RESILIENCY INVESTMENTS TO CUSTOMERS AND COMMUNITIES SERVED BY CENTERPOINT HOUSTON.

A. Guidehouse found evidence of resiliency measure effectiveness for each of the five technology resiliency measures and two situational awareness resiliency measures (see Section V for details) that add potential value to customers and communities served by CenterPoint Houston. The Network Security & Vulnerability Management (RM-30) and IT/OT – Cybersecurity Monitoring Program (RM-31) resiliency measure investments provide direct value to consumers and communities by improving CenterPoint Houston's ability to detect, deter, and defend against cyber attacks that could adversely impact CenterPoint Houston's electric delivery system. The Spectrum Acquisition (RM-28) and Cloud Security, Product Security & Risk Management (RM-32) resiliency measures also provide direct value as enabling technologies to support a resilient electrical distribution system, as well as efficient and effective customer services. The two situational awareness resiliency measures, Voice & Mobile Data Radio System (RM-36) and Backhaul Microwave Communications (RM-37) will provide upgraded communications capability to facilitate and expedite system restoration efforts for weather related and other resiliency events, as described in Mr. Shlatz' testimony. The final technology resiliency measure, Data Center Modernization (RM-29), replaces end-of-life systems with upgraded functionality, including predictive maintenance, asset management, and other critical functions, and includes a proposed redundant Advanced Distribution Management System and SCADA communications link that increase CenterPoint Houston's capabilities within its operating environment. In summation, Guidehouse found the five technology resiliency measures and the two situational awareness resiliency measures provide more effective operational capabilities and represent diverse resiliency investments and enabling

technologies that add significant benefits and potential value to customers and communities served by CenterPoint Houston.

iii. BENCHMARKING ANALYSIS

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 pertinent to each of CenterPoint Houston's proposed technology resiliency measures are presented below.

Q. PLEASE SUMMARIZE THE FINDINGS OF THE JURISDICTIONAL BENCHMARKING REPORT AND HOW THIS PROVIDES AN INDICATOR OF INDUSTRY BEST PRACTICES FOR TECHNOLOGY RESILEINCY 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 and the two situational awareness 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 Modernization 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 Data Radio System resiliency measure (see Ameren example)]

iv. RESILIENCY MEASURE ASSESSMENT

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

A. My assessment of each CenterPoint Houston technology or cybersecurity resiliency measure is presented in my responses to the following seven sets of questions, in the order presented below. For each resiliency measure, I summarize my assessment and conclusions drawn from the Guidehouse report.

- Spectrum Acquisition (RM-28)
- Data Center Modernization (RM-29)
- Network Security & Vulnerability Management (RM-30)
- IT/OT – Cybersecurity Monitoring Program (RM-31)
- Cloud Security, Product Security & Risk Management (RM-32)
- Voice and Mobile Data Radio System Refresh (RM-36)
- Backhaul Microwave Communication (RM-37)

Additional details and comprehensive analyses of these seven resiliency measures can be found in ELS-2.

Q. PLEASE DESCRIBE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S SPECTRUM ACQUISITION (RM-28) RESILIENCY MEASURE.

A. Based on information provided by CEHE, Guidehouse gained a reasonable assurance the Spectrum Acquisition resiliency measure is needed to support grid modernization projects and determined CEHE can obtain significant benefits in a cost-effective manner through the implementation of the Spectrum Acquisition resiliency measure. Overall, the Spectrum Acquisition resiliency measure exhibited strong correlation with NIST CSF subcategories: PR-DS-02 (higher security for data in transit over private networks) and PR.IS-04 (ensuring adequate resource capacity). Guidehouse further concluded that CenterPoint's Spectrum Acquisition resiliency measure is justified with regard to a demonstrated need for higher bandwidth and lower latency rates to support grid modernization and other proposed resiliency measures. The Spectrum Acquisition resiliency measure is also supported by similar utility spectrum projects, which have been approved or are in the review process by various regulatory jurisdictions.

I concur with the Guidehouse assessment and determine the Spectrum Acquisition resiliency measure provides significant benefits for and adds resiliency to the CEHE electrical distribution system by enabling more effective communications that will meet the future needs.

Q. PLEASE DESCRIBE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S DATA CENTER MODERNIZATION (RM-29) RESILIENCY MEASURE.

A. Guidehouse concludes there is a high level of correlation with critical CSF system and business resilience and system restoration practices with CenterPoint Houston's Data

Center Modernization resiliency measure. I concur with this determination. Particular areas in which this resiliency measure supports a strong and resilient electric transmission and distribution system include enhancements in the following practice areas:

- Business Environment
- Governance
- Access Control
- Data Security
- Protective Technology
- Improvements

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

Guidehouse determined the proposed Data Center Modernization resiliency measure is consistent with resiliency practices deployed at other utilities, based on Guidehouse experience and peer utility benchmarking survey results described in ELS-2. I concur with the Guidehouse assessment and findings.

