundancy would allow for business continuity and a clear view of communications link failures.

5.9.8 Emergency Operations Center

5.9.8.1 Resiliency Measure Description

CenterPoint Houston's proposed Emergency Operations Center (EOC) is a $56 million dollar investment designed to create a centralized location that can be utilized during resiliency events. Staging site enhancements and building the new EOC will commence in 2025 and available for use in 2026. The EOC will serve as a safe location for employees for coordination, response, and recovery functions as CenterPoint Houston determines the best course of action for restoration activities. Staging sites that will be used as coordination locations for restoration during resiliency events, will be enhanced via identifying and evaluating preferred properties within CenterPoint Houston's service territory. During a resiliency event, these properties will then be reviewed for use as a staging site.

5.9.8.2 Revisions from the Prior System Resiliency Plan

None. This measure was not included in the prior SRP.

5.9.8.3 Resiliency Measure Targets

CenterPoint Houston's proposes to have the new Emergency Operations Center (EOC) operational by end-of-year 2026.

5.9.8.4 Alternatives Considered

The only alternative to the new EOC is to rely on current processes and staging sites. This option was rejected by CenterPoint Houston is the increasing number and severity of resiliency events supports the new EOC and enhanced staging site options associated with this measure.

5.9.8.5 Resiliency Measure Metrics and Effectiveness

Where CenterPoint Houston completes construction on the new Emergency Operations Center, CenterPoint Houston will track and report to the Commission annually on whether or not the structure is damaged during a resiliency event.

5.9.8.6 Benefits Analysis

The primary benefit of the new EOC is the assurance of a safe and secure central location for coordinating restoration activities and requisite staging sites to expedite outage restoration during resiliency events.

5.9.8.7 Resiliency Measure Assessment and Conclusions

Guidehouse concludes that CenterPoint Houston's EOC resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's SRP as it provides a safe and secure site for the coordination of restoration activities and suitable sites during resiliency events, each of which will expedite repair and restoration of service to its customers.

5.9.9 Hardened Service Centers

5.9.9.1 Resiliency Measure Description

CenterPoint Houston's Hardened Service Centers will be a $107.6 million dollar investment. These four new hardened service centers will be able to withstand extreme wind speeds up to 162 miles per hour. This exceeds the intensity of a Category 4 storm and surpasses the wind speed recorded during Hurricane Beryl (see Section 4.2.1.1). These hardened service centers have critical resources to support situational awareness events.

5.9.9.2 Revisions from the Prior System Resiliency Plan

None. This measure was not included in CEHE's prior 2024 SRP.

5.9.9.3 Resiliency Measure Targets

CenterPoint Houston proposes to have the four new hardened service centers available for use prior to end-of-year 2028.

5.9.9.4 Alternatives Considered

The only alternative to hardening existing service centers is to continue to use existing service centers. This option was rejected by CenterPoint Houston is the increasing severity of resiliency events and risk of severe damage (and potential safety of restoration personnel) supports the installation of new hardened service centers.

5.9.9.5 Resiliency Measure Metrics and Effectiveness

Where CenterPoint Houston completes construction on the new hardened service centers, CenterPoint Houston will track and report to the Commission annually on whether or not the structures are damaged during a resiliency event.

5.9.9.6 Benefits Analysis

The primary benefit of adding four new hardened service center is the assurance of a safe and secure service centers during resiliency events. Existing service centers were not designed to withstand the higher winds associated with projected extreme wind events, raising safety concerns and longer restoration of service to customers.

5.9.9.7 Resiliency Measure Assessment and Conclusions

Guidehouse concludes that CenterPoint Houston's Hardened Service Center resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's SRP as it provides a safe and secure service centers for CenterPoint Houston crews and support staff during resiliency events and will expedite repair and restoration of service to its customers.

6. Circuit-Level Analysis

To enhance the effectiveness of its 2026-2028 SRP, CenterPoint Houston has developed prioritized investments for certain measures based on locationally-specific analyses. These analyses vary by measure but generally target high fall-in-risk areas and circuits, sections, or substations with high system criticality. To provide recommendations and considerations for vulnerable grid locations, Guidehouse conducted complementary circuit-level analyses focusing on mid- to long-term climate forecasts and location criticality. CenterPoint Houston's detailed project prioritization analyses identify areas of present risk appropriate for inclusion in the 2026-2028 plan. Guidehouse's forward-looking model provides additional risk metrics for consideration during this period and may support CenterPoint Houston's prioritization considerations beyond the 2026-2028 plan.

Guidehouse's circuit-level analysis uses GIS data from CenterPoint Houston—which identifies the precise location of individual transmission and distribution system assets—and high-resolution climate forecast data from Jupiter Intelligence. The circuit-level analysis includes three components:

1. **Climate Vulnerability Assessment.** Analysis to identify areas of the transmission and distribution systems that are vulnerable to flood, wind, wildfire, and drought-induced salt contamination.

2. **Circuit-level Analysis of Measure Impacts.** Analysis of the expected CMI reduction impact of individual circuit-level resilience investments under a selected group of measures including Distribution Circuit Resiliency, Strategic Undergrounding, Distribution Pole Replacement, Substation Flood Control, Wildfire Mitigation, and Targeted Critical Circuit Vegetation Management. Guidehouse assessed circuit measure applicability separately for main line vs. lateral segments to target resilience investments more granularly.

3. **Implementation Plan Assessment.** Guidehouse compared the results of its circuit-level measure impacts analysis to CenterPoint Houston's implementation plans to develop recommendations for considering additional vulnerabilities. Guidehouse developed a spatial analysis for prioritizing Wildfire Mitigation and Vegetation Management using custom methods described in the sections below.

The following sections describe the methodology and results of each of these three components of the circuit-level analysis.

6.1 Vulnerability Assessment

Guidehouse assessed the vulnerability of transmission and distribution assets to climate-related disaster events including flood, extreme wind, wildfire, and salt contamination (which is associated with periods of relative drought). The flood, wind, and salt contamination analyses

focus on the vulnerability of transmission and distribution system assets to resiliency events. The wildfire analysis focuses on societal vulnerability, including potential impacts on people, buildings, and agriculture.

6.1.1 Data Inputs

Table 6-1 contains descriptions of the data that Guidehouse collected and used as inputs to the vulnerability assessment.

