

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 the purpose of this report, Guidehouse is only reporting on features, applications, or business processes with a high or, in some instances, medium correlation to subcategories of the NIST CSF.

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

CenterPoint Houston also plans to use the following performance metrics for tracking the effectiveness of the Network Security and 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 on a daily basis,
- 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

Q. WHAT BENEFITS WILL BE REALIZED FROM CENTERPOINT HOUSTON'S NETWORK SECURITY & VULNERABILITY MANAGEMENT RESILIENCY MEASURE?

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

The Guidehouse analysis identified the following areas where the CSF functions, categories, and associated subcategories have a high and medium correlation to the Network Security and Vulnerability Management Resiliency measure's functions and security practices:

- **Asset Management (ID.AM):** Guidehouse determined CenterPoint Houston is upgrading and refreshing technology that needs to be updated. The Network Security and Vulnerability Management resiliency measure helps ensure CenterPoint Houston has network and security tools that meet industry standards and best practices to achieve resiliency of the services it provides. CenterPoint Houston listed the hardware and software it will upgrade and refresh with a priority

in criticality and business need. End-of-life network devices are being prioritized for replacement as part of this resiliency measure. Having the latest network hardware available will ensure the network is updated and has the latest security features installed to ensure a robust and resilient network

- **Business Environment (ID.BE):** Guidehouse determined CenterPoint Houston plans to improve resilience by upgrading its ability to failover or switch from its primary and/or backup control center. Additionally, CenterPoint Houston will include a GRC tool that will ensure a strong process flow is in place for critical steps towards security and resiliency activities.
- **Governance (ID.GV):** Guidehouse determined CenterPoint Houston will implement a GRC tool and migrate from a manual process to an automated solution. This provides a simpler method for approval and revising 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 practice will improve upper management's view on actions that need to be approved to move forward with risks.
- **Risk Assessment (ID.RA):** Guidehouse determined CenterPoint Houston will improve the mitigation of potential risks by refreshing its Vulnerability Assessment tool and scanning individual machines periodically to assess potential security risks. The refresh will ensure CenterPoint Houston has the latest version and threat intelligence libraries for assessing against any potential security gaps to develop appropriate mitigation plans.

- **Supply Chain Risk Management (ID.SC):** Guidehouse determined CenterPoint Houston plans to engage a resident Palo Alto representative to assist with the implementation of its network refresh for Palo Alto network devices. Additionally, a team of Palo Alto engineers can assist around the clock for any issues with implementation and ongoing maintenance or issues. Having these third-party service providers supporting through implementation improves CenterPoint Houston's ability to ensure its network is fully functioning and resilient.
- **Anomalies and Events (DE.AE):** Guidehouse determined CenterPoint Houston will implement security measures that detect potential security gaps in its network and associated systems. CenterPoint Houston stated it has architecture diagrams that allow it to be aware of the data flows of communication in its network, which is a good practice for detecting anomalous activity.
- **Security Continuous Monitoring (DE.CM):** Guidehouse determined CenterPoint Houston will implement malicious communication detection as part of the network equipment to be refreshed during this resiliency measure to monitor the network for unwanted communication. CenterPoint Houston will also monitor for gaps or vulnerabilities within the system using a refreshed vulnerability scanner, such as the current Rapid 7 or replacement scanning platform.
- **Detection Processes (DE.DP):** Guidehouse determined CenterPoint Houston will refresh the systems that assist with threat detections in its network and on system endpoints. CenterPoint Houston will improve its detection efficiency by replacing its current QRadar system with a 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 to provide balanced detection processes across its network attack surface.

- **Access Control (PR.AC):** Guidehouse determined CenterPoint Houston has access control for remote users and protects its systems by limiting the users who can access its system remotely. CenterPoint Houston is including an update on hardware for Cyber Ark which is used as a vault for passwords and also plans to further limit remote access to the system to only a privileged team that requires monitored requests and access approvals prior to access provisioning. This process includes the vulnerability servers and network security appliances as part of the resiliency measure. In addition, CenterPoint Houston has physical protections in place to further prevent unauthorized access to critical cyber systems, further improving its resiliency posture.
- **Awareness and Training (PR.AT):** Guidehouse determined CenterPoint Houston will include awareness and training for the GRC tool for 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):** Guidehouse determined CenterPoint Houston will implement several data protection controls to ensure the security of new hardware and software. CenterPoint Houston will implement encryption and secure communication protocols such as Hypertext Transfer Protocol Secure (“HTTPS”). For some hardware, CenterPoint Houston will forward network log information to a log aggregator. This information will be sent using encryption methods. For data that resides within the hardware itself, CenterPoint Houston plans to destroy hard

drives rather than send them back to the manufacturer to prevent retrieval of critical data.

- **Information Protection Processes and Procedures (PR.IP):** Guidehouse determined CenterPoint Houston will include information protection techniques such as hard drive shredding in this resiliency measure. CenterPoint Houston plans to mature its information protection methodologies and 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):** Guidehouse determined CenterPoint Houston will upgrade its network equipment with the latest firewalls, routers, and switches to protect its communication and control networks. CenterPoint Houston will include system redundancy to ensure high availability on the network and will 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.

Q. PLEASE PROVIDE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S PROPOSED NETWORK SECURITY & VULNERABILITY MANAGEMENT RESILIENCY MEASURE.

A. Guidehouse concludes there is robust linkage between resiliency and CenterPoint Houston's Network Security and Vulnerability Management resiliency measure, based on the high levels of correlation the resiliency measure has in relation to NIST CSF Functions and Categories.

- I concur CenterPoint Houston's Network Security & Vulnerability Management resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's Resiliency Plan. This resiliency measure supports a strong and resilient electric transmission and distribution system in key NIST CSF categories, including:
 - Access Control – Managing and controlling who can access critical systems is vital for a more secure and resilient system.
 - Data Security – Protecting an organization's data is key to maintaining integrity of data and confidentiality.
 - Detection Processes – Detecting system anomalies helps ensure awareness of cybersecurity events and prepare for quick remediation or mitigation actions.
 - Governance – Implementing an automated solution will improve managing NIST CSF alignment and regulatory compliance efforts.
 - Information Protection Processes and Procedures – Information protection techniques are necessary to maintain confidentiality and secure critical information.
 - Protective Technology – Protecting assets using security solutions that ensure networks are protected and are available can ensure a functional and resilient communication infrastructure.

- Risk Assessment – Implementing a tool that will scan for vulnerabilities will improve the view of potential weaknesses or gaps in a system, further reducing risk of impact to the system.
- Security Continuous Monitoring – As part of its ongoing system security resiliency measure, CenterPoint Houston will integrate monitoring features from the refreshed hardware and software to expand monitoring of the system’s network, users, and vulnerabilities.
- I concur CenterPoint Houston’s Network Security and Vulnerability Management resiliency measure supports grid resiliency by ensuring the stability and integrity of its infrastructure. Integrating continuous monitoring and proactive risk management controls, CenterPoint Houston will fortify its defenses to protect against potential cyber threats, thereby minimizing the risk of cyber-related disruptions to critical grid operations.
- The proposed Network Security and Vulnerability Management resiliency measure is consistent with resiliency practices deployed at other utilities, based on Guidehouse experience and peer utility benchmarking survey results described in Section VI.

Q. PLEASE DESCRIBE CENTERPOINT HOUSTON’S IT/OT-CYBERSECURITY MONITORING RESILIENCY MEASURE.

A. The IT/OT-Cybersecurity Monitoring Resiliency Measure is a comprehensive resiliency measure that will include deployment of advanced firewalls, passive network sensors and other cyber technologies to over 400 sites. CenterPoint Houston is proposing to build 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 was not previously available. It shows network traffic detection, OT asset visibility and provide 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).²⁹ The resiliency measure will fill gaps in segmentation, monitoring and OT asset management.

CenterPoint will implement Splunk as their logging system as well as for KPI visibility 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 to identify anomalous activity that could lead to a cybersecurity incident. As part of the resiliency measure, CenterPoint Houston will include 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.

IT/OT – Cybersecurity Monitoring 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, and

²⁹ NIST. (2023 September). NIST SP 800-82r3: Guide to Operational Technology (OT) Security. <https://doi.org/10.6028/NIST.SP.800-82r3.ipd>

- Tentative schedule - begins in 2024, continues into 2025, and completed by end of 2025.

Q. WHAT ALTERNATIVES WERE CONSIDERED IN CENTERPOINT HOUSTON'S EVALUATION OF IT/OT-CYBERSECURITY MONITORING REQUIREMENTS?

A. Other technology platforms were considered and evaluated by CenterPoint Houston via an objective process that aligned business requirements, company and product features, and included other important factors such as fiscal and support considerations. The Guidehouse analysis team determined the proposed IT/OT – Cybersecurity Monitoring resiliency measure is directly related to monitoring for cybersecurity breaches and addresses other cybersecurity threats and vulnerabilities, therefore did not evaluate other methods.

Q. WHAT METRICS DOES CENTERPOINT HOUSTON PROPOSE TO MEASURE AND TRACK THE EFFECTIVENESS OF THE IT/OT-CYBERSECURITY MONITORING?

A. 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 plays a crucial role 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.

Guidehouse evaluated the benefits and features associated with CenterPoint Houston's proposed IT/OT-Cybersecurity Monitoring on a qualitative basis with resiliency measure-specific inputs and assumptions. This analysis compared CenterPoint Houston's resiliency measure with the NIST CSF to identify levels of correlation between the five CSF Functions (Identify, Detect, Protect, Respond, and Recover), and the proposed system in terms of developing resilient systems. Guidehouse performed the analysis and identified whether the resiliency measure had high, medium, or low correlations to the individual subcategories of the CSF. For 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 that were mapping to low correlation were considered to be relatively ineffective in improving resiliency, although depending on the context of the proposed resiliency measure, they may still have value in pursuing from reliability or policy perspectives. CenterPoint Houston also plans to use the following performance metrics for tracking the effectiveness of the 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.

Q. WHAT BENEFITS WILL BE REALIZED FROM CENTERPOINT HOUSTON'S IT/OT-CYBERSECURITY MONITORING?

A. Guidehouse evaluated the benefits associated with CenterPoint Houston's proposed IT/OT Cybersecurity Monitoring resiliency measure on a qualitative basis. The Guidehouse analysis indicates that the resiliency measure will provide a high level of effectiveness for detection of threats to the system because of the monitoring, alerting, and additional functionality performed by the Splunk and Nozomi systems. Based on the results of a comparative analysis, Guidehouse determined that the resiliency measure offers resiliency benefits. All determinations below are based on CenterPoint Houston information on resiliency measure descriptions, interviews, and responses to data requests for additional details.

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

- **Risk Assessment (ID.RA):** Guidehouse determined CenterPoint 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 how to respond to potential threats. The monitoring system will inherently document the identified threats for processing. Identifying these threats and vulnerabilities will provide CenterPoint 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”) critical information necessary 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):** Guidehouse determined CenterPoint Houston will ensure all cyber-related assets and their software/applications will be inventoried. The inventory will be maintained on an annual basis to ensure accuracy. The inventory practice ensures that all cyber systems and associated software is identified and tracked for monitoring. The data flows from each cyber system will be included as part of the monitoring resiliency 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):** Guidehouse determined CenterPoint Houston’s proposed cybersecurity monitoring system will 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. The

machine learning would also constantly update the threshold for incident alerts and escalation. CenterPoint Houston will be deploying Nozomi, which will analyze and catalog attack data and allow for impact evaluation for potential attacks. The paired Splunk and Nozomi cyber systems will allow CenterPoint Houston to better detect and evaluate the potential impacts of events.

- **Security Continuous Monitoring (DE.CM):** Guidehouse determined 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 off 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.
- **Detection Processes (DE.DP):** Guidehouse determined CenterPoint's deployment of the resiliency measure will have detection requirements in place 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 an improvement to the detection process, which has the benefit of increasing system awareness for appropriate, necessary, and timely responses to events. Additionally, an effective cybersecurity monitoring system encompasses security event

detection, including communication of the information to System Operation Control (“SOC”) personnel via alerts. CenterPoint indicated that SOC personnel will receive alerts through this new system and take action in response to the detected events.

- **Data Security (PR.DS):** Guidehouse determined the IT/OT Cybersecurity Monitoring resiliency measure will assist in availability with use of RAID technology for backing up. 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 in as part of this resiliency measure.