Q. PLEASE DESCRIBE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S NETWORK SECURITY& VULNERABILITY MANAGEMENT (RM-30) 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 SRP. 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.

Guidehouse determined 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 ELS-2. I concur with the Guidehouse assessment and findings.

Q. PLEASE DESCRIBE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S IT/OT CYBERSECURITY MONITORING PROGRAM (RM-31) RESILIENCY MEASURE.

A. Guidehouse concludes CenterPoint Houston's IT/OT-Cybersecurity Monitoring is reasonable and beneficial for inclusion in CenterPoint Houston's SRP. 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 Program 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 information 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.
- The IT/OT-Cybersecurity Monitoring Program 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 Program resiliency measure in their SRP. 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.

Guidehouse determined the proposed IT/OT – Cybersecurity Monitoring Program resiliency measure is consistent with resiliency practices deployed at other utilities, based on Guidehouse experience and peer utility benchmarking survey results described in ELS-2. I concur with the Guidehouse assessment and findings.

Q. PLEASE DESCRIBE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S CLOUD SECURITY, PRODUCT SECURITY & RISK MANAGEMENT (RM-32) RESILIENCY MEASURE.

A. Guidehouse concludes the proposed Product Security, Cloud Security, & Risk Management resiliency measure is justified with regard to strong correlations for proposed tools with applicable NIST CSF (v2.0) Core function subcategories (see ELS-2, Table 5-18) Guidehouse also confirmed CEHE has established a strong cybersecurity foundation by applying existing frameworks, processes, and other risk management approaches (see ELS-2, Table 5-19). Guidehouse further determined CEHE has a feasible three-year plan to expand cybersecurity protective measures and controls to enhance cybersecurity as an enabling factor and provide better resiliency to the CEHE cyber systems and associated electrical distribution system services and facilities.

Guidehouse gained a reasonable assurance the CSPSRM resiliency measure is needed to support higher operational service levels and improved resiliency for electrical system operations and determined CEHE can obtain significant benefits in a cost-effective manner through the implementation of this resiliency measure. I concur with the Guidehouse assessment and findings.

Q. PLEASE DESCRIBE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S VOICE AND MOBILE DATA RADIO SYSTEM REFRESH (RM-36) RESILIENCY MEASURE.

A. The Guidehouse team concluded that CenterPoint Houston's Voice and Mobile Data Radio System Refresh resiliency measure has a high level of correlation with system and business resilience and system restoration. This resiliency measure represents the most feasible approach to obtain the desired communications improvements in support of resiliency of CenterPoint Houston's electric system during normal and emergency operations The Voice and Mobile Data Radio System Refresh resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's SRP, as the resiliency measure supports a stronger and more resilient electric transmission and distribution system by providing:

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

In addition, Guidehouse determined that CenterPoint Houston's proposed Voice and Mobile Data Radio System Refresh resiliency measure is consistent with resiliency practices deployed at other utilities, based on Guidehouse experience and peer utility benchmarking survey results described in ELS-2.

Q. PLEASE DESCRIBE YOUR ASSESSMENT OF CENTERPOINT HOUSTON'S BACKHAUL MICROWAVE COMMUNICATION (RM-37) RESILIENCY MEASURE.

A. Guidehouse concludes that CenterPoint's IT – Backhaul Microwave Communication Resiliency measure provides resiliency benefits. I concur with this determination that CenterPoint Houston's Backhaul Microwave Communications resiliency measure is reasonable and beneficial for inclusion in CenterPoint Houston's SRP for the following reasons:

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

Guidehouse determined the proposed resiliency measure is consistent with resiliency practices deployed at other utilities, based on Guidehouse experience and peer utility benchmarking survey results described in ELS-2. I concur with the Guidehouse assessment and findings.

VI. SUMMARY OF FINDINGS AND RECOMMENDATIONS

Q. HOW DID GUIDEHOUSE DETERMINE ITS FINDINGS AND RECOMMENDATIONS ON CENTERPOINT ENERGY HOUSTON ELECTRIC'S SYSTEM 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 System 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.[30]

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

A. First, Guidehouse finds that CenterPoint Houston's SRP 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 for continued

[30] First Quartile Consulting provided peer utility benchmarking data.

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 ELS-2 indicates that proposed resiliency measures included in CenterPoint Houston's SRP are consistent with those deployed at other utilities.