Table 6-1. Vulnerability Assessment Data Inputs

Data	Contents	Source
Transmission and Distribution Asset GIS Database	Asset-level characteristics, including: • Asset class (pole, tower, conductor, transformer, etc.) • Location (latitude/longitude) • Class-specific asset characteristics (*e.g.*, pole height and material, conductor voltage, etc.)	CenterPoint
Substation and Service Center Locations	A list of CenterPoint substations and service centers with location coordinates	CenterPoint
Locational Climate Risk	High spatial-resolution forecast of the probability of climate-related events under various climate scenarios. variables included: • Maximum annual flood depth by return interval (*e.g.*, 1/100-year) • Maximum annual sustained 1-minute wind speed by return interval (*e.g.*, 1/100-year) • Annual probability of catastrophic wildfire • Months per year where the rolling average Standardized Precipitation Evapotranspiration Index (SPEI) is below -2	Jupiter Intelligence
Circuit-level Vegetation Encroachment	• Circuit-level mileage by the degree of vegetation encroachment	CenterPoint (internal analysis of satellite imagery data)
Salt-contamination Risk Areas	• Spatial polygons identifying known areas of concern for salt contamination risk to transmission/distribution system assets	CenterPoint
FEMA National Risk Index Fire Exposure and Loss Ratio	Census tract-level data, including: • Historic loss ratio (HLR) for buildings, population, and agriculture due to wildfire • Exposure value of buildings, population, and agriculture to a potential wildfire	FEMA[119]

6.1.2 Approach

Guidehouse developed a grid subdividing CenterPoint Houston's service territory into approximately 3,300 hexagonal cells using the H3R7 hexagon methodology, commonly used in

[119] Map | National Risk Index

geospatial analysis. Jupiter Intelligence provided locational climate forecasts for each hexagonal cell's centroid and an additional set of coordinates for substation and service centers at 90 m^2 resolution to augment the vulnerability analysis for these critical assets. The climate forecast data included three common IPCC climate scenarios aligning with CMIP6: SSP1-RCP2.6, SSP2-RCP4.5, and SSP5-RCP8.5. These represent a range of potential future climate warming scenarios. The definitions of these IPCC scenarios are detailed in the Resiliency Risk analysis assumptions section of this report in Table 4-1.

Guidehouse chose SSP2-RCP4.5 for the circuit-level analysis as it represents a middle-of-the-road scenario with a slow decline in radiative forcing emissions.

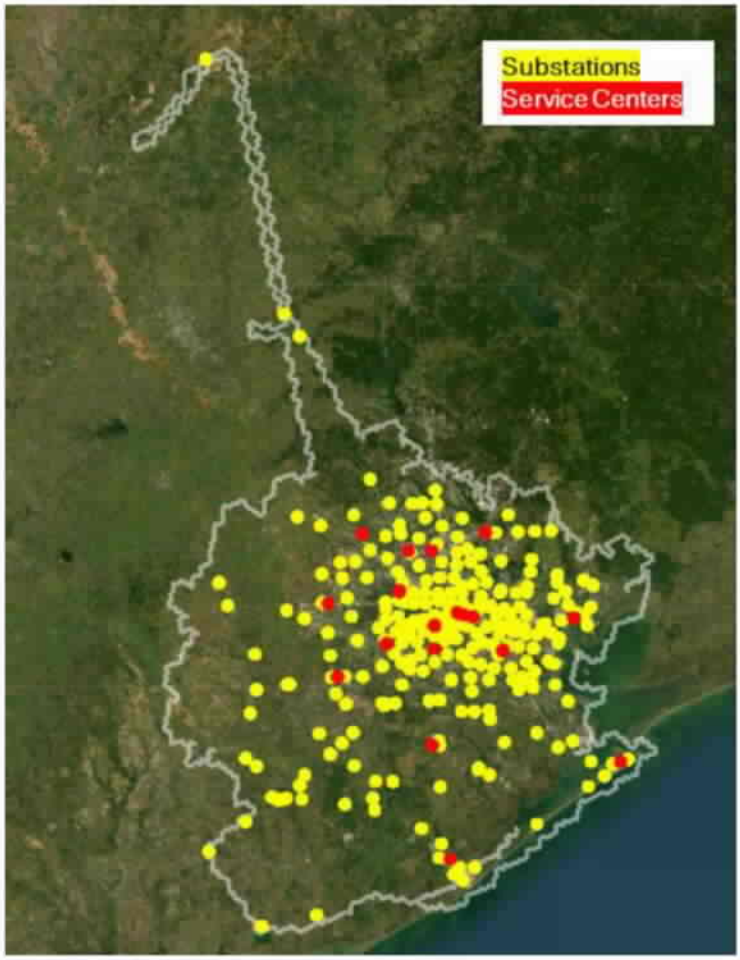
Guidehouse compared the Jupiter Intelligence climate forecast data to CenterPoint Houston's installed asset base to identify the locations and assets where exposure to climate-related hazards may increase the risk of outages. The climate vulnerability assessment does not incorporate the system criticality of feeders or substation equipment and, therefore, does not attempt to prioritize project locations within vulnerable areas. These factors, including the expected number of customers impacted and outage durations from weather-related causes, are introduced in Section 6.2.

The following sections describe the findings of the climate vulnerability assessment for flood, extreme wind, wildfire, and drought-induced salt contamination events. Throughout the vulnerability assessment, results are provided at the 1/100-year return interval (*i.e.*, the severity of a 1 in 100-year event with a 1% annual probability of occurrence). As utility transmission and distribution assets are generally expected to survive between 25-75 years in the field—depending on the asset class—the 1/100 return interval provides an event severity that is expected to be experienced by an asset within its lifetime at rates of 25-75% and is therefore useful for a higher-level assessment.

6.1.3 Flood

The vulnerability assessment for flood events focused on substations and service centers in CenterPoint Houston's service territory including transmission corridor areas to the north and southwest of the main service area. CenterPoint Houston's territory and transmission corridors contain 20 service centers and 267 substations. Of these, 2 service centers and 18 substations are in coastal areas with most substations concentrated in the central Houston area. Figure 6-1 shows the locations of substations and service centers within the boundary of the service territory, including transmission corridors.

Figure 6-1. Service Territory, Substations, and Service Centers



As flood probabilities are highly spatially dependent (relative to other perils such as wind), Guidehouse examined the flood peril for substations and service centers using risk estimates for the exact coordinates of each asset at 90 m^2 resolution, rather than using a hexagon centroid.