Additionally, Guidehouse determined CenterPoint Houston plans to actively monitor data 24x7, not just for alerts but also ensure only authorized users access the information. OT data will be kept on-premises within 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):** Guidehouse determined CenterPoint Houston will be implementing a system development life cycle 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):** Guidehouse determined CenterPoint Houston will deploy Splunk as part of their central logging system. Guidehouse concluded CenterPoint Houston has implemented firewalls and follows network architecture best practices to protect the CenterPoint Houston environment, which will be vital for the successful implementation of the CenterPoint’s cybersecurity monitoring system resiliency measure. Nozomi provides system level broadcasts for detection of removable media to ensure appropriate levels of protections and restrictions are in place. Additionally, CenterPoint Houston will design Nozomi alert use cases.
- **Awareness and Training (PR.AT):** Guidehouse determined CenterPoint Houston will ensure the efficient functioning of essential cyber monitoring systems by training personnel with a role in the use and execution of the related monitoring systems. The training should equip the necessary SOC personnel with knowledge to ensure readiness to respond appropriately. CenterPoint Houston has established SME architects that understand the necessity of understanding their roles and responsibilities as it pertains to cybersecurity.
- **Analysis (RS.AN):** Guidehouse determined CenterPoint’s IT/OT cybersecurity monitoring system will provide greater understanding of cyber incidents using network forensic analysis capabilities and historical monitoring. These components will provide improved analysis capability for both proactive and reactive threats.

Monitoring occurs on OT environments 24x7, which will provide additional analysis to support response and recovery efforts, and the program will provide enhancements to alerting that can provide notifications to guide response type and potentially reduce response time.

Q. PLEASE PROVIDE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S PROPOSED IT/OT-CYBERSECURITY MONITORING.

A. Guidehouse concludes CenterPoint Houston's IT/OT-Cybersecurity Monitoring is reasonable and beneficial for inclusion in CenterPoint Houston's Resiliency Plan. After reviewing the Guidehouse report, I agree this resiliency measure represents the most feasible approach to obtain the desired business process improvements and support higher resiliency of the CenterPoint Houston electrical system during normal and emergency operations. I concur with the Guidehouse analysis for the following reasons:

- The IT/OT-Cybersecurity Monitoring focuses on receiving cyber threat intelligence 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 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.
- I concur the IT/OT-Cybersecurity Monitoring implements several best practices that support strong resiliency by providing baselining of the network, 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 found a significant correlation of detective controls for system protection from malicious events, and potential intrusions to support inclusion of CenterPoint's IT/OT – Cybersecurity Monitoring resiliency measure in their Resiliency Plan. I concur this resiliency measure will provide CenterPoint 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 by enabling a quicker response to malicious events and attempts at intrusion, enhancing overall organizational resilience.
- The proposed IT/OT – Cybersecurity Monitoring resiliency measure is consistent with resiliency practices deployed at other utilities, based on Guidehouse experience and peer utility benchmarking survey results described in Section VI.

VI. INDEPENDENT BENCHMARKING OF CENTERPOINT HOUSTON'S RESILIENCY PLAN INVESTMENTS TO A PEER UTILITY GROUP

Q. PLEASE DESCRIBE HOW THE PEER ELECTRIC UTILITY BENCHMARKING ANALYSIS WAS GENERATED, INCLUDING HOW THE PEER GROUP OF ELECTRIC UTILITIES WAS SELECTED.

- A. The benchmarking analysis was designed to solicit responses from a peer group of electric utilities that have implemented resiliency measures. Guidehouse identified resiliency

measures to include in the survey questionnaire while an independent contractor³⁰ prepared survey questions and selected the peer utility group. The resiliency survey included questions designed to identify the types of resiliency investments U.S. electric utilities are deploying and the types of system issues that they are seeking to address through these investments. The survey was conducted “blind,” with the identities of participating utilities undisclosed to ensure confidentiality and included the types of resiliency investments being made by survey participants. Specific results for each of the five technology resiliency measures are addressed in the following response. These include identifying responses from participating Electric Utilities for the technology-related resiliency measures included in their resiliency plans as efficient and cost-effective investments to improve transmission and distribution system performance during resiliency events.

Q. PLEASE SUMMARIZE THE FINDINGS OF THE PEER ELECTRIC UTILITY BENCHMARKING AND HOW THIS PROVIDES AN INDICATOR OF INDUSTRY BEST PRACTICE FOR RESILIENCY-BASED INVESTMENTS.

A. Guidehouse finds that results from the peer utility benchmarking survey indicate making resiliency-focused investments in technology and cybersecurity is consistent with practices of other electric utilities engaging in resiliency planning. Benchmarking survey responses most pertinent to each of CenterPoint Houston’s proposed technology resiliency measures is presented below.

Q. PLEASE SUMMARIZE THE FINDINGS OF THE JURISDICTIONAL BENCHMARKING REPORT AND HOW THIS PROVIDES AN INDICATOR OF

³⁰ First Quartile Consulting

INDUSTRY BEST PRACTICES FOR TECHNOLOGY RESILIENCY MEASURES.

A. I reviewed the Jurisdictional Benchmarking Report provided as Appendix A in Exhibit ELS-2 and identified how the report provides indicators of best practices for the five technology resiliency measures:

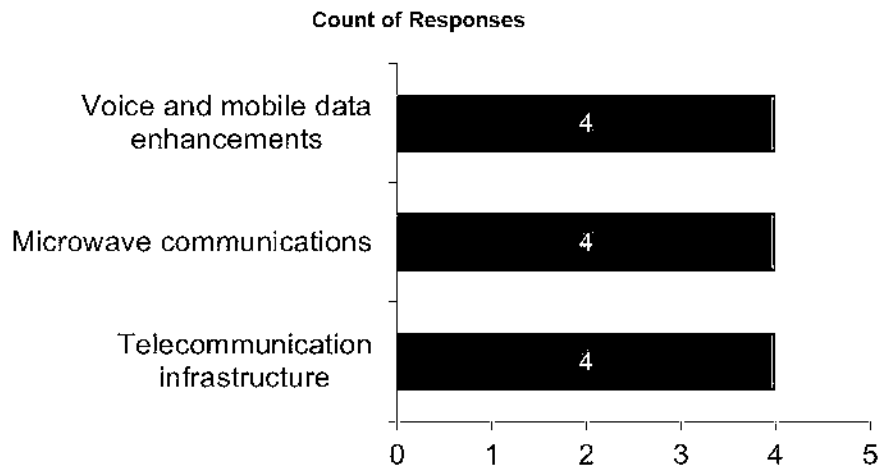
- **Projects for failover systems:** Selection is based on the ability to provide enhanced levels of redundancy and resiliency to key operational systems that could more easily succumb to extreme weather-related impacts or cyberattacks in their current configuration [Bullets 10.2 & 10.3: Data Center Refresh resiliency measure (see Dominion example)], or those that are critical to customer restorations during extreme weather events [Bullet 10.2: IT/OT-Cybersecurity Monitoring and Network Security & Vulnerability Management resiliency measures (see Duke & SCE examples)]
- **Communications projects:** Selected based upon the ability to provide an additional platform for stakeholder and emergency response information and resource sharing with the utility [Bullets 10.1 & 10.3: Backhaul Microwave Communications resiliency measure, Voice & Mobile Radio System Refresh resiliency measure (see Ameren example)]

Q. HOW DOES CENTERPOINT ENERGY HOUSTON ELECTRIC'S RESILIENCY PLAN COMPARE TO THE TYPES OF RESILIENCY INVESTMENTS BEING MADE BY THE PEER GROUP?

VOICE AND MOBILE DATA RADIO SYSTEM REFRESH

Guidehouse determined that the following three peer utility benchmarking survey resiliency investment categories are relevant to CenterPoint Houston's Voice and Mobile Data Radio System Refresh resiliency measure: voice and mobile data enhancements, microwave communications, and telecommunication infrastructure. As shown in Figure JBB-1. Four of the nine utilities that responded to the survey indicated they are making these types of investments for resiliency purposes.

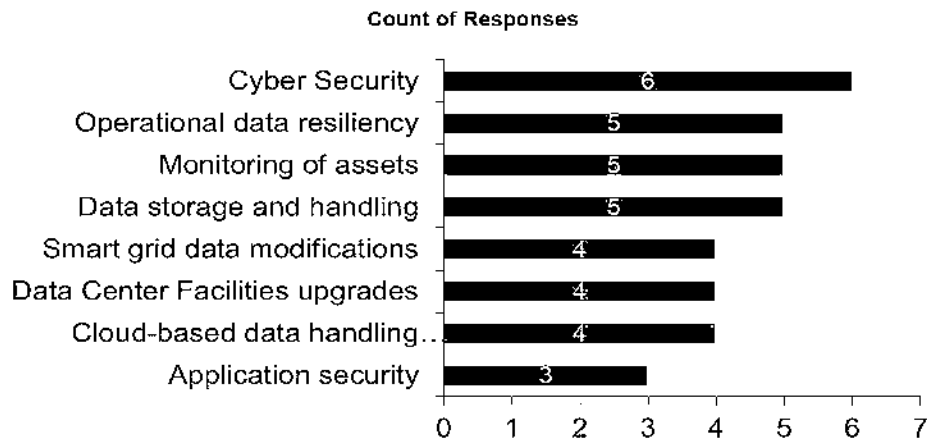
Figure JBB-1: Utility Investments In Voice And Mobile Technology



BACKHAUL MICROWAVE COMMUNICATIONS

Guidehouse determined that the following three peer utility benchmarking survey resiliency investment categories are applicable to CenterPoint Houston’s Backhaul Microwave Communications resiliency measure: operational data resiliency, microwave communications, and telecommunication infrastructure. As shown in Figure JBB-1, four of the nine utilities that responded to the survey indicated that they are making microwave communications and telecommunication investments for resiliency purposes. As shown in Figure JBB-2, five of the nine utilities that responded to the survey indicated that they are making operational data resiliency investments for resiliency purposes.

Figure JBB-2: IT Benchmarks



DATA CENTER REFRESH

Guidehouse determined that the following three peer utility benchmarking survey resiliency investment categories are relevant to CenterPoint Houston’s Data Center Refresh resiliency measure: data center facility upgrades, cloud-based data handling, and data storage and handling. As shown in JBB-3, between four and five of the nine utilities that responded to the survey indicated they are making these types of investments for resiliency purposes.

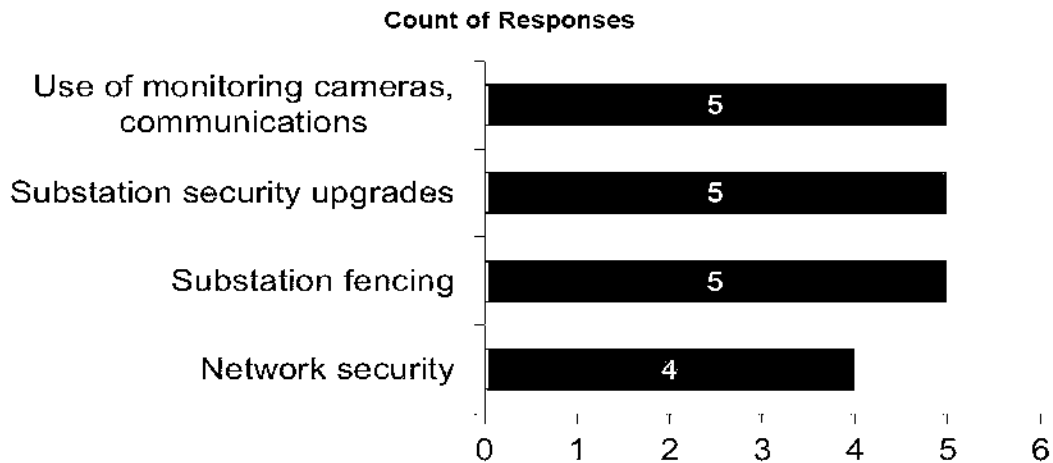
NETWORK SECURITY AND VULNERABILITY MANAGEMENT

Guidehouse determined that the following five peer utility benchmarking survey resiliency investment categories are relevant to CenterPoint Houston’s Network Security and Vulnerability Management resiliency measure as well as the Substation Security Upgrades and Substation Fencing resiliency measures reviewed in Mr. Shlitz’ (Guidehouse) testimony: cybersecurity, monitoring of assets, use of monitoring cameras, communications, and network security. As shown in Figure JBB-2 and Figure JBB-3, between four and six of the nine utilities that responded to the survey indicated they are making these types of investments for resiliency purposes.