In summation, I conclude the five technology resiliency measures and two situational awareness resiliency measures in CenterPoint Houston's SRP are:

- appropriate for addressing relevant physical security and cybersecurity risks and attack vectors;
- aligned with industry best practice and the NIST Cybersecurity Framework; 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 SRP for the five technology resiliency measures and two situational resiliency measures:

1. **Spectrum Acquisition (RM-28)**– Evaluate broadband spectrum options with an objective analysis tool to ensure CEHE near– and long–term goals, and other business objectives are achieved.
2. **Data Center Modernization (RM-29)** – When considering any type of data migration, ensure that all on-premises options such as application, workflow, and process optimizations are investigated to determine if they can be migrated, as

migrating data to any new environment will affect uptime, application reliability, and support overall resilience. This is due to the eccentricities of any new environment, regardless of cloud or another on premise environment.

3. **Networking, Vulnerability, and Security – Data Management (RM-30)** – 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.
4. **IT/OT-Cybersecurity Monitoring Program (RM-31)** – 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.
5. **Cloud Security, Product Security & Risk Management (RM-32)** – Develop an objective product and services evaluation tool to ensure CEHE business goals and objectives, including cybersecurity features and functionality, and supply

chain risk management are met when selecting and procuring components for installation and support of the CSPSRM resiliency measure.

6. **Voice and Mobile Data Radio System Refresh (RM-36)**– 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.
7. **Backhaul Microwave Communication (RM-37)** – 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.

I concur with these recommendations for each of the seven resiliency measures.

VII. CONCLUSION

Q. PLEASE SUMMARIZE YOUR DIRECT TESTIMONY.

A. Guidehouse reviewed the five CenterPoint Houston technology resiliency measures two situational awareness 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 SRP appropriately prioritizes technology resiliency measures and situational awareness resiliency measures that will mitigate cybersecurity risks. 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 ELS-2 indicates that proposed resiliency measures included in CenterPoint Houston's SRP are consistent with resiliency measures deployed at other utilities.

I concluded the five technology resiliency measures and two situational awareness resiliency measures in CenterPoint Houston's SRP are:

- appropriate for addressing the physical and cyber security risks and attack vectors, as described above;
- aligned with industry best practices and the NIST Cybersecurity Framework; 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

Guidehouse
Outwit Complexity

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.

Guidehouse
Outwit Complexity

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.

Guidehouse
Outwit Complexity

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 (PGAE)** (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.

Guidehouse
Outwit Complexity

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)
- 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)
- Irby Construction Company, Groundman, Apprentice Lineman, Journeyman Lineman, Foreman, Transmission power line construction projects across U.S. (1973-1980)

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)

Guidehouse
Outwit Complexity

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).

Guidehouse
Outwit Complexity

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].

Guidehouse
Outwit Complexity

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
- 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.

Guidehouse
Outwit Complexity

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.

Guidehouse
Outwit Complexity

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.revistaiic.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.revistaiic.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.

Guidehouse
Outwit Complexity

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

EXHIBIT 14

NOTICE OF SYSTEM RESILIENCY PLAN FILING

This page was intentionally left blank.

NOTICE OF SYSTEM RESILIENCY PLAN FILING

On January 31, 2025, 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 2026-2028 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. 57579.

Attached to the Application, the Company presents its three-year plan (2026-2028) for enhancing the resiliency of its transmission and distribution systems in the face of resiliency events and other resiliency-related risks (the "System Resiliency Plan"). In the System 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 thirty-nine programs or initiatives designed to prevent, withstand, mitigate, or more promptly recover from Resiliency Events (each, a "Resiliency Measure"). The Company estimates that the thirty-nine Resiliency Measures will cost approximately $5.543 billion in capital costs and $210.7 million in incremental O&M expense over the three-year period from 2026 to 2028. The table below summarizes the cost of each Resiliency Measure in the Company's System Resiliency Plan.

Figure PFN-1.
Resiliency Measures, Costs, and 3-Year CMI Savings

Resiliency Measure	Estimated Capital Costs (millions)	Estimated Incremental O&M Expense (millions)	Estimated 3-Year CMI Savings (millions)
Extreme Wind			
Distribution Circuit Resiliency (RM-1)	$513.4	-	263.0
Strategic Undergrounding (RM-2)	$860.0	-	81.1
Restoration IGSD (RM-3)	$107.3	$0.5	97.0
Distribution Pole Replacement/Bracing Program (RM-4)	$251.6	-	121.0
Vegetation Management (RM-5)	-	$146.1	137.0
Transmission System Hardening (RM-6)	$1,467.3	$0.8	223.8
69kV Conversion Projects (RM-7)	$369.3	-	65.5