Figure 6-2 shows the annual maximum 1/100-year flood depth for substations and service centers. Flood depths will increase slightly from 2025 to 2050. However, few sites are forecasted to experience significant change between the depicted flood depth binned ranges over time. Sites with high flood depths (> 6 ft) at the 1/100-year return interval are concentrated in coastal areas or near the mouth of the San Jacinto River in Galveston Bay.

Figure 6-2. Average Flood Depth for Substations and Service Centers (1/100-year return interval)

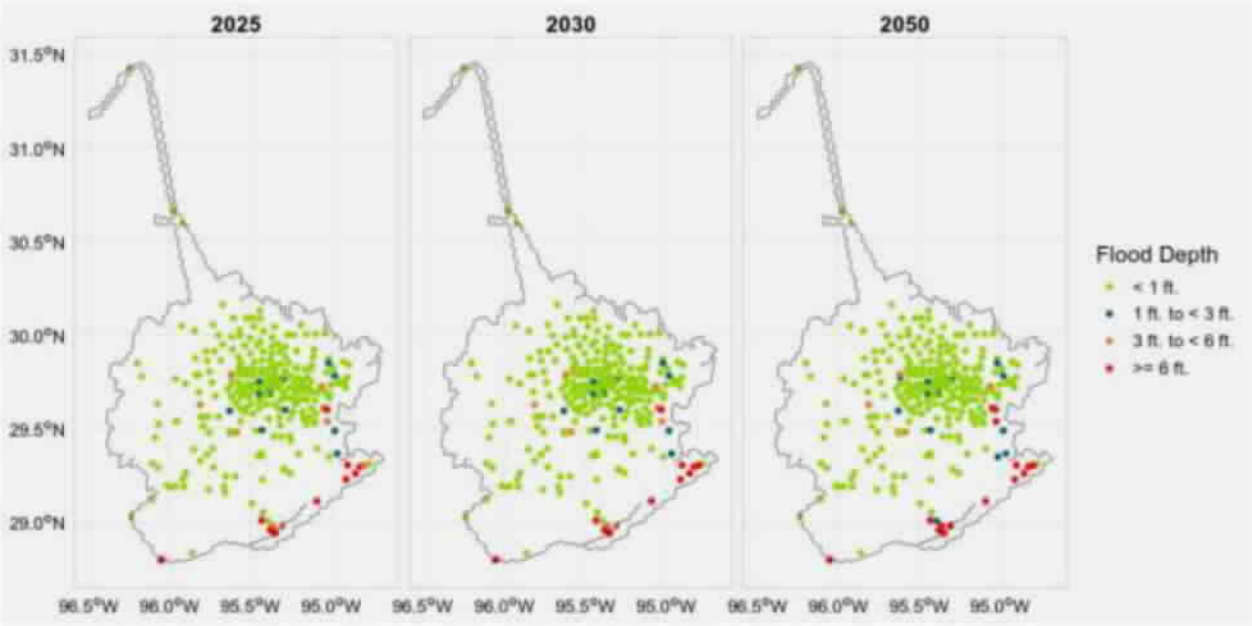


Table 6-2 contains the count of substations and service centers by flood depth bin. In 2050, 8% of sites are at risk of flooding with 3 or more feet of water.

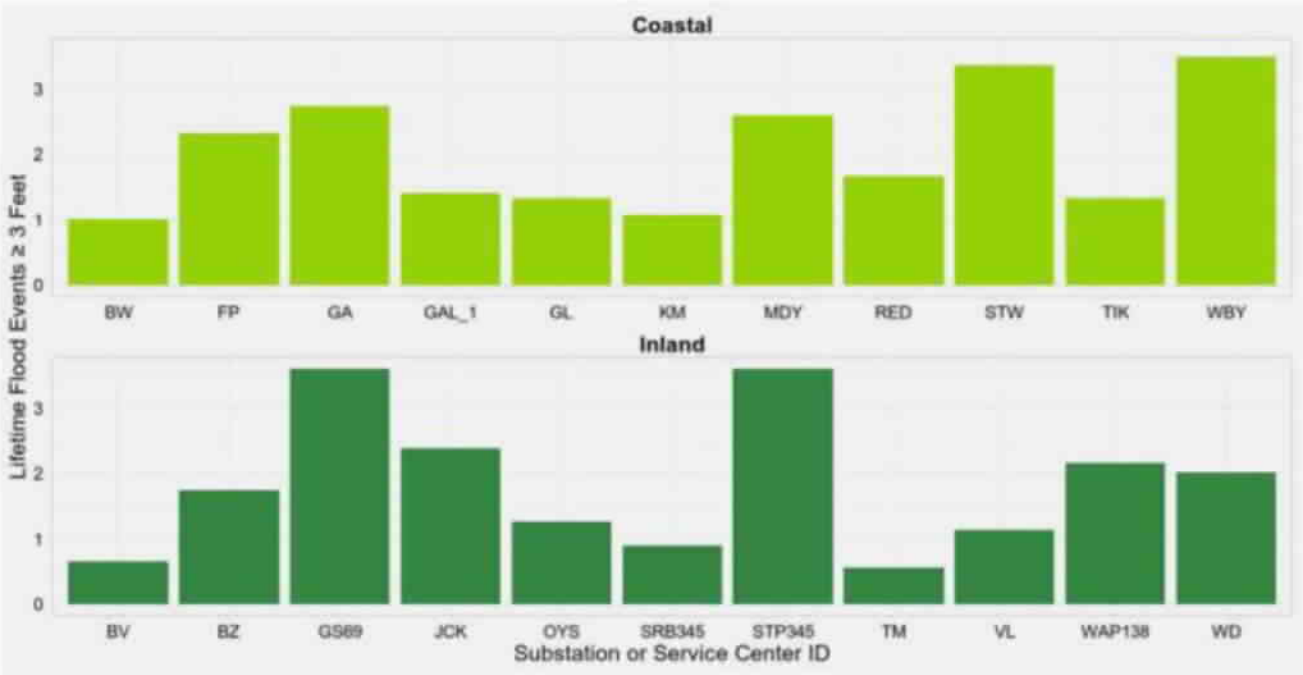
Table 6-2. Number of Substations and Service Centers by Flood Depth, (1/100-year return interval)

Location	Total Substations and Service Centers	Flood Depth	2025	2030	2050
Coastal	22	< 1 ft.	10	10	10
		1 ft. to < 3 ft.	1	1	1
		3 ft. to < 6 ft.	4	3	0
		>= 6 ft.	7	8	11
Inland	267	< 1 ft.	244	244	242
		1 ft. to < 3 ft.	10	10	12
		3 ft. to < 6 ft.	7	7	5
		>= 6 ft.	4	4	6

Guidehouse estimated the expected number of flood events for substations and service centers with ≥ 3-foot flood risk (SSP2-4.5) across the lifetime of each asset. The probability of a max flood depth of 3 feet or above was estimated from 2025 through the lifetime of the asset using the maximum flood depths at each return interval and year. The sum of the probabilities across

an asset's lifetime is the number of events it is expected to experience, shown in Figure 6-3. Guidehouse assumed a lifetime of 45 years based on EUL data provided by CenterPoint Houston. The expected frequency of flood events over ≥ 3 feet is similar for inland and coastal substations, with an average frequency of 2 events for coastal assets and 1.8 events for inland assets. Two coastal assets and two inland assets are expected to experience at least 3 flood events of 3+ feet during their lifetimes.