IT/OT CYBERSECURITY MONITORING

Guidehouse determined that the following three peer utility benchmarking survey resiliency investment categories are relevant to CenterPoint Houston’s IT/OT – Cybersecurity Monitoring resiliency measure: cybersecurity, operational data resiliency, and monitoring of assets. As shown in JBB-2, between five and six of the nine utilities that

Figure JBB-3: Network Security & Vulnerability Management Benchmarks



responded to the survey indicated that they are making these types of investments for resiliency purposes.

Q. WHAT RECOMMENDATIONS WERE PROVIDED TO CENTERPOINT ENERGY HOUSTON ELECTRIC FOR CONSIDERATION IN THE DEVELOPMENT OF ITS RESILIENCY PLAN BASED ON THE PEER ELECTRIC UTILITY BENCHMARKING?

A. CenterPoint Houston’s proposed technology resiliency measures align with technology-related resiliency investments made by the peer benchmarking survey participants, therefore, Guidehouse did not make any recommendations specific to the benchmarking results.

Q. DID CENTERPOINT ENERGY MAKE MODIFICATIONS TO ITS RESILIENCY PLAN BASED ON THE FINDINGS PROVIDED BY GUIDEHOUSE FROM THE PEER ELECTRIC UTILITY BENCHMARKING?

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

VII. SUMMARY OF FINDINGS AND RECOMMENDATIONS

Q. HOW DID GUIDEHOUSE DETERMINE ITS FINDINGS AND RECOMMENDATIONS ON CENTERPOINT ENERGY HOUSTON ELECTRIC'S RESILIENCY PLAN?

A. The findings and recommendations offered in my testimony are based on the results of Guidehouse's independent analysis of resiliency risk for CenterPoint Houston's service area as well as qualitative comparative analysis of CenterPoint Houston's proposed resiliency plan investments for technology, including benchmarking of industry best practices in resiliency planning for electric utilities.

Further detail on Guidehouse's independent analysis and review is provided in Exhibit ELS-2, *Guidehouse's Independent Analysis and Review of CenterPoint Energy Houston Electric's Resiliency Plan*. This report supports my testimony and was prepared with assistance from Guidehouse staff and an outside consulting firm to conduct the peer utility benchmarking study.³¹

Q. PLEASE SUMMARIZE THE OVERALL FINDINGS FROM GUIDEHOUSE'S INDEPENDENT ANALYSIS AND REVIEW OF CENTERPOINT ENERGY HOUSTON ELECTRIC'S RESILIENCY PLAN.

A. First, Guidehouse finds that CenterPoint Houston's Resiliency Plan appropriately prioritizes technology resiliency measures that help mitigate cybersecurity risk. Guidehouse's physical and cyber security risk assessment confirms that the frequency and magnitude of physical and cyber-attacks is likely to increase over time, suggesting the need

³¹ First Quartile Consulting provided peer utility benchmarking data.

for continued resiliency investments in these areas. Given this, I also concur with the findings included in Mr. Shlatz' testimony that support CenterPoint Houston's proposed physical security resiliency measures to address cybersecurity risk.

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

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

- appropriate for addressing the risks it faces;
- aligned with industry best practice; and
- beneficial to customers and communities served by CenterPoint Houston.

Q. PLEASE SUMMARIZE THE RECOMMENDATIONS GUIDEHOUSE PROVIDED FOR CENTERPOINT ENERGY HOUSTON ELECTRIC'S CONSIDERATION

A. In its report, Guidehouse offered the following recommendations to CenterPoint Houston to further enhance its Resiliency Plan for the five technology resiliency measures:

1. **Voice and Mobile Data Refresh – Field Devices** – Leverage multiple sources of asset (field device) information in accordance with visual checks to ensure all legacy technology is properly tracked and decommissioned. Assets with end-of-life software that are still attached to the system and unaccounted for can either affect uptime/ resilience of the overall system if there is a malfunction, as well as become an attack vector for an external threat.

2. **Backhaul Microwave Communication Device Migration** – Develop a settings checklist, or asset configuration guide, so they can be easily replicated and installed on all new field devices, to remove the opportunity for incorrect settings being applied. This could potentially impact communication and responses in a weather or other event that could impact the distribution and transmission systems.
3. **Data Center Refresh** – When considering any type of data migration, ensure that all on-premises options such as application, workflow, and process optimizations are investigated to determine if they can be migrated, as migrating data to any new environment will affect uptime, application reliability, and support overall resilience. This is due to the eccentricities of any new environment, regardless of cloud or another on premise environment.
4. **Networking, Vulnerability, and Security – Data Management** – Investigate if downstream applications support encryption for data-in-transit, as applications that do not support for encryption for data-in-transit may be affected in relation to uptime, availability, and general resilience. For vulnerability, review patterns in deployment, such as applications, components, or any system component, that has repeatable settings and configurations so that CenterPoint Houston is aligned to industry general and cybersecurity best practices. For network, analyze network component and system best practices, so that CenterPoint Houston's network environment is further logically secured to ensure network zones are locked down and isolated.

5. **IT/OT-Cybersecurity Monitoring** – During implementation and deployment of Splunk and Nozomi, notify all users of the deployment, including detail on expectations to limit false flags while ensuring suspicious events and alerts and unexpected interactions are addressed. For the Splunk Integration, tune ingested information to minimize false alarms and unnecessary resource usage. Lastly, for the Nozomi Integration, refine vulnerability scanning so that only relevant suspicious or anomalous code is present in reports and Nozomi’s finding and vulnerability dashboards.

Q. PLEASE SUMMARIZE HOW CENTERPOINT ENERGY MADE MODIFICATIONS TO ITS RESILIENCY PLAN BASED ON THE FINDINGS AND RECOMMENDATIONS PROVIDED BY GUIDEHOUSE

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

VIII. CONCLUSION

Q. PLEASE SUMMARIZE YOUR DIRECT TESTIMONY.

A. Guidehouse reviewed the five CenterPoint Houston technology resiliency measures and identified the effectiveness and benefits of each resiliency measure in a qualitative comparative analysis process that compared relevant functions and security practices in each resiliency measure with industry best practices from the NIST CSF.

Guidehouse finds that CenterPoint Houston's Resiliency Plan appropriately prioritizes technology resiliency measures that help mitigate cybersecurity risk. Guidehouse's physical and cyber security risk assessment confirms that the frequency and magnitude of physical and cyber-attacks is likely to increase over time, indicating a need for continued resiliency investments in these areas.

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

I concluded the five technology resiliency measures in CenterPoint Houston's Resiliency Plan are:

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

Q. DOES THIS CONCLUDE YOUR DIRECT TESTIMONY?

A. Yes.

Exhibit JBB-1: Professional Experience of Dr. Joseph B. Baugh



Dr. Joseph B. Baugh

Associate Principal

joseph.baugh@guidehouse.com

Austin TX

Direct: 520.331.6351

Professional Summary

Dr. Baugh has a strong background in power system operations, information technology, business management, operational reliability, cyber and physical security, and regulatory compliance issues in the energy sector, including the North American electrical grid and the oil and gas sector. He applies those experiences to each client project to achieve the client's desired business goals and objectives in a cost-effective manner.

As an experienced academic professor and technical instructor, Dr. Baugh designs and delivers customized training programs to meet client needs and support timely implementations, knowledge transfer, and project handoffs to client personnel.

To accomplish these key objectives, he communicates effectively with client and Guidehouse management teams to keep them abreast of project development issues, project status, and issues associated with project change management.

Professional Experience

Dr. Baugh's professional career spans more than 50 years in the electrical utility and energy fields. Dr. Baugh is currently an Associate Principal in the Cybersecurity and Compliance team of the Energy, Sustainability, Infrastructure, State & Local Government (ESISL) practice. He currently supports Guidehouse clients with NIST 800-53r5 and other NIST control integrations, Supply Chain Risk Management implementation efforts, physical security risk assessments, and securing critical communication links between transmission and distribution system control centers. Dr. Baugh works closely with Guidehouse clients to apply the Department of Energy – Cybersecurity Capability Maturity Model (DOE-C2M2), NIST Cybersecurity Framework (CSF) and Risk Management Framework (RMF) models to assess the current state of client cyber security, risk management, and controls; identify significant gaps; design and develop high-quality solutions to mitigate identified gaps and achieve a desired target state. He also manages client projects to implement effective solutions across complex workstreams and multiple business units.

While at WECC, Dr. Baugh participated in electrical industry task forces and developed numerous outreach presentations for participants in the North American electrical grid, CIP compliance personnel, and industry user groups at WECC Reliability & Security Workshops, NERC meetings, and other industry outreach venues. Dr. Baugh completed several industry-based studies on the impact of the CIPv5 transition and implementation phases on Registered Entities in the North American electrical grid, the Transmission Owner Control Center issue, and Supply Chain Risk Management. His presentations on these studies to various industry associations and federal regulatory bodies helped influence beneficial policy changes in these crucial compliance areas. Dr. Baugh continues to bring his strong analytical and problem-solving skills to bear on problems faced by Guidehouse clients.



Dr. Joseph B. Baugh

Associate Principal

Dr. Baugh has served as an adjunct faculty member at several learning institutions since 1996 and is currently affiliated with the University of Phoenix, where he teaches information technology, business management, organizational behavior, and leadership courses in the College of Doctoral Studies. He mentors doctoral students throughout the dissertation process in the Doctor of Business Administration and Doctor of Management programs.

Dr. Baugh is a member of the Guidehouse Coaching and Mentoring team and works with numerous junior team members to support their growth and development as consulting professionals. He also teaches in the Guidehouse Project Management Professional (PMP) training program to share his insights on implementing sound project management practices to benefit our clients.

Dr. Baugh's professional and academic research interests include organizations in transition, organizational structures, and change management. He presents his research in domestic and international venues and regularly publishes papers in scholarly journals.

Representative Guidehouse Client List and Engagements

- » **Alberta Electric System Operator (AESO)** (Sep 2020-present). Provided audit preparation evidence reviews, compliance recommendations, and training. Currently developing training for internal audit team to perform CIP audits for participating Albertan electrical entities.
- » **American Gas Foundation (AGF)** (Apr 2020 – Sep 2020). Leading the cybersecurity team effort for a study on gas sector programs and procedures to enhance resiliency and security for local gas distribution companies.
- » **American Electric Power (AEP)** (Feb 2020 – Jun 2020). Worked with CIP-002, CIP-013, and CIP-014 teams to review and improve compliance documentation, audit evidence, RSAW narratives, Level 1 ERT questions.
- » **British Columbia Hydro (BC-Hydro)** (Jan 2023 – Present) Supporting Site C compliance team, performing BCUC Reliability Standard sufficiency reviews.
- » **California Department of Water Resources (CDWR)** (Mar 2020 – present). Developing CIP-012, CIP-013, and other compliance programs, processes, and procedures. Developing training programs for medium impact Control Centers.
- » **California Public Utility Commission (CPUC)** (2022). Served as Subject Matter Expert for CPUC Utility Cybersecurity Assessment engagement. Developed NIST CSF-based cyber security assessment and data analysis tools to support the assessment study.
- » **CenterPoint Energy (CNP)** (Jan 2024 – Present).
 - Developed comparative analysis methodology based on the NIST CSF to support Guidehouse review of technology resiliency measures for CenterPoint Houston Electric PUCT resiliency rate filing.
 - Serving as expert witness for technology resiliency measure component of PUCT resiliency rate filing.
- » **Con Edison of New York (CENY)** (Jan – Jul 2020). Supported cybersecurity component of study into Home Area Network implementations in a major metropolitan service territory.
- » **Florida Power & Light (FPL)** (2021-2022). Supported regulatory compliance efforts for Supply Chain Risk Management, critical asset identification, and other compliance related activities.