Figure 6-3. Expected Lifetime Flood Events ≥ 3 Feet for Substations and Service Centers with >3-foot flood risk, SSP2-4.5



6.1.4 Wind

Guidehouse assessed the probability of extreme wind events impacting transmission and distribution poles and overhead lines, which may require repair or replacement after experiencing sustained wind speeds exceeding a threshold of 70 mph (depending on asset material, tree encroachment, and condition). The wind is less spatially dependent than a flood. Therefore, Guidehouse assigned all assets within a hexagon to the risk associated with its hexagon's centroid.

Figure 6-4 shows the expected maximum 1/100-year wind speed for each hexagon. Houston experiences relatively high winds compared to typical asset failure thresholds, with average maximum 1/100-year wind speeds projected to increase slightly from 93 mph in 2020 to 94.7 mph in 2100. All hexagons within the CenterPoint Houston service territory are expected to experience maximum sustained 1-minute wind speeds of 70 mph or greater from 2020 through 2100 at the 1/100-year return interval.

Figure 6-4. Maximum Sustained 1-minute Wind Speed by Hexagon (1/100-year return interval, SSP2-4.5)[120]

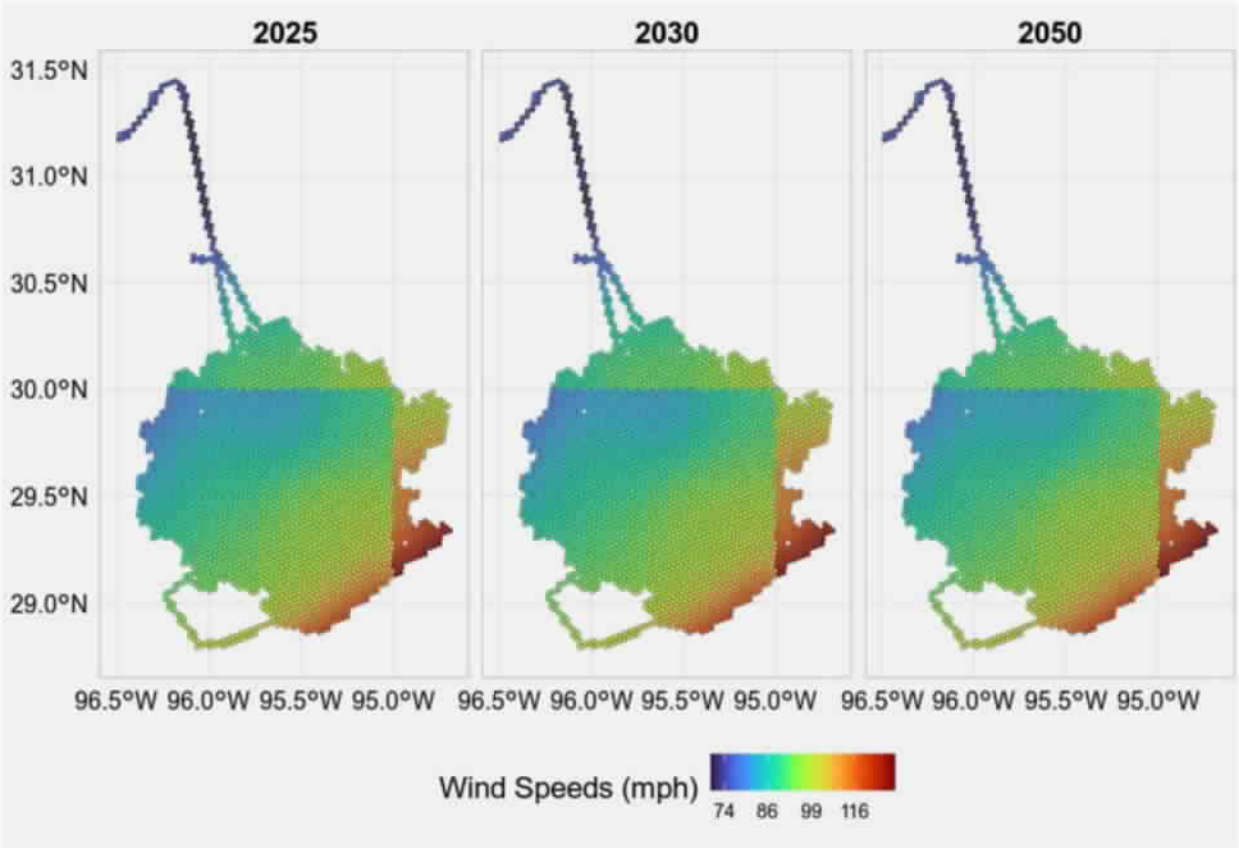


Table 6-3 contains counts of assets by expected 1-in-100-year wind speed. Approximately one-quarter of coastal poles and overhead lines are predicted to experience wind speeds greater than 120 mph, with a maximum wind speed of 131 mph. Inland hexagons experience lower wind speeds on average, with close to half of assets expected to experience 1-in-100-year maximum sustained wind speeds between 70 and 90 mph and half between 90 and 120 mph.