Dr. Joseph B. Baugh

Associate Principal

- » **Imperial Irrigation District (IID)** (Jan 2020 – Present). Developing emerging compliance programs for cybersecurity and cold weather event NERC Standards and reviewing existing compliance programs to support pre-audit activities.
- » **Los Angeles Department of Water & Power (LADWP)** (Dec 2019 – present).
 - Support Critical Infrastructure Protection (CIP) teams, as needed, on internal controls, audit preparation, and addressed ad-hoc questions, as needed.
 - Develop training materials and deliver cybersecurity training for compliance personnel and business unit Subject Matter Experts (SME).
 - Implemented initial DOE-C2M2 evaluation across LADWP Water, Power, and Shared Services groups.
- » **New York Power Authority (NYPA)** (Jun 2021 – Apr 2022) PER-005-2 readiness assessment and PER-005-2 training program plan development.
- » **Ontario Power Generation (OPG)** (Oct 2022 – Feb 2023) Performed FAC-008 & MOD-032 compliance sufficiency reviews and supported multiple PRC sufficiency reviews.
- » **Pacific Gas & Electric (PG&E)** (Jan 2020 – present). Supporting CIP-002 and CIP-014 teams to assess and classify transmission system components, supported CIP-013 SCRM program development.
- » **Sacramento Municipal Utility District (SMUD)** (Jan 2020 – Jun 2020). Updated and modified SMUD CIP-011-2 Information Protection Program. Supported development of CIP-013 program, addressed ad-hoc questions, as needed.
- » **San Diego Gas & Electric (SDGE)** (Dec 2019 – Aug 2021). Supported development of CIP-013 program, developed training materials, addressed ad-hoc questions for other NERC Reliability Standards. Supported CIP-014 internal controls development.
- » **Tallgrass Energy (TGE)** (Nov – Dec 2022) Performed physical and cyber security gap assessment, integrated NIST CSF and NIST SP 800-53r5 controls into development of client's TSA Pipeline Security Directive SD02C: Cybersecurity Implementation Plan.
- » **Tennessee Valley Authority (TVA)** (Jun 2021 – Oct 2021; Jan 2023 – May 2023) Supported Supply Chain Risk Management program and Digital IoT Center of Excellence (CoE) program development.
- » **Western Electric Coordinating Council (WECC)** (Nov 2019 – May 2021) Served as expert witness for compliance violation enforcement case.
- » **Other Guidehouse clients** (Dec 2019 – present). Reviewing compliance program and internal controls documentation to identify compliance gaps and develop recommendations for improvements across the gamut of CIP and O&P Reliability Standards.
- » **Guidehouse Industry Outreach** – see *Articles, Publications and Discussion Panels* section below.



Dr. Joseph B. Baugh

Associate Principal

Work History

- » Guidehouse, Inc., Associate Principal (2022-Present)
- » Guidehouse, Inc., Managing Consultant (2019-2022)
- » Western Electric Coordinating Council, Senior Compliance Auditor, Cybersecurity (2011-2019)
- » Arizona Electric Power Cooperative, Power Trading & Scheduling Manager (2008-2011)
- » Irby Construction Company, Groundman, Apprentice Lineman, Journeyman Lineman, Foreman, Transmission power line construction projects across U.S. (1973-1980)
- » Sierra Southwest Electric Cooperative, multiple IT roles culminating in IT Services Manager (1998-2008)
- » Arizona Electric Power Cooperative, Power System Controller (1990-1998)
- » Arizona Electric Power Cooperative, Journeyman Lineman – Live Line & Barehand Transmission Maintenance crew (1982-1990)
- » Anamax Mining, Journeyman Lineman (1980-1982)

Education

- » Ph.D., Organization & Management with specialization in Leadership, Capella University (2008);
 - *Deregulation and Management Strategies: A Case Study of Georgia System Operations Corporation*. [Doctoral Dissertation, Capella University, 2008]. In ProQuest Dissertations and Theses Database [UMI# 3296749].
- » MBA, Eller College of Management, University of Arizona (2004);
- » Bachelor of Science, Computer Science, University of Arizona (2000);
- » Associate of Arts, Spanish, Cochise College (1997);
- » Associate of Science, Computer Science, Cochise College (1996).

Current Professional Certifications (initial certification date)

- » Project Management
 - PMP - PMI #41619 (2001)
- » Cybersecurity
 - NCSP - APMG Intl. #2001109035 (2022)
 - CISA - ISACA #12103648 (2012)
 - CRISC - ISACA #1112935 (2011)
 - CISM - ISACA #0300492 (2003)
 - CISSP - ISC^2 #32233 (2002)
- » Power System Operations
 - NERC Certified System Operator - NERC -#BI200911009 (2009)
- » Physical Security
 - PCI - ASIS Intl. #21806 (2019)
 - CPP - ASIS Intl. #20742 (2018)
 - PSP - ASIS Intl. #20077 (2017)



Dr. Joseph B. Baugh

Associate Principal

Articles, Publications and Discussion Panels

- » Baugh, J. (2023 February 15). *Adapting the NIST Cybersecurity Framework to the Energy Sector*. APMG International [Videocast]. <https://www.youtube.com/watch?v=O3fWhOgjkOA>
- » Baugh, J. (2021 November 4). *Cybersecurity*. Ontario Energy Association: Speaker Series [Webinar: Cybersecurity Panel Moderator]. <https://mailchi.mp/energyontario/oea-speaker-series-cyber-security-panel-discussion-register-now-for-nov-4-webinar>
- » Baugh, J. (2021 February 2). *Addressing "Weak Link" Vendors in the Power Grid*. Waterfall Security Solutions Industrial Security Podcast series [Episode #52, Moderated by Andrew Ginter]. <https://waterfall-security.com/joseph-baugh/>
- » Baugh, J., Luras, C., Dury, J., Bailey, M., Sarin, K., & Kintzer, G. (2020 May 26). *Executive Order 13920: Position Paper*. Guidehouse, Inc.: Chicago IL. White paper developed to address potential impacts on participants in the North American electrical grid created by *Executive Order 13920: Securing the United States Bulk-Power System* (Trump, D. J., 2020 May 1). https://guidehouse.com/-/media/www/site/insights/energy/2020/eo-13920_gh_positionpaper_final.pdf
- » Baugh, J. B. (2020 April 23). *COVID-19: Balancing Reliability of the Electrical Grid and Compliance*. [Open Webinar]. PowerPoint outreach presentation on managing reliability, security, and compliance with NERC Standards in the North American electrical grid during the COVID-19 pandemic. <https://www.linkedin.com/feed/update/urn:li:activity:6659493312686284801/>
- » Baugh, J. B. (2019 November 18). *CIP-013-1: Compliance Auditing Approach* [Modified to include key topics addressed at NERC SCRM SGAS meetings in Buckhead GA]. WECC Tech Talk taped in Salt Lake City UT to archive October 2019 presentation delivered at WECC R&S Workshop for stakeholders in the Western Interconnection.
- » Baugh, J. B. (2019 November 4). *CIP-013-1 Supply Chain Risk Management (SCRM) Planning*. Outreach presentation at California Independent System Operator (CAISO) in Folsom CA for CAISO and RC West SCRM planning personnel.
- » Baugh, J. B., & Carver, K. (2019 October 30). *Open Forum Panel Discussion on Supply Chain Risk Management (SCRM)* during NERC SCRM Small Group Advisory Sessions in Buckhead GA (October 29-31, 2019).
- » Baugh, J. B. (2019 October 23). *CIP-013-1: Compliance Auditing Approach*. Outreach presentation at WECC Reliability & Security Workshop. Las Vegas NV
- » Baugh, J. B. (2019 August 28). *CIP-013-1: Supply Chain Risk Management and Low Impact BES Cyber Systems*. Webinar presentation for the Western Interconnection Forum (WICF) Small Entity Focus Group to support voluntary compliance with CIP-013-1 for LIBCS across WICF and the North American electrical grid.
- » Baugh, J. B. (2019 August 7). *CIP-013-1 Supply Chain Risk Management (SCRM) Update*. Outreach presentation at Farmington Electrical Utility Services (Farmington NM) for small entities in the Western Interconnection of the North American electrical grid (also attended by three FERC observers).



Dr. Joseph B. Baugh

Associate Principal

- » Baugh, J. B. (2019 July 30). *CIP-013-1: Developing the Audit Approach & Appropriate Internal Control Questions*. Internal training presentation at WECC Office (Salt Lake City UT) for Critical Infrastructure Protection [CIP] and Risk Assessment and Mitigation [RAM] teams.
- » Baugh, J. B. (2019 July 23). *CIP-013-1 Supply Chain Risk Management: Audit Approach & Internal Controls*. Presentation at NERC Compliance & Standards Workshop (Minneapolis MN) for stakeholders in the North American electrical grid.
- » Baugh, J. B. (2019 July 18). *CIP-013-1 Supply Chain Risk Management (SCRM) Update*. Outreach presentation at PacifiCorp (Portland OR) to support the development of utility SCRM project teams and compliance efforts in the Northwest region of the Western Interconnection of the North American electrical grid.
- » Baugh, J. B. (2019 July 11). *CIP-013-1 Supply Chain Risk Management (SCRM) Update*. Presentation at WICF Peer Share Event (Albuquerque NM) for stakeholders in the Western Interconnection of the North American electrical grid.
- » Baugh, J. B. (2019 May 30). *CIP-013-1 Supply Chain Risk Management (SCRM) Update*. Presentation in WECC Open Webinar [WebEx format] for stakeholders in the Western Interconnection of the North American electrical grid.
- » Baugh, J. B. (2019 March 21). *Aligning the Purposeful Parts: Developing a Strong Research Proposal by Applying an Alignment Mantra*. Presentation in D. Martin (Chair), Oxford Education Research Symposium, Green Templeton College, University of Oxford, England [March 20-22, 2019].
- » Baugh, J. B. (2019 February 6). *CIP-002-5.1a-BC: Auditing CIP-002 in the BCUC Footprint*. Presentation at British Columbia Utility Commission [BCUC]/WECC outreach event. Held at BCUC Hearing Room, Vancouver BC. [February 6-7, 2019].
- » Baugh, J. B. (2019 January 9). *Interview Techniques*. Internal training presentation at WECC Compliance Team Meetings in WECC office, Salt Lake City UT [January 8-10, 2019] for members of the WECC Compliance Department.
- » Baugh, J. B. (2019 January 7). *Tech Talk with Dr. Baugh on Essential Cyber Assets, Identifying and Managing Essential Cyber Assets: Closing the Loop on the BCS*. Taped during WECC Compliance Team Meetings in WECC office, Salt Lake City UT [January 8-10, 2019].
- » Baugh, J. B. (2018 October 24). *Supply chain risk management [CIP-013-1 SCRM]* Presentation delivered at the WECC Reliability and Security Workshop, San Diego CA. [October 22-25, 2018].
- » Baugh, J. B. (2018 October 23). *Identifying and managing essential Cyber Assets: Closing the loop on the BCS*. Presentation delivered at the WECC Reliability and Security Workshop, San Diego CA. [October 22-25, 2018].
- » Baugh, J. B. (2018 August 23). *Low impact BES Assets: The clock is ticking – Looking ahead to CIP-003-7*. Presentation delivered at NAES 2019 Utility User Group conference, Seattle Washington. [August 22-24, 2018].



Dr. Joseph B. Baugh

Associate Principal

- » Baugh, J. B. (2018 January 18). *CIP-002-6: Standard Update*. Presentation to WECC entities on WECC Open Webinar [Salt Lake City UT].
https://www.wecc.biz/_layouts/15/WopiFrame.aspx?sourcedoc=/Administrative/WECC_Open%20Mic%20Presentation%201.18.18.pdf&action=default&DefaultItemOpen=1
- » Baugh, J. B. (2018 January 9). *BCUC – Transitioning to CIP-002-5.1 (Session 1)*. Presentation at British Columbia Utility Commission [BCUC] CIPv5 Compliance Outreach in Salt Lake City UT.
https://www.wecc.biz/Administrative/01_WECC_BCUC_CIP-002-5.1_Low_Impact_SLC_JBaugh.pdf
- » Baugh, J. B. (2018 January 9). *BCUC - Identifying & Auditing Low Impact BES Assets: A Mock Audit (Session 2)*. Presentation at British Columbia Utility Commission [BCUC] CIPv5 Compliance Outreach in Salt Lake City UT.
https://www.wecc.biz/Administrative/02_WECC_BCUC_Low_Impact_Mock_Audit_SLC_JBaugh.pdf
- » Baugh, J. B. (2018 January 9). *BCUC - Low Impact BES Assets: Best Practices (Session 3)*. Presentation at British Columbia Utility Commission [BCUC] CIPv5 Compliance Outreach in Salt Lake City UT.
https://www.wecc.biz/Administrative/03_WECC_BCUC_Low_Impact_Best_Practices_SLC_JBaugh.pdf
- » Baugh, J. B. (2017 November 14). *CIP-013-1: Update on Supply Chain Risk Management [SCRM] Standard*. Presentation at WECC Compliance Workshop, Portland OR [November 14-16, 2017].
[https://www.wecc.biz/_layouts/15/WopiFrame.aspx?sourcedoc=/Administrative/03%202017-11-14%20Update%20on%20New%20Supply%20Chain%20Risk%20Management%20\(SCRM\)%20Standard.%20Baugh.pdf&action=default&DefaultItemOpen=1](https://www.wecc.biz/_layouts/15/WopiFrame.aspx?sourcedoc=/Administrative/03%202017-11-14%20Update%20on%20New%20Supply%20Chain%20Risk%20Management%20(SCRM)%20Standard.%20Baugh.pdf&action=default&DefaultItemOpen=1)
- » Baugh, J. B., & Dalebout, M. (2017 November 14). *Evaluating Dispersed Generation Resources: Solar Inverters and MVAR Support*. Presentation at WECC Compliance Workshop, Portland OR [November 14-16, 2017].
https://www.wecc.biz/_layouts/15/WopiFrame.aspx?sourcedoc=/Administrative/02%202017-11-14%20Solar%20Inverters%20with%20MVAR%20Support.Baugh.Dalebout.pdf&action=default&DefaultItemOpen=1
- » Baugh, J. B. (2017 October 31). *IEC 61850 Deployment: Security, Reliability and CIP Compliance Considerations*. Peer-reviewed presentation at SEAM Fall 2017 meeting during CEATI Conference, Burnaby British Columbia, October 30-November 2, 2017.
- » Baugh, J. B. (2017 September 18). *Critical Electrical Infrastructure: Threats, Vulnerabilities & Regulatory Issues*. Presentation at Power Grid Resiliency Summit, San Diego CA [September 18-20, 2017].
- » Baugh, J. B. (2017 September 7). *Managing a Major Governance Change Initiative: Implementing New Critical Infrastructure Protection Standards across the North American Electrical Grid*. Presentation at ISACA Phoenix Security and Audit Conference, Tempe AZ at the Desert Willow Conference Center, Phoenix AZ.



Dr. Joseph B. Baugh

Associate Principal

- » Baugh, J. B. (2016 October 27). *CIPv5 Project Follow-up Survey*. Presentation on Critical Infrastructure Protection implementation project. Phase 2 slide deck presented at WECC Compliance Workshop, Scottsdale AZ [October 27-28, 2016].
https://www.wecc.biz/_layouts/15/WopiFrame.aspx?sourcedoc=/Administrative/13%20WECC_CIPv5_Survey_JBaugh_CW_Oct2016.pdf&action=default&DefaultItemOpen=1
- » Baugh, J. B. (2016 August 23). *Who's Driving the Bus: Compliance or Security?* [Moderator] Panel Discussion at EnergySec Summit. 2016, Anaheim CA. [August 22-24, 2016].
- » Baugh, J. B. (2016 June). *Examining the impact of team dynamics on academic and professional performance: A cross-sectional study at three levels of higher education*. *Journal of Academic Perspectives*, 2016(2), 1-22. <http://www.journalofacademicperspectives.com/back-issues/volume-2016/volume-2016-no-2/>
- » Baugh, J. B. (2016, March 18). *Examining the impact of team dynamics on academic and professional performance: A cross-sectional study at three levels of higher education – Phase 2*. Presentation in D. Martin (Chair), Oxford Education Research Symposium, Oxford University Club, University of Oxford, England. [March 17-19, 2016].
- » Baugh, J. B. (2015, August-September). *CIPv5 Transition Project Survey*. Unpublished mixed-methodology study on organizational impacts incurred during the implementation of upcoming Critical Infrastructure Protection (CIP version 5) Reliability Standards on electrical utilities and other participants in the Western Interconnection of the North American Electrical Grid. Survey results presented to the Western Electricity Coordinating Council [WECC] Board of Directors (Salt Lake City UT: September 15, 2015), WECC CIP Users Group [CIPUG] (San Diego CA: October 13, 2015), North American Electric Reliability Corporation [NERC] Electric Reliability Organization [ERO] workshop (Cleveland OH: October 21, 2015), NERC - Critical Infrastructure Protection Committee [CIPC] (Atlanta GA, December 15, 2015), and Federal Energy Regulatory Commission [FERC] (Washington DC, Jan 27, 2016). Retrieved from:
https://www.wecc.biz/_layouts/15/WopiFrame.aspx?sourcedoc=/Administrative/05%20CIPv5%20Transition%20Project%20Survey.pdf&action=default&DefaultItemOpen=1
- » Baugh, J. B. (2014, March). *Examining the impact of team dynamics on academic and professional performance: A cross-sectional study at three levels of higher education – Phase 1*. Presentation in D. Martin (Chair), Oxford Education Research Symposium, St. Edmund Hall, University of Oxford, England [March 25-27, 2014]
- » Baugh, J. B. (2013, March). *Developing critical thinking capacities: A practical perspective*. Proceedings of INTED2013, (pp. 3391-3399), 7th International Technology, Education and Development Conference. March 4-5, 2013. Valencia, Spain.
<https://library.iated.org/view/BAUGH2013DEV>.
- » Harris, M. E., Dew, K. E., Hallcom, A. S., & Baugh, J. B. (2012, August). *The informal economy of stressors: Detouring successful completion of a holistic doctoral journey*. Professional Development Workshop presented at the 2012 Academy of Management Annual Conference & Doctoral Consortium, Boston, MA.



Dr. Joseph B. Baugh

Associate Principal

- » Harris, M. E., Baugh, J. B., Dew, K. E., & Hallcom, A. S. (2011, August). *West meets East: Managing the successful completion of a holistic doctoral journey*. Professional Development Workshop presented at the 2011 Academy of Management Annual Conference & Doctoral Consortium, San Antonio, TX.
- » Baugh, J. B. (2011, June). *Managing a major organizational change initiative: Lessons learned about coping with complexity induced by homogeneous internal teams and globally diverse external partners*. Proceedings of the 2011 5th Annual Management Consulting Division of the Academy of Management Conference on Exploring the Professional Identities of Management Consultants. Amsterdam, Netherlands.
- » Harris, M. E., Hallcom, A. S., Dew, K. E., & Baugh, J. B. (2011, June). *Exploring research assessing management consultants as agents of change*. Proceedings of the 2011 5th Annual Management Consulting Division of the Academy of Management Conference on Exploring the Professional Identities of Management Consultants. Amsterdam, Netherlands.
- » Baugh, J. B. (2011, June). *Improving the impact of qualitative research: A practical perspective of a study supported by qualitative data analysis software from inception to completion*. Professional Development Workshop presented at the 2011 ISEOR-Academy of Management Research Methods Division Joint Conference on Performance Metrics of the Impact of Management Research. Lyon, France.
- » Baugh, J. B., Hallcom, A. S., Dew, K. E., & Harris, M. E. (2011, June). *Developing applied researchers: A holistic view of the doctoral journey*. Proceedings of the 2011 ISEOR-Academy of Management Research Methods Division Joint Conference on Performance Metrics of the Impact of Management Research. Lyon, France.
- » Baugh, J. B., Hallcom, A. S., & Harris, M. E. (2011, January). *Changes that make a difference: Attaining a PhD while maintaining an active life*. Revista del Instituto Internacional de Costos, (8), 61-72. ISSN: 1646-6896. http://www.revistaic.org/articulos/num8/articulo3_esp.pdf.
- » Harris, M. E., Hallcom, A. S., Dew, K. E., & Baugh, J. B. (2010, August). *Dare to Care: Using a new paradigm to successfully complete the doctoral journey*. Professional Development Workshop at the Academy of Management 2010 Annual Conference & Doctoral Consortium, Montreal, Canada.
- » Baugh, J. B., Hallcom, A. S., & Harris, M. E. (2010, June). *Computer assisted qualitative data analysis software: A practical perspective for applied research*. Revista del Instituto Internacional de Costos (6), 69-81. ISSN: 1646-6896. http://www.revistaic.org/articulos/num6/articulo4_esp.pdf.
- » Baugh, J. B. (2010, February). *Securing social media: Using AIM in AEPCO power scheduling and trading operations*. Presentation at NRECA 2010 TechAdvantage Conference, Atlanta GA.
- » Baugh, J. B. (2009, November). *Qualitative data analysis software: A discussion and demonstration of Atlas.ti®*. Presented to University of Arizona South Faculty and Staff.
- » Baugh, J. B. (2009, October). *Identifying stakeholders and collecting requirements: Better project planning and control*. Presented at PMI-Tucson Chapter Meeting.



Dr. Joseph B. Baugh

Associate Principal

- » Harris, M. E., Hallcom, A. S., & Baugh, J. B. (2009, August). *Making a difference in successfully completing a holistic doctoral journey*. Professional Development Workshop at the Academy of Management 2009 Annual Conference & Doctoral Consortium, Chicago IL.
- » Baugh, J. B., Hallcom, A. S., & Harris, M. E. (2009, June). *Computer assisted qualitative data analysis software: A practical perspective for applied research*. Proceedings from the 2009 ISEOR - Academy of Management International Conference and Doctoral Consortium on Social Responsibility and Corporate Environmental Evaluation Indicators (Vol. 1, pp. 173-182). Lyon, France: ISEOR.
- » Baugh, J. B. (2009, May). *Project risk management: Managing the four C's of stakeholder expectations*. Presented at PMI-Tucson Chapter Meeting.
- » Baugh, J. B. (2009, March). *Developing critical thinking for applied research*. Paper presented at the Critical Thinking Forum, sponsored by the United States Army Intelligence Center, Ft. Huachuca AZ.
- » Baugh, J. B. (2008, Fall). *Project risk management: Managing the four C's of stakeholder expectations*. PMI-ISSIG Review, 12(4), 5-8.
- » Baugh, J. B. (2008, Summer). *Cooperatives in transition: Restructuring and recovery in Georgia*. NRECA Management Quarterly, 49(2), 2-19.
- » Baugh, J. B. (2006, December). *Surviving comps on the expedited plan*, Capella University doctoral colloquium presentation, Wyndham Resort Hotel and Convention Center, Orlando FL.
- » *Threat Management*, Discussion Panel Member. Sponsored by Symantec and GMT Technologies, University Marriott Hotel, Tucson AZ, January 18 2005.
- » *Plain Talk about Information Assurance for Business Executives and Non-Profit Organizations*, Security Seminar Discussion Panel Member. Sponsored by CITA, Doubletree Hotel, Tucson AZ, April 29, 2003.
- » *Emerging Technology Conference*, Discussion Panel Member. Sponsored by GIGA, Phoenician Resort, Scottsdale, December 10, 2002

Exhibit JBB-2: Glossary of Acronyms

AI	Artificial Intelligence
ADMS	Advanced Distribution Maintenance System
ASIS	American Society for Industrial Security
BC	Business Continuity
BC/DR	Business Continuity and Disaster Recovery
BPS	Bulk Power System
BS	Bachelor of Science
C2M2	Cybersecurity Capability Maturity Model
CenterPoint Houston or the Company	CenterPoint Energy Houston Electric, LLC
CIP	Critical Infrastructure Protection
CISA	Certified Information Systems Auditor
CISA	Also, Cybersecurity and Infrastructure Security Agency
CISA-ISD	CISA Infrastructure Security Division
CISM	Certified Information Security Manager
Commission	Public Utility Commission of Texas
Core	The Framework Core
CPP	Certified Protection Professional
CRISC	Certified in Risk and Information Systems Control
CSF	Cybersecurity Framework
CVE	Common Vulnerability and Exposure
DDoS	Distributed Denial-of-Service
DERs	Distributed Energy Resources
DMR	Digital Mobile Radio
DOE	Department of Energy
GRC	Governance, Reliability, Compliance
HTTPS	Hypertext Transfer Protocol Secure
ICC	Illinois Commerce Commission
IEA	International Energy Agency
IPSec	Internet Protocol Security
IR	Incident Response
IT	Information Technology
KPI	Key Performance Indicator
LMR	Land Mobile Radio
LTE	Long Term Evolution
MBA	Master of Business Administration
NCSO-BI	NERC Certified System Operator Balancing and Interchange
NCSP	NIST Cybersecurity Professional
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NJBPU	New Jersey Board of Public Utilities
O&M	Operations and maintenance