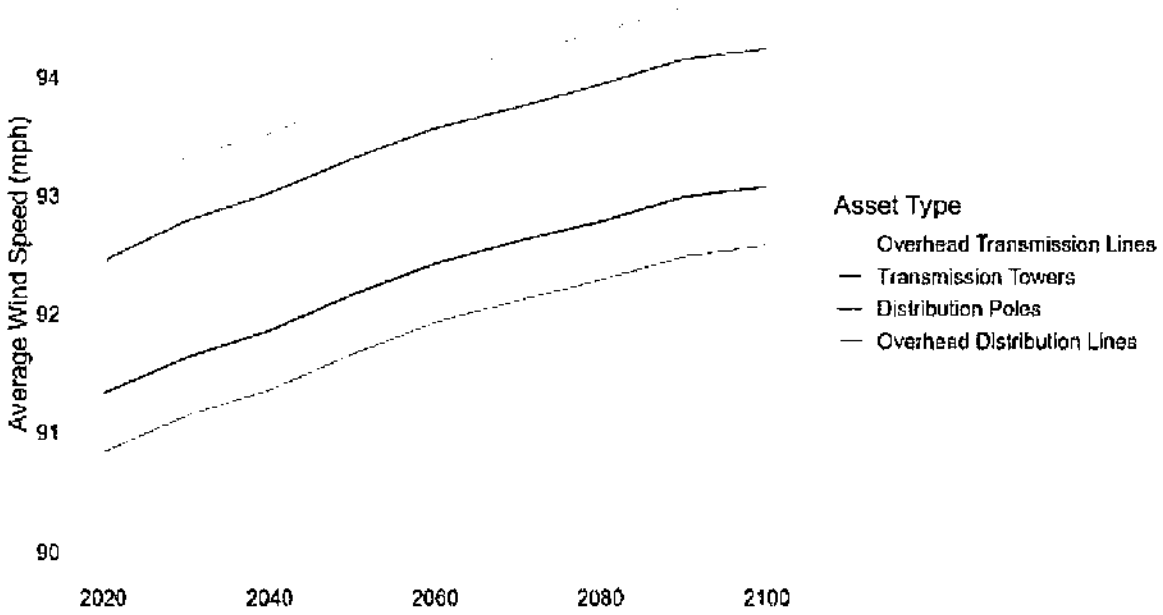
[120] The shift in color gradient at 95.0° W and 30.0° N are an outcome of the statistical downscaling methodology applied by Jupiter Intelligence.

Table 6-3. Number of Poles and Overhead Lines by Maximum Sustained Wind Speed (1/100-year return interval, SSP2-4.5)

Location	Total Assets	Wind Speed	2025	2030	2050
Coastal	126,920	70 mph – 90 mph	0	0	0
		90 mph – 120 mph	93,908	93,908	93,491
		120+ mph	33,012	33,012	33,429
Inland	1,977,830	70 mph – 90 mph	1,049,034	1,008,977	919,673
		90 mph – 120 mph	928,796	968,853	1,058,157
		120+ mph	0	0	0

Guidehouse also estimated max sustained wind speed probabilities by asset class. This was calculated using average probability across hexagons, weighted based on the number of assets in each hexagon. Figure 6-5 shows the weighted average maximum sustained wind speeds by asset class from 2020 to 2100. Transmission lines and towers are subject to slightly higher predicted wind speeds than other asset types. For all asset classes, wind speed forecasts trend upward over time, increasing by approximately 1.5 mph from 2020 to 2100.

Figure 6-5. Weighted Average Max Sustained Wind Speed by Asset Class, 2020 - 2100 (1/100-year return interval, SSP2-4.5)



Vegetation encroachment is an additional factor that contributes to the probability of damage to utility assets and service interruptions during extreme wind events. To incorporate vegetation encroachment into the vulnerability assessment, Guidehouse estimated hexagon-level vegetation encroachment percentages using circuit-level vegetation and asset data. For each hexagon, Guidehouse calculated the weighted average of the per circuit percent of mileage at the 0-15 ft vegetation encroachment level, weighting based on the number of assets per circuit within a given hexagon. Figure 6-6 shows a heatmap of the resulting vegetation encroachment estimates by hexagon, with high encroachment areas in red and low encroachment in blue. Areas along the coast are predicted to experience the most severe sustained wind speed but have relatively low levels of vegetation encroachment.

Figure 6-6. Vegetation Encroachment Concentration by Hexagon

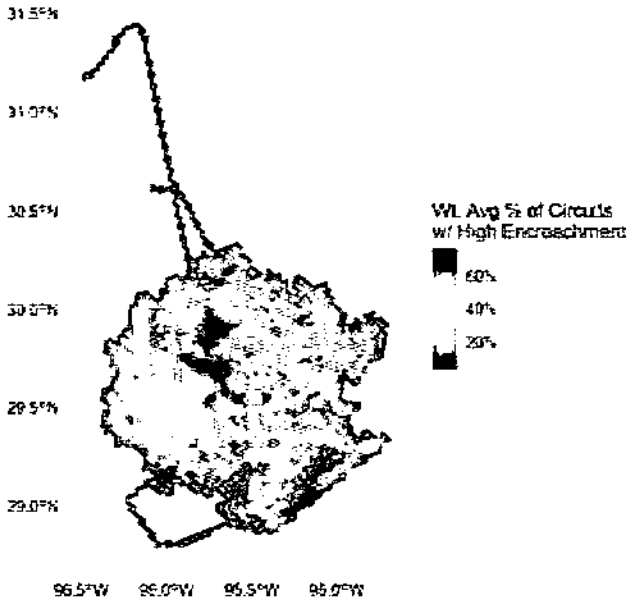
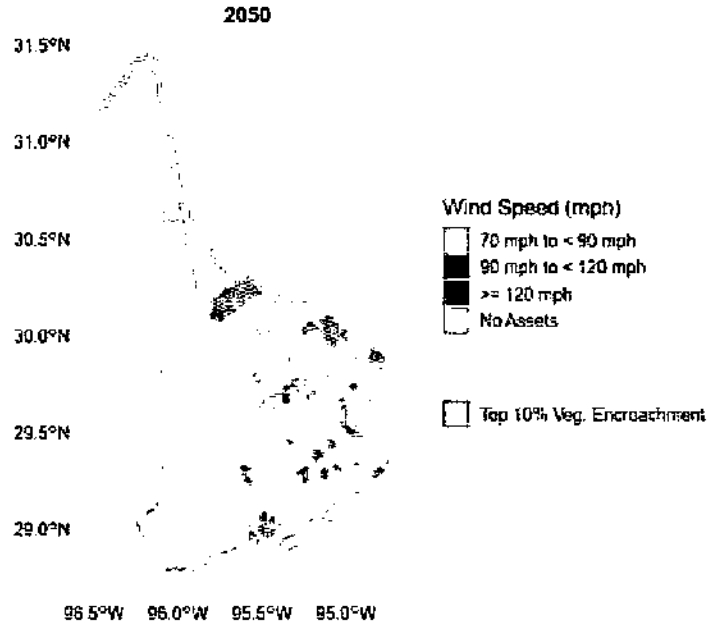


Figure 6-7 shows an overlay of hexagon-level wind speed with areas within the top 10% of vegetation encroachment (outlined in blue). Hexagons in the area just south of the northern transmission corridor have both high vegetation levels and high predicted wind speeds (90+ mph), along with several clusters of hexagons parallel to the coast. Assets within these hexagons may be subject to damage or failure at lower wind speeds than assets in areas with lower vegetation encroachment due to fall-in risk.