OT	Operations Technology
P25	Project 25
PCI	Professional Certified Investigator
Ph.D.	Doctor of Philosophy
PMP	Project Management Professional
PPD-21	Presidential Policy Directive 21
PSP	Physical Security Professional
Resiliency Event	A low frequency, high impact event that, if not mitigated, poses a material risk to the safe and reliable operation of the Company's transmission and distribution system
Resiliency Measure	A measure designed to mitigate the risks posed to the Company's transmission and distribution system by a Resiliency Event
ROI	Return on Investment
SAN	Storage Area Network
SED	Self Encrypting Drives
Service Company	CenterPoint Energy Service Company, LLC
SME	Subject Matter Expert
SOC	Security Operations Center
SSDLC	Secure Software Development Lifecycle
TDHS	Texas Department of Homeland Security
THSSP	Texas Homeland Security Strategy Plan
WECC	Western Electricity Coordinating Council

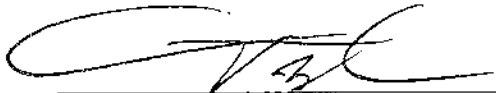
STATE OF TEXAS §
 §
COUNTY OF HARRIS §

AFFIDAVIT OF DR. JOSEPH B. BAUGH

Before me, the undersigned authority, on this day personally appeared Dr. Joseph B. Baugh, who being by me first duly sworn, on oath, deposed and said the following:

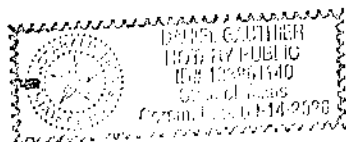
1. “My name is Dr. Joseph B. Baugh. I am of sound mind and capable of making this affidavit. The facts stated herein are true and correct based on my personal knowledge. I am currently an Associate Principal on the Cybersecurity and Compliance team in the Energy, Sustainability, and Infrastructure, State, & Local Government (ESISL) practice for Guidehouse Inc.
2. The foregoing direct testimony and the attached exhibits have been prepared by me or under my direct supervision and are true and correct to the best of my knowledge.”


Further affiant sayeth not.



Dr. Joseph B. Baugh

Subscribed and sworn to before me on this 18th day of March 2024.





Notary Public in and for the State of Texas

NOTICE OF RESILIENCY PLAN FILING

On April 29, 2024, CenterPoint Energy Houston Electric, LLC (“CenterPoint Houston” or the “Company”) filed with the Public Utility Commission of Texas (the “Commission”) an Application for Approval of its Transmission and Distribution System Resiliency Plan (the “Application”). The Company filed the Application in compliance with the Transmission and Distribution System Resiliency Plan requirements under 16 Tex. Admin. Code (“TAC”) § 25.62. The Application has been assigned Docket No. 56548.

Attached to the Application, the Company presents its three-year plan (2025-2027) for enhancing the resiliency of its transmission and distribution systems in the face of resiliency events and other resiliency-related risks (the “Resiliency Plan”). In the Resiliency Plan, the Company defines each event, including extreme weather conditions, vegetation management, wildfires, cybersecurity threats, or physical security threats, that poses a material risk to the safe and reliable service to customers in the Company’s service area (each, a “Resiliency Event”). To mitigate the impacts of such Resiliency Events, the Company identified twenty-five programs or initiatives designed to prevent, withstand, mitigate, or more promptly recover from Resiliency Events (each, a “Resiliency Measure”). The Company estimates that the twenty-five Resiliency Measures will cost approximately \$2.19 billion in capital costs and \$85.9 million in incremental O&M expense over the three-year period from 2025 to 2027. The table below summarizes the cost of each Resiliency Measure in the Company’s Resiliency Plan.

Resiliency Measure	Estimated Capital Costs (millions)	Estimated Incremental O&M Costs (millions)	Estimated Timeframe (years)
<u>System Hardening</u>			
Transmission System Hardening	\$376.0	\$0.75	2025-2027
S90 Tower Replacements	\$103.8	None	2025-2027
69kV-138kV Conversion Projects	\$268.4	None	2025-2027
Coastal Resiliency Upgrades	\$259.0	\$0.75	2025-2027
Substation Transformer Fire Protection Barriers	\$2.4	None	2025-2027
Distribution Pole Replacements/Bracing	\$99.3	None	2025-2027
Distribution Resiliency – Circuit Rebuilds	\$312.8	None	2025-2027
Strategic Undergrounding/Freeway Crossings	\$31.2	None	2025-2027
Subtotal	\$1,452.9	\$1.5	

Grid Modernization

TripSaver®	\$58.9	\$0.03	2025-2027
IGSD Installation	\$53.8	\$0.82	2025-2027
Texas Medical Center Substation	\$102.0	\$0.15	2025-2027
Subtotal	\$214.7	\$1.0	

Flood Control

Substation Flood Control	\$30.6	None	2025-2027
Control Center Facility Upgrades	\$7.0	None	2025-2027
Subtotal	\$37.6	None	

Information Technology to Support Operations

Advanced Aerial Imagery Platform/Digital Twin	\$9.9	\$0.06	2025-2027
Advanced Distribution Technology	\$225.8	\$15	2025-2027
Digital Substation	\$25.0	(\$0.6)	2025-2027
Subtotal	\$260.7	\$14.46	

Information Technology

Voice and Mobile Data Radio System Refresh	\$15.6	None	2025-2027
Backhaul Microwave Communication	\$12.1	None	2025-2027
Data Center Refresh and Resiliency	\$2.9	\$0.25	2025-2027
Network Security and Vulnerability Management	\$1.0	None	2025-2027
IT/OT Cybersecurity Monitoring Program	\$22.5	None	2025-2027
Subtotal	\$54.1	\$0.25	

Physical Security

Substation Physical Security Fencing	\$15.0	None	2025-2027
Substation Security Upgrades	\$19.5	\$0.09	2025-2027
Subtotal	\$34.5	\$0.09	

Vegetation Management

Targeted Critical Circuit Vegetation Management	-	\$25.0	2025-2027
Subtotal	-	\$25.0	

Wildfire Mitigation

Wildfire Mitigation Projects	\$137.2	\$43.7	2025-2027
Subtotal	\$137.2	\$43.7	

Total for all Resiliency Measures **\$2,191.7** **\$85.9**

The Company also seeks Commission approval of two pilot programs (1) a utility-scale microgrid pilot program and (2) a pilot program to fund a City of Houston employee that would be responsible for overseeing resiliency issues for the City of Houston (with funding not to exceed \$200,000 per year). To provide the Commission a full picture of CenterPoint Houston's resiliency efforts, the Company also describes the eventual transition and migration of the Company's SAP software to a cloud-based application, which will support resiliency in a number of ways.

Lastly, as part of the Company's Resiliency Plan, the Company requests the following accounting language in any Commission order approving the Company's Resiliency Plan:

CenterPoint Houston may defer all or a portion of the distribution-related costs relating to the implementation of the Company's Resiliency Plan for future recovery as a regulatory asset, including depreciation expense and carrying costs at the Company's weighted average cost of capital established in the Commission's final order in the Company's most recent base rate proceeding, and use Commission-authorized cost recovery alternatives under 16 TAC §§ 25.239 and 25.243 or another general rate proceeding.

Persons with questions or who want more information about the Application may contact CenterPoint Houston at 1111 Louisiana Street, Houston, Texas 77002, or by calling Stacey Murphree at 713-207-6537. A complete copy of the filing will be available for inspection at the address listed above and at the Company's offices in Austin, Texas. In addition, questions may be sent to stacey.murphree@centerpointenergy.com.

Persons who wish to intervene in or comment upon these proceedings should notify the Commission as soon as possible, as an intervention deadline will be established. A request to intervene or for further information should be mailed to the Public Utility Commission of Texas, P.O. Box 13326, Austin, Texas 78711-3326. Further information may also be obtained by calling the Commission at (512) 936-7120 or (888) 782-8477. Hearing- and speech-impaired individuals with text telephones (TTY) may contact the Commission at (512) 936-7136. The deadline for intervention in the proceeding is 30 days after the date the Application was filed with the Commission. The 30th day after the date that the Company filed its Application is May 29, 2024.

DOCKET NO. 56548

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

PROTECTIVE ORDER

This Protective Order shall govern the use of all information deemed confidential (Protected Materials) or highly confidential (Highly Sensitive Protected Materials) by a party providing information to the Public Utility Commission of Texas (Commission), including information whose confidentiality is currently under dispute.

It is ORDERED that:

1. Designation of Protected Materials. Upon producing or filing a document, including, but not limited to, records stored or encoded on a computer disk or other similar electronic storage medium in this proceeding, the producing party may designate that document, or any portion of it, as confidential pursuant to this Protective Order by typing or stamping on its face “PROTECTED PURSUANT TO PROTECTIVE ORDER ISSUED IN DOCKET NO. 56548” or words to this effect and consecutively Bates Stamping each page. Protected Materials and Highly Sensitive Protected Materials include not only the documents so designated, but also the substance of the information contained in the documents and any description, report, summary, or statement about the substance of the information contained in the documents.
2. Materials Excluded from Protected Materials Designation. Protected Materials shall not include any information or document contained in the public files of the Commission or any other federal or state agency, court, or local governmental authority subject to the Texas Public Information Act. Protected Materials also shall not include documents or information which at the time of, or prior to disclosure in a proceeding, is or was public knowledge, or which becomes public knowledge other than through disclosure in violation of this Protective Order.

3. Reviewing Party. For the purposes of this Protective Order, a Reviewing Party is a party to this docket.
4. Procedures for Designation of Protected Materials. On or before the date the Protected Materials or Highly Sensitive Protected Materials are provided to the Commission, the producing party shall file with the Commission and deliver to each party to the proceeding a written statement, which may be in the form of an objection, indicating: (1) any and all exemptions to the Public Information Act, Tex. Gov't. Code Ann., Chapter 552, claimed to be applicable to the alleged Protected Materials; (2) the reasons supporting the providing party's claim that the responsive information is exempt from public disclosure under the Public Information Act and subject to treatment as protected materials; and (3) that counsel for the providing party has reviewed the information sufficiently to state in good faith that the information is exempt from public disclosure under the Public Information Act and merits the Protected Materials designation.
5. Persons Permitted Access to Protected Materials. Except as otherwise provided in this Protective Order, a Reviewing Party shall be permitted access to Protected Materials only through its Reviewing Representatives who have signed the Protective Order Certification Form. Reviewing Representatives of a Reviewing Party include its counsel of record in this proceeding and associated attorneys, paralegals, economists, statisticians, accountants, consultants, or other persons employed or retained by the Reviewing Party and directly engaged in these proceedings. At the request of the Commissioners or their staff, copies of Protected Materials may be produced by the Staff of the Public Utility Commission of Texas (Commission Staff) or the Commission's Office of Policy and Docket Management (OPDM) to the Commissioners. The Commissioners and their staff shall be informed of the existence and coverage of this Protective Order and shall observe the restrictions of the Protective Order.
6. Highly Sensitive Protected Material Described. The term Highly Sensitive Protected Materials is a subset of Protected Materials and refers to documents or information which

a producing party claims is of such a highly sensitive nature that making copies of such documents or information or providing access to such documents to employees of the Reviewing Party (except as set forth herein) would expose a producing party to unreasonable risk of harm, including but not limited to: (1) customer-specific information protected by § 32.101(c) of the Public Utility Regulatory Act; (2) contractual information pertaining to contracts that specify that their terms are confidential or which are confidential pursuant to an order entered in litigation to which the producing party is a party; (3) market-sensitive fuel price forecasts, wholesale transactions information and/or market-sensitive marketing plans; and (4) business operations or financial information that is commercially sensitive. Documents or information so classified by a producing party shall bear the designation “HIGHLY SENSITIVE PROTECTED MATERIALS PROVIDED PURSUANT TO PROTECTIVE ORDER ISSUED IN DOCKET NO. 56548” or words to this effect and shall be consecutively Bates Stamped in accordance with the provisions of this Protective Order. The provisions of this Protective Order pertaining to Protected Materials also apply to Highly Sensitive Protected Materials, except where this Protective Order provides for additional protections for Highly Sensitive Protected Materials. In particular, the procedures herein for challenging the producing party’s designation of information as Protected Materials also apply to information that a producing party designates as Highly Sensitive Protected Materials.

7. Restrictions on Copying and Inspection of Highly Sensitive Protected Material. Except as expressly provided herein, only one copy may be made of any Highly Sensitive Protected Materials except that additional copies may be made in order to have sufficient copies for introduction of the material into the evidentiary record if the material is to be offered for admission into the record. A record of any copies that are made of Highly Sensitive Protected Material shall be kept and a copy of the record shall be sent to the producing party at the time the copy or copies are made. The record shall include information on the location and the person in possession of the copy. Highly Sensitive Protected Material

shall be made available for inspection only at the location or locations provided by the producing party, except as provided by Paragraph 9. Limited notes may be made of Highly Sensitive Protected Materials, and such notes shall themselves be treated as Highly Sensitive Protected Materials unless such notes are limited to a description of the document and a general characterization of its subject matter in a manner that does not state any substantive information contained in the document.

8. Restricting Persons Who May Have Access to Highly Sensitive Protected Material. With the exception of Commission Staff, the Office of Public Utility Counsel (OPC), and the Office of the Attorney General (OAG) when the OAG is representing a party to the proceeding and except as provided herein, the Reviewing Representatives for the purpose of access to Highly Sensitive Protected Materials may be persons who are: (1) outside counsel for the Reviewing Party; (2) outside consultants for the Reviewing Party working under the direction of Reviewing Party's counsel; or (3) employees of the Reviewing Party working with and under the direction of Reviewing Party's counsel who have been authorized by the presiding officer to review Highly Sensitive Protected Materials. The Reviewing Party shall limit the number of Reviewing Representatives that review each Highly Sensitive Protected document to the minimum number of persons necessary. The Reviewing Party is under a good faith obligation to limit access to each portion of any Highly Sensitive Protected Materials to two Reviewing Representatives whenever possible. Reviewing Representatives for Commission Staff, OAG and OPC, for the purpose of access to Highly Sensitive Protected Materials, shall consist of their respective counsel of record in this proceeding and associated attorneys, paralegals, economists, statisticians, accountants, consultants, or other persons employed or retained by them and directly engaged in these proceedings.
9. Copies Provided of Highly Sensitive Protected Material. A producing party shall provide one copy of Highly Sensitive Protected Materials specifically requested by the Reviewing Party to the person designated by the Reviewing Party who must be a person authorized to

review Highly Sensitive Protected Material under Paragraph 8 and be either outside counsel or an outside consultant. Other representatives of the reviewing party who are authorized to view Highly Sensitive Material may review the copy of Highly Sensitive Protected Materials at the office of the Reviewing Party's representative designated to receive the information. Any Highly Sensitive Protected documents provided to a Reviewing Party may not be copied except as provided in Paragraph 7 and shall be returned along with any copies made pursuant to Paragraph 7 to the producing party within two weeks after the close of the evidence in this proceeding. The restrictions contained herein do not apply to Commission Staff, OPC, and the OAG when the OAG is representing a party to the proceeding.

10. Procedures in Paragraphs 10-14 Apply to Commission Staff, OPC, and the OAG and Control in the Event of Conflict. The procedures set forth in Paragraphs 10 through 14 apply to responses to requests for documents or information that the producing party designates as Highly Sensitive Protected Materials and provides to Commission Staff, OPC, and the OAG in recognition of their purely public functions. To the extent the requirements of Paragraphs 10 through 14 conflict with any requirements contained in other paragraphs of this Protective Order, the requirements of these Paragraphs shall control.
11. Copy of Highly Sensitive Protected Material to be Provided to Commission Staff, OPC, and the OAG. When, in response to a request for information by a Reviewing Party, the producing party makes available for review documents or information claimed to be Highly Sensitive Protected Materials, the producing party shall also deliver one copy of the Highly Sensitive Protected Materials to the Commission Staff, OPC (if OPC is a party), and the OAG (if the OAG is representing a party) in Austin, Texas. Provided however, that in the event such Highly Sensitive Protected Materials are voluminous, the materials will be made available for review by Commission Staff, OPC (if OPC is a party), and the OAG (if the OAG is representing a party) at the designated office in Austin, Texas. The Commission

Staff, OPC (if OPC is a party), and the OAG (if the OAG is representing a party) may request such copies as are necessary of such voluminous material under the copying procedures set forth herein.

12. Delivery of the Copy of Highly Sensitive Protected Material to Staff and Outside Consultants. The Commission Staff, OPC (if OPC is a party), and the OAG (if the OAG is representing a party) may deliver the copy of Highly Sensitive Protected Materials received by them to the appropriate members of their staff for review, provided such staff members first sign the certification provided in Paragraph 15. After obtaining the agreement of the producing party, Commission Staff, OPC, and the OAG (if the OAG is representing a party) may deliver the copy of Highly Sensitive Protected Materials received by it to the agreed, appropriate members of their outside consultants for review, provided such outside consultants first sign the certification attached hereto.
13. Restriction on Copying by Commission Staff, OPC, and the OAG. Except as allowed by Paragraph 7, Commission Staff, OPC, and the OAG may not make additional copies of the Highly Sensitive Protected Materials furnished to them unless the producing party agrees in writing otherwise, or, upon a showing of good cause, the Presiding Officer directs otherwise. Limited notes may be made by Commission Staff, OPC (if OPC is a party), and the OAG (if the OAG is representing a party) of Highly Sensitive Protected Materials furnished to them and all such handwritten notes will be treated as Highly Sensitive Protected Materials as are the materials from which the notes are taken.
14. Public Information Requests. In the event of a request for any of the Highly Sensitive Protected Materials under the Public Information Act, an authorized representative of the Commission, OPC, or the OAG may furnish a copy of the requested Highly Sensitive Protected Materials to the Open Records Division at the OAG together with a copy of this Protective Order after notifying the producing party that such documents are being furnished to the OAG. Such notification may be provided simultaneously with the delivery of the Highly Sensitive Protected Materials to the OAG.

15. Required Certification. Each person who inspects the Protected Materials shall, before such inspection, agree in writing to the following certification set forth in the attachment to this Protective Order:

I certify my understanding that the Protected Materials are provided to me pursuant to the terms and restrictions of the Protective Order in this docket, and that I have been given a copy of it and have read the Protective Order and agree to be bound by it. I understand that the contents of the Protected Materials, any notes, memoranda, or any other form of information regarding or derived from the Protected Materials shall not be disclosed to anyone other than in accordance with the Protective Order and unless I am an employee of Commission Staff or OPC shall be used only for the purpose of the proceeding in Docket No. 56548. I acknowledge that the obligations imposed by this certification are pursuant to such Protective Order. Provided, however, if the information contained in the Protected Materials is obtained from independent public sources, the understanding stated herein shall not apply.

In addition, Reviewing Representatives who are permitted access to Highly Sensitive Protected Material under the terms of this Protective Order shall, before inspection of such material, agree in writing to the following certification set forth in the Attachment to this Protective Order:

I certify that I am eligible to have access to Highly Sensitive Protected Material under the terms of the Protective Order in this docket.

A copy of each signed certification shall be provided by the reviewing party to counsel for the producing party and served upon all parties of record.

16. Disclosures Between Reviewing Representatives and Continuation of Disclosure Restrictions After a Person is no Longer Engaged in the Proceeding. Any Reviewing Representative may disclose Protected Materials, other than Highly Sensitive Protected Materials, to any other person who is a Reviewing Representative provided that, if the person to whom disclosure is to be made has not executed and provided for delivery of a

signed certification to the party asserting confidentiality, that certification shall be executed prior to any disclosure. A Reviewing Representative may disclose Highly Sensitive Protected Material to other Reviewing Representatives who are permitted access to such material and have executed the additional certification required for persons who receive access to Highly Sensitive Protected Material. In the event that any Reviewing Representative to whom Protected Materials are disclosed ceases to be engaged in these proceedings, access to Protected Materials by that person shall be terminated and all notes, memoranda, or other information derived from the Protected Material shall either be destroyed or given to another Reviewing Representative of that party who is authorized pursuant to this Protective Order to receive the protected materials. Any person who has agreed to the foregoing certification shall continue to be bound by the provisions of this Protective Order so long as it is in effect, even if no longer engaged in these proceedings.

17. Producing Party to Provide One Copy of Certain Protected Material and Procedures for Making Additional Copies of Such Materials. Except for Highly Sensitive Protected Materials, which shall be provided to the Reviewing Parties pursuant to Paragraph 9, and voluminous Protected Materials, the producing party shall provide a Reviewing Party one copy of the Protected Materials upon receipt of the signed certification described in Paragraph 15. Except for Highly Sensitive Protected Materials, a Reviewing Party may make further copies of Protected Materials for use in this proceeding pursuant to this Protective Order, but a record shall be maintained as to the documents reproduced and the number of copies made, and upon request the Reviewing Party shall provide the party asserting confidentiality with a copy of that record.
18. Procedures Regarding Voluminous Protected Materials. Production of voluminous Protected Materials will be governed by 16 Tex. Admin. Code § 22.144(h). Voluminous Protected Materials will be made available in the producing party's voluminous room, in Austin, Texas, or at a mutually agreed upon location, Monday through Friday, 9:00 a.m. to

5:00 p.m. (except on state or Federal holidays), and at other mutually convenient times upon reasonable request.

19. Reviewing Period Defined. The Protected Materials may be reviewed only during the Reviewing Period, which shall commence upon entry of this Protective Order and continue until the expiration of the Commission's plenary jurisdiction. The Reviewing Period shall reopen if the Commission regains jurisdiction due to a remand as provided by law. Protected materials that are admitted into the evidentiary record or accompanying the evidentiary record as offers of proof may be reviewed throughout the pendency of this proceeding and any appeals.
20. Procedures for Making Copies of Voluminous Protected Materials. Other than Highly Sensitive Protected Materials, Reviewing Parties may take notes regarding the information contained in voluminous Protected Materials made available for inspection or they may make photographic, mechanical, or electronic copies of the Protected Materials, subject to the conditions hereof; provided, however, that before photographic, mechanical, or electronic copies can be made, the Reviewing Party seeking photographic, mechanical, or electronic copies must complete a written receipt for copies on the attached form identifying each piece of Protected Materials or portions thereof the Reviewing Party will need.
21. Protected Materials to be Used Solely for the Purposes of These Proceedings. All Protected Materials shall be made available to the Reviewing Parties and their Reviewing Representatives solely for the purposes of these proceedings. Access to the Protected Materials may not be used in the furtherance of any other purpose, including, without limitation: (1) any other pending or potential proceeding involving any claim, complaint, or other grievance of whatever nature, except appellate review proceedings that may arise from or be subject to these proceedings; or (2) any business or competitive endeavor of whatever nature. Because of their statutory regulatory obligations, these restrictions do not apply to Commission Staff or OPC.

22. Procedures for Confidential Treatment of Protected Materials and Information Derived from those Materials. Protected Materials, as well as a Reviewing Party's notes, memoranda, or other information regarding or derived from the Protected Materials are to be treated confidentially by the Reviewing Party and shall not be disclosed or used by the Reviewing Party except as permitted and provided in this Protective Order. Information derived from or describing the Protected Materials shall be maintained in a secure place and shall not be placed in the public or general files of the Reviewing Party except in accordance with the provisions of this Protective Order. A Reviewing Party must take all reasonable precautions to ensure that the Protected Materials including notes and analyses made from Protected Materials that disclose Protected Materials are not viewed or taken by any person other than a Reviewing Representative of a Reviewing Party.
23. Procedures for Submission of Protected Materials. If a Reviewing Party tenders for filing any Protected Materials, including Highly Sensitive Protected Materials, or any written testimony, exhibit, brief, motion, or other type of pleading or other submission at the Commission or before any other judicial body that quotes from Protected Materials or discloses the content of Protected Materials, the confidential portion of such submission shall be filed and served in sealed envelopes or other appropriate containers endorsed to the effect that they contain Protected Material or Highly Sensitive Protected Material and are sealed pursuant to this Protective Order. If filed at the Commission, such documents shall be marked "PROTECTED MATERIAL" and shall be filed under seal with the Presiding Officer and served under seal to the counsel of record for the Reviewing Parties. The Presiding Officer may subsequently, on his/her own motion or on motion of a party, issue a ruling respecting whether or not the inclusion, incorporation or reference to Protected Materials is such that such submission should remain under seal. If filing before a judicial body, the filing party: (1) shall notify the party which provided the information within sufficient time so that the providing party may seek a temporary sealing order; and

(2) shall otherwise follow the procedures set forth in Rule 76a, Texas Rules of Civil Procedure.