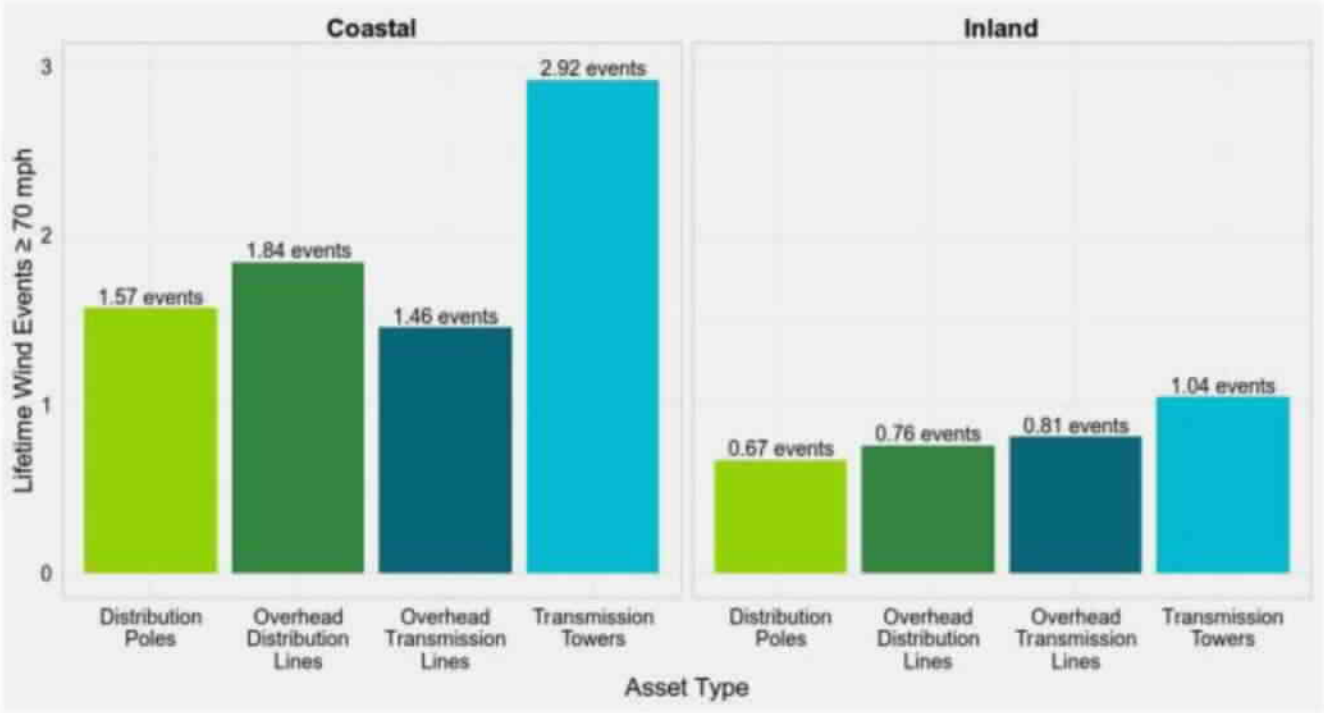
Figure 6-7. Average Maximum Sustained Wind Speed by Hexagon in 2050 and Top 10% of Hexagons by Vegetation Encroachment (1/100-year return interval, SSP2-4.5)



Guidehouse estimated the average expected number of wind events by asset class ≥ 70 mph across the lifetime of each asset type, shown in Figure 6-8. The probability of a max wind speed of 70 mph or above was estimated from 2025 through the lifetime of the asset using the maximum wind speeds at each return interval and year. The sum of the probabilities across an asset's lifetime is the number of events it is expected to experience. Coastal assets are more likely to experience winds over 70 mph, with an average of 1 – 3 events per asset lifetime. Transmission towers are expected to experience the most wind events.

Inland assets are expected to experience one or fewer wind events over 70 mph during their lifetimes. However, the expected event frequencies vary for each individual hexagon area. The expected number of wind events is lower near central Houston and generally increases with proximity to the coastal area.

Figure 6-8.Expected Lifetime Wind Events ≥ 70 mph by Region and Asset Type, SSP2-4.5



6.1.5 Wildfire

Wildfires are distinct from the other hazards included in the vulnerability assessment. Unlike wind, flood, or drought, utility assets can contribute to the ignition of wildfire events. Therefore, the wildfire vulnerability analysis focuses on potential societal impacts beyond utility assets. Societal impacts include loss of population, buildings, and agriculture as defined by the FEMA National Risk Index[121].

To assess societal impacts, Guidehouse collected FEMA data including the value of population, buildings, and agriculture in each census tract that intersects CenterPoint Houston's service territory. Guidehouse also collected FEMA data on the historic loss ratio (HLR) of each of the societal risk categories, conditional on the occurrence of a significant local fire event.

Guidehouse paired the FEMA exposure and HLR data with estimates of wildfire provided by Jupiter Intelligence to identify areas of CenterPoint Houston's service territory with higher vulnerability to wildfire events. Specifically, Guidehouse used data on wildfire exposure and loss ratios that interacted with the Jupiter wildfire data at the hexagon level, as shown in Equation 1.

[121] Map | National Risk Index

Equation 1. Expected Annual Losses[122]

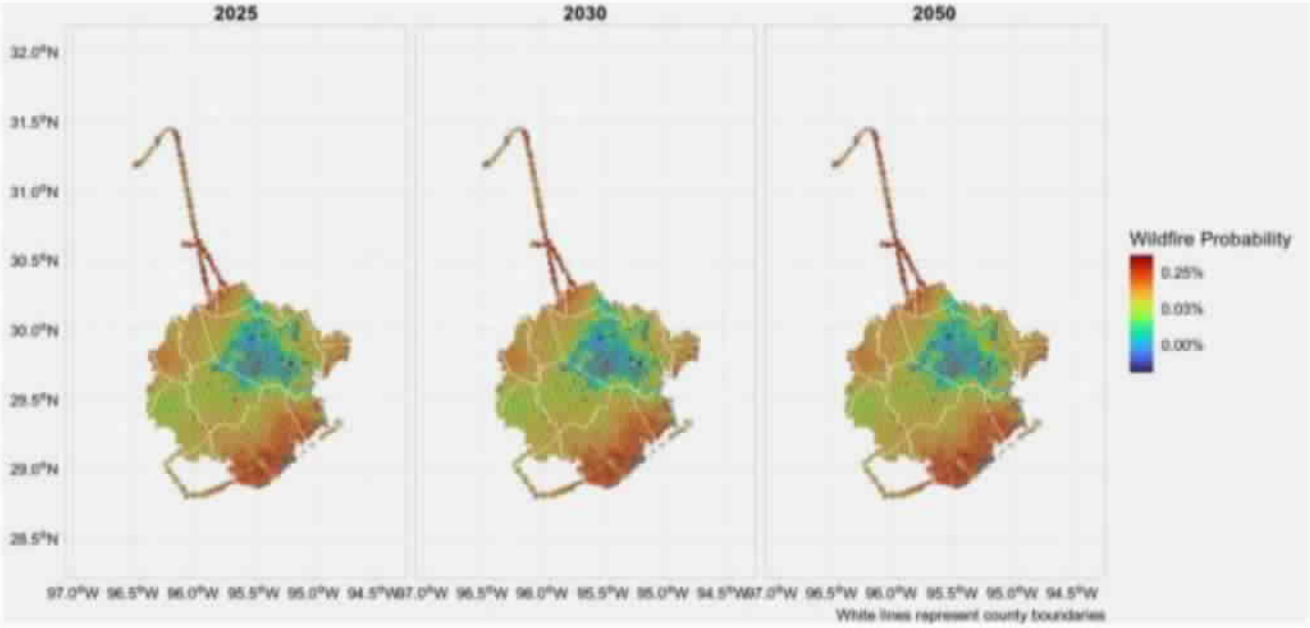
$$EAL_{h,y} = WildfireProb_{h,y} * \sum_{t=1}^{T=3} Exposure_{h,t} * LossRatio_{h,t}$$

Where:

- $EAL_{h,y}$ = Expected annual loss estimate for hexagon *h* in year *y* (in dollars).
- $WildfireProb_{h,y}$ = Jupiter annual wildfire probability for hexagon *h* in year *y* under SSP2-4.5.
- $Exposure_{h,t}$ = Sum of FEMA estimated wildfire exposure for hexagon h and consequence type t (buildings, population, or agriculture). Includes exposure for all census tracts overlapping with hexagon h, scaled based on the percent of each census tract in hexagon h.
- $LossRatio_{h,t}$ = Weighted average f FEMA estimated wildfire loss ratio for hexagon h and consequence type t (buildings, population, or agriculture). Weighted based on the exposure for consequence t in hexagon h.

Figure 6-9 shows the Jupiter annual wildfire probability for each hexagon in 2025, 2030, and 2050. The annual probability of catastrophic wildfires is low across the service territory, with a maximum value of 0.47% in hexagons with any assets and an average value of 0.06%. Wildfire probability is lowest in central Houston and higher in areas near urban wildlife boundaries.

Figure 6-9. Annual Wildfire Probability



[122] Based on the **FEMA Census block to wildfire equation**.

Figure Figure 6-10 shows the resulting total expected annual loss (EAL) from wildfire by hexagon in 2025, 2030, and 2050. EALs are low throughout most of the service territory due to relatively low annual probabilities of wildfire occurrence, in combination with low historical loss ratios for consequence types with high exposure. However, there are areas with heightened potential for wildfire loss in the wildland-urban interface around the perimeter of the Houston metropolitan area as well as near Lake Jackson and Katy. Across the service territory, total EAL increases from $6.71 million in 2025 to $7.31 million in 2050.

Figure 6-10. Total Expected Annual Loss

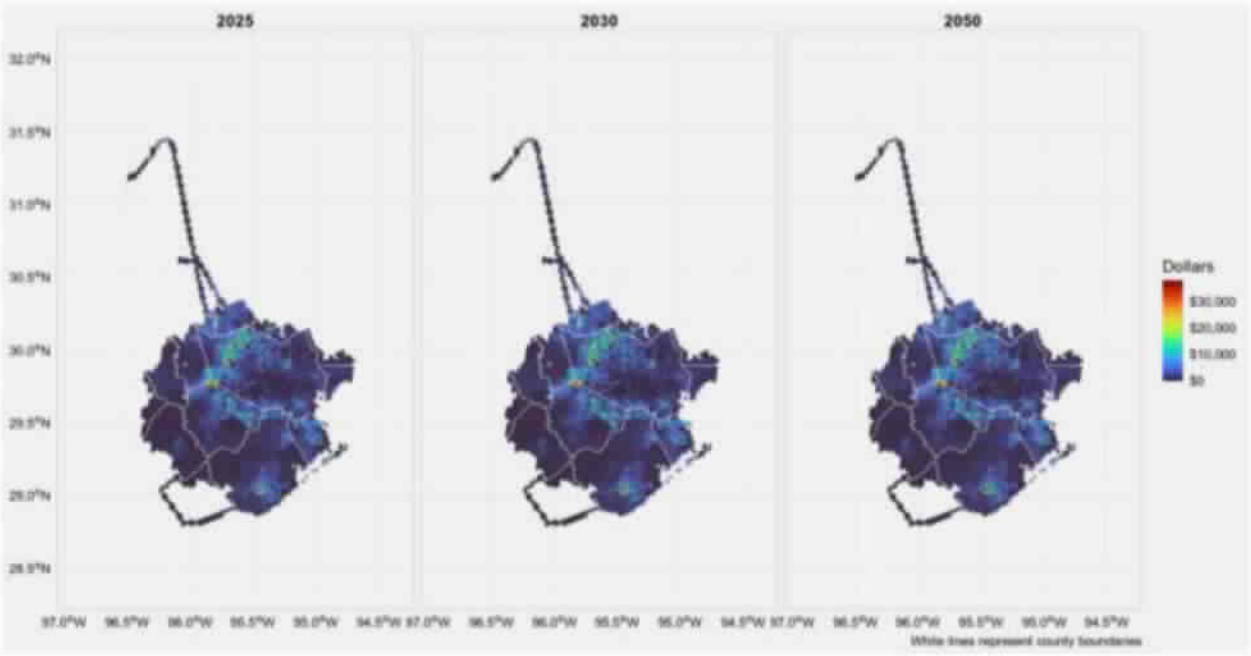
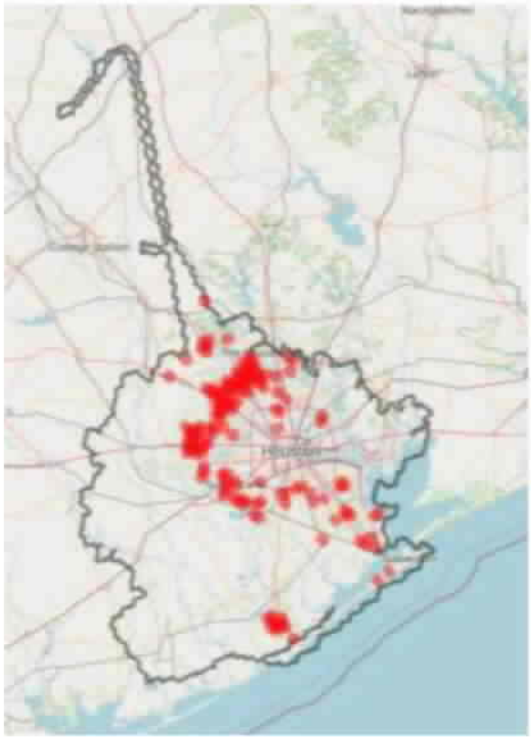