24. Maintenance of Protected Status of Materials During Pendency of Appeal of Order Holding Materials are Not Protected Materials. In the event that the Presiding Officer at any time in the course of this proceeding finds that all or part of the Protected Materials are not confidential or proprietary, by finding, for example, that such materials have entered the public domain or materials claimed to be Highly Sensitive Protected Materials are only Protected Materials, those materials shall nevertheless be subject to the protection afforded by this Protective Order for three (3) full working days, unless otherwise ordered, from the date the party asserting confidentiality receives notice of the Presiding Officer's order. Such notification will be by written communication. This provision establishes a deadline for appeal of a Presiding Officer's order to the Commission. In the event an appeal to the Commissioners is filed within those three (3) working days from notice, the Protected Materials shall be afforded the confidential treatment and status provided in this Protective Order during the pendency of such appeal. Neither the party asserting confidentiality nor any Reviewing Party waives its right to seek additional administrative or judicial remedies after the Commission's denial of any appeal.
25. Notice of Intent to Use Protected Materials or Change Materials Designation. Parties intending to use Protected Materials shall notify the other parties prior to offering them into evidence or otherwise disclosing such information into the record of the proceeding. During the pendency of Docket No. 56548 at the Commission, in the event that a Reviewing Party wishes to disclose Protected Materials to any person to whom disclosure is not authorized by this Protective Order, or wishes to have changed the designation of certain information or material as Protected Materials by alleging, for example, that such information or material has entered the public domain, such Reviewing Party shall first file and serve on all parties written notice of such proposed disclosure or request for change in designation, identifying with particularity each of such Protected Materials. A Reviewing

Party shall at any time be able to file a written motion to challenge the designation of information as Protected Materials.

26. Procedures to Contest Disclosure or Change in Designation. In the event that the party asserting confidentiality wishes to contest a proposed disclosure or request for change in designation, the party asserting confidentiality shall file with the appropriate Presiding Officer its objection to a proposal, with supporting affidavits, if any, within five (5) working days after receiving such notice of proposed disclosure or change in designation. Failure of the party asserting confidentiality to file such an objection within this period shall be deemed a waiver of objection to the proposed disclosure or request for change in designation. Within five (5) working days after the party asserting confidentiality files its objection and supporting materials, the party challenging confidentiality may respond. Any such response shall include a statement by counsel for the party challenging such confidentiality that he or she has reviewed all portions of the materials in dispute and without disclosing the Protected Materials, a statement as to why the Protected Materials should not be held to be confidential under current legal standards, or alternatively that the party asserting confidentiality for some reason did not allow such counsel to review such materials. If either party wishes to submit the material in question for in camera inspection, it shall do so no later than five (5) working days after the party challenging confidentiality has made its written filing.
27. Procedures for Presiding Officer Determination Regarding Proposed Disclosure or Change in Designation. If the party asserting confidentiality files an objection, the appropriate Presiding Officer will determine whether the proposed disclosure or change in designation is appropriate. Upon the request of either the producing or reviewing party or upon the Presiding Officer's own initiative, the presiding officer may conduct a prehearing conference. The burden is on the party asserting confidentiality to show that such proposed disclosure or change in designation should not be made. If the Presiding Officer determines that such proposed disclosure or change in designation should be made, disclosure shall

not take place earlier than three (3) full working days after such determination unless otherwise ordered. No party waives any right to seek additional administrative or judicial remedies concerning such Presiding Officer's ruling.

28. Maintenance of Protected Status During Periods Specified for Challenging Various Orders.

Any party electing to challenge, in the courts of this state, a Commission or Presiding Officer determination allowing disclosure or a change in designation shall have a period of ten (10) days from: (1) the date of an unfavorable Commission order; or (2) if the Commission does not rule on an appeal of an interim order, the date an appeal of an interim order to the Commission is overruled by operation of law, to obtain a favorable ruling in state district court. Any party challenging a state district court determination allowing disclosure or a change in designation shall have an additional period of ten (10) days from the date of the order to obtain a favorable ruling from a state appeals court. Finally, any party challenging a determination of a state appeals court allowing disclosure or a change in designation shall have an additional period of ten (10) days from the date of the order to obtain a favorable ruling from the state supreme court, or other appellate court. All Protected Materials shall be afforded the confidential treatment and status provided for in this Protective Order during the periods for challenging the various orders referenced in this Paragraph. For purposes of this Paragraph, a favorable ruling of a state district court, state appeals court, supreme court or other appellate court includes any order extending the deadlines set forth in this Paragraph.

29. Other Grounds for Objection to Use of Protected Materials Remain Applicable. Nothing

in this Protective Order shall be construed as precluding any party from objecting to the use of Protected Materials on grounds other than confidentiality, including the lack of required relevance. Nothing in this Protective Order constitutes a waiver of the right to argue for more disclosure, provided, however, that unless and until such additional disclosure is ordered by the Commission or a court, all parties will abide by the restrictions imposed by the Protective Order.

30. Protection of Materials from Unauthorized Disclosure. All notices, applications, responses, or other correspondence shall be made in a manner, which protects Protected Materials from unauthorized disclosure.
31. Return of Copies of Protected Materials and Destruction of Information Derived from Protected Materials. Following the conclusion of these proceedings, each Reviewing Party must, no later than thirty (30) days following receipt of the notice described below, return to the party asserting confidentiality all copies of the Protected Materials provided by that party pursuant to this Protective Order and all copies reproduced by a Reviewing Party, and counsel for each Reviewing Party must provide to the party asserting confidentiality a letter by counsel that, to the best of his or her knowledge, information, and belief, all copies of notes, memoranda, and other documents regarding or derived from the Protected Materials (including copies of Protected Materials) that have not been so returned, if any, have been destroyed, other than notes, memoranda, or other documents which contain information in a form which, if made public, would not cause disclosure of the substance of Protected Materials. As used in this Protective Order, “conclusion of these proceedings” refers to the exhaustion of available appeals, or the running of the time for the making of such appeals, as provided by applicable law. If, following any appeal, the Commission conducts a remand proceeding, then the “conclusion of these proceedings” is extended by the remand to the exhaustion of available appeals of the remand, or the running of the time for making such appeals of the remand, as provided by applicable law. Promptly following the conclusion of these proceedings, counsel for the party asserting confidentiality will send a written notice to all other parties, reminding them of their obligations under this Paragraph. Nothing in this Paragraph shall prohibit counsel for each Reviewing Party from retaining two (2) copies of any filed testimony, brief, application for rehearing, hearing exhibit, or other pleading which refers to Protected Materials provided that any such Protected Materials retained by counsel shall remain subject to the provisions of this Protective Order.

32. Applicability of Other Law. This Protective Order is subject to the requirements of the Public Information Act, the Open Meetings Act, and any other applicable law, provided that parties subject to those acts will give the party asserting confidentiality notice, if possible under those acts, prior to disclosure pursuant to those acts.
33. Procedures for Release of Information Under Order. If required by order of a governmental or judicial body, the Reviewing Party may release to such body the confidential information required by such order; provided, however, that: (1) the Reviewing Party shall notify the party asserting confidentiality of such order at least five (5) calendar days in advance of the release of the information in order for the party asserting confidentiality to contest any release of the confidential information; (2) the Reviewing Party shall notify the producing party that there is a request for such information within five (5) calendar days of the date the Reviewing Party is notified of the request for information; and (3) the Reviewing Party shall use its best efforts to prevent such materials from being disclosed to the public. The terms of this Protective Order do not preclude the Reviewing Party from complying with any valid and enforceable order of a state or federal court with competent jurisdiction specifically requiring disclosure of Protected Materials earlier than contemplated herein.
34. Best Efforts Defined. The term “best efforts” as used in the preceding paragraph requires that the Reviewing Party attempt to ensure that disclosure is not made unless such disclosure is pursuant to a final order of a Texas governmental or Texas judicial body or written opinion of the Texas Attorney General which was sought in compliance with the Public Information Act. The Reviewing Party is not required to delay compliance with a lawful order to disclose such information but is simply required to timely notify the party asserting confidentiality, or its counsel, that it has received a challenge to the confidentiality of the information and that the Reviewing Party will either proceed under the provisions of § 552.301 of the Public Information Act, or intends to comply with the final governmental or court order.

35. Notify Defined. Notify, for purposes of Paragraphs 33 and 34, shall mean written notice to the party asserting confidentiality at least five (5) calendar days prior to release; including when a Reviewing Party receives a request under the Public Information Act. However, the Commission, OAG or OPC may provide a copy of Protected Materials to the Open Records Division of the OAG as provided herein.
36. Requests for Non-Disclosure. If the producing party asserts that the requested information should not be disclosed at all, or should not be disclosed to certain parties under the protection afforded by this Order, the producing party shall tender the information for in camera review to the presiding officers within ten (10) calendar days of the request. At the same time, the producing party shall file and serve on all parties its argument, including any supporting affidavits, in support of its position of non-disclosure. The burden is on the producing party to establish that the material should not be disclosed. The producing party shall serve a copy of the information under the classification of Highly Sensitive Protected Material to all parties requesting the information that the producing party has not alleged should be prohibited from reviewing the information. Parties wishing to respond to the producing party's argument for non-disclosure shall do so within five working days. Responding parties should explain why the information should be disclosed to them, including why disclosure is necessary for a fair adjudication of the case if the material is determined to constitute a trade secret. If the Presiding Officer finds that the information should be disclosed as Protected Material under the terms of this Protective Order, the Presiding Officer shall stay the order of disclosure for such period of time as the Presiding Officer deems necessary to allow the producing party to appeal the ruling to the commission.
37. Sanctions Available for Abuse of Designation. If the Presiding Officer finds that a producing party unreasonably designated material as Protected Material or as Highly Sensitive Protected Material, or unreasonably attempted to prevent disclosure pursuant to

Paragraph 36, the Presiding Officer may sanction the producing party pursuant to 16 Tex. Admin. Code § 22.161.

38. Modification of Protective Order. Each party shall have the right to seek changes in this Protective Order as appropriate from the Presiding Officer.
39. Breach of Protective Order. In the event of a breach of the provisions of this Protective Order, the producing party, if it sustains its burden of proof required to establish the right to injunctive relief, shall be entitled to an injunction against such breach without any requirements to post bond as a condition of such relief. The producing party shall not be relieved of proof of any element required to establish the right to injunctive relief. In addition to injunctive relief, the producing party shall be entitled to pursue any other form of relief to which it is entitled.

Protective Order Certification

I certify my understanding that the Protected Materials are provided to me pursuant to the terms and restrictions of the Protective Order in this docket, and that I have been given a copy of it and have read the Protective Order and agree to be bound by it. I understand that the contents of the Protected Materials, any notes, memoranda, or any other form of information regarding or derived from the Protected Materials shall not be disclosed to anyone other than in accordance with the Protective Order and unless I am an employee of Commission Staff or OPC shall be used only for the purpose of the proceeding in Docket No. 56548. I acknowledge that the obligations imposed by this certification are pursuant to such Protective Order. Provided, however, if the information contained in the Protected Materials is obtained from independent public sources, the understanding stated herein shall not apply.

Signature

Party Represented

Printed Name

Date

I certify that I am eligible to have access to Highly Sensitive Protected Material under the terms of the Protective Order in this docket.

Signature

Party Represented

Printed Name

Date

DOCKET NO. 56548

I request to view/copy the following documents:

<u>Document Requested</u>	<u># of Copies</u>	<u>Non-Confidential</u>	<u>Confidential and/or H.S.</u>

Signature

Party Represented

Printed Name

Date