Figure 6-11 shows the areas with the greatest wildfire vulnerability based on hexagon level EAL in 2050. Only hexagons in the top 5% of EAL are illustrated, with EAL values for these hexagons ranging from $8,235 to $38,144. In comparison, EAL for the bottom 95% of hexagons averages $1,722.

Figure 6-11. Areas with Highest Wildfire Vulnerability (top 5%)



6.1.6 Drought

Salt contamination on utility assets, including overhead lines and substation insulators susceptible to flashover events under this condition, is associated with periods of relative drought. Therefore, drought was used as a proxy for salt contamination vulnerability with a focus on the probability of drought events at substation locations. Jupiter Intelligence provides several drought metrics, including mean months per year where the rolling 3-month average Standardized Precipitation and Evapotranspiration Index (SPEI) is below -2. Guidehouse converted this value to mean days per year from months. The SPEI captures temperature and precipitation, with values above zero indicating above-normal (wetter) periods and below zero representing below-normal (dry) periods. The SPEI is approximately equal to the number of standard deviations the precipitation evapotranspiration amount differs from the mean, with an SPEI below -2 commonly used to reflect severe drought periods[123].

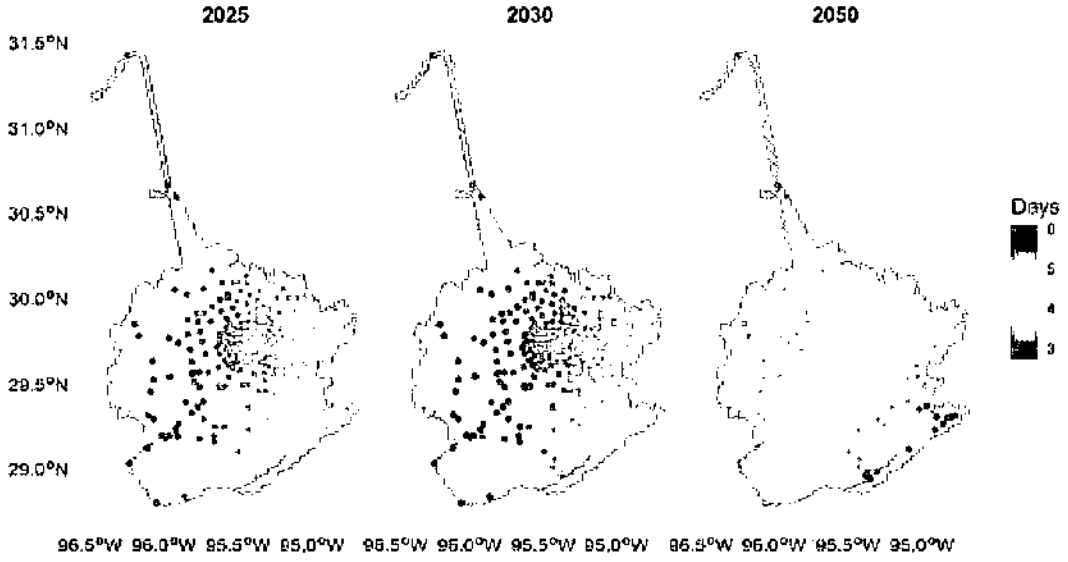
Drought is less spatially dependent than flooding, so all assets within a hexagon are assigned the risk associated with their hexagon's centroid. However, for substations, location-specific granularity at 90 m^2 was used.

Figure 6-12 shows the number of days with a rolling 3-month average SPEI less than -2 by substation. Houston has a humid subtropical climate and typically experiences a significant

[123] Paulo, A. A., Rosa, R. D., and Pereira, L. S.: Climate trends and behaviour of drought indices based on precipitation and evapotranspiration in Portugal, Nat. Hazards Earth Syst. Sci., 12, 1481–1491, https://doi.org/10.5194/nhess-12-1481-2012, 2012.

amount of annual rainfall, averaging over 50 inches[124]. However, climate forecasts indicate that dry periods are expected to become more frequent over time, with the number of days with a rolling 3-month average SPEI below -2 increasing from 3.61 in 2020 to 4.58 in 2050. Stations near the coast are expected to experience the greatest exposure to these events. Compared to other climate hazards, the upward trend is less linear, with drought decreasing slightly in some decades.[125]

Figure 6-12. Number of Days with Rolling 3-month Average SPEI Below -2 (SSP2-4.5)



Guidehouse used data provided by CenterPoint Houston to identify areas exposed to high risk of corrosion, most of which fall on the eastern side of the service territory and along the coast. Figure 6-13 shows these corrosive areas by type. Of 267 substations, 69 (26%) fall within a corrosive area, indicating an increased risk of failure during drought conditions. Assets within the freshwater corrosive area have a lower drought risk than those in other areas.

[124] **https://www.weather.gov/hgx/climate_iah_normals_summary**

[125] Year-over-year variation in the drought forecast is negatively correlated with the variation in the Jupiter precipitation forecast.