Resiliency Measure	Estimated Capital Costs (millions)	Estimated Incremental O&M Expense (millions)	Estimated 3-Year CMI Savings (millions)
S90 Tower Replacements (RM-8)	$118.4	-	59.5
Coastal Resiliency Projects (RM-9)	$177.4	$0.8	7.8
Extreme Water			
Substation Flood Control (RM-10)	$43.8	-	3.9
Control Center Flood Control (RM-11)	$7.0	-	2.5
Major Underground Control and Monitoring System (MUCAMS) (RM-12)	$10.8	-	0.6
Mobile Substation (RM-13)	$30.0	-	3.9
Extreme Temperature (Freeze)			
Anti-Galloping Technologies (RM-14)	$14.0	$1.0	5.3
Load Shed IGSD (RM-15)	$4.5	$0.1	N/A
Microgrid Pilot Project (PP-1)	$35.0	$1.5	N/A
Extreme Temperature (Heat)			
Distribution Capacity Enhancements/Substations (RM-16)	$579.6	-	138.1
MUG Reconductor (RM-17)	$245.0	-	13.6
URD Cable Modernization (RM-18)	$128.4	-	13.0
Contamination Mitigation (RM-19)	$144.0	$6.0	15.7
Substation Fire Barriers (RM-20)	$9.0	-	1.5
Digital Substation (RM-21)	$31.8	-	1.2
Wildfire Advanced Analytics (RM-22)	-	$0.9	N/A
Wildfire Strategic Undergrounding (RM-23)	$50.0	-	N/A
Wildfire Vegetation Management (RM-24)	-	$30.0	N/A
Wildfire IGSD (RM-25)	$19.4	$0.3	N/A
Physical Attack			
Substation Physical Security Fencing (RM-26)	$18.0	-	17.6
Substation Security Upgrades (RM-27)	$19.4	$0.1	25.1
Technology & Cybersecurity			
Spectrum Acquisition (RM-28)	$42.0	-	N/A
Data Center Modernization (RM-29)	$12.7	$1.3	N/A
Network Security & Vulnerability Management (RM-30)	$7.5	$2.0	N/A
IT/OT Cybersecurity Monitoring (RM-31)	$13.4	$4.2	N/A
Cloud Security, Product Security & Risk Management (RM-32)	$4.0	$6.0	N/A
Situational Awareness			
Advanced Aerial Imagery Platform / Digital Twin (RM-33)	$18.4	$2.0	10.8

Resiliency Measure	Estimated Capital Costs (millions)	Estimated Incremental O&M Expense (millions)	Estimated 3-Year CMI Savings (millions)
Weather Stations (RM-34)	-	$0.3	N/A
Wildfire Cameras (RM-35)	-	$0.9	N/A
Voice and Mobile Data Radio System (RM-36)	$20.9	-	N/A
Backhaul Microwave Communication (RM-37)	$12.7	-	N/A
Emergency Operations Center (RM-38)	$50.0	$6.0	N/A
Hardened Service Centers (RM-39)	$107.6	-	N/A
Total	**$5,543.3**	**$210.7**	**1,308.6**

The Company also seeks Commission approval of a utility-scale microgrid pilot project. Lastly, as part of the Company's System Resiliency Plan, the Company requests the following accounting language in any Commission order approving the Company's System Resiliency Plan:

> Effective on the earlier of the date of a final order in this proceeding or January 1, 2026, CenterPoint Houston may defer all or a portion of the distribution-related costs relating to the implementation of the Company's System Resiliency Plan over a 3-year period for future recovery as a regulatory asset, including depreciation expense and carrying costs at the Company's weighted average cost of capital as established by the Commission's final order in the Company's most recent base rate proceeding, and use Commission-authorized cost recovery alternatives under 16 Tex. Admin. Code §§ 25.239 and 25.243 or another general rate proceeding.

The Company also requests specific accounting language that would allow the Company to defer costs associated with distribution-related vegetation management costs relating to the implementation of the Company's System Resiliency Plan. The Company requests the following language in any Commission order approving the Company's System Resiliency Plan:

> Effective on the earlier of the date of a final order in this proceeding or January 1, 2026, CenterPoint Houston may defer the annual incremental distribution-related vegetation management costs relating to the implementation of the Company's System Resiliency Plan over a 3-year period for future recovery as a regulatory asset, including 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 Tex. Admin. Code §§ 25.239 and 25.243 or another general rate

proceeding. The annual baseline amount that will be used to determine the annual incremental distribution-related vegetation management costs shall be $46 million. Annual distribution-related vegetation management costs that exceed the annual baseline amount of $46 million shall be considered the annual incremental distribution-related vegetation management costs relating to the implementation of the Company's System Resiliency Plan and thus eligible to be deferred for future recovery as a regulatory asset.

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 March 2, 2025.

EXHIBIT 15

PROTECTIVE ORDER

This page was intentionally left blank.

DOCKET NO. 57579

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

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. 57579" 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. 57579" 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. 57579. 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 Protected 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. 57579 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. 57579. 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

I request to view/copy the following documents:

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

Signature

Party Represented

Printed Name

Date

The following files are not convertible:

WP MA-1 Texas T&D provider rate history and inflation.xlsx
WP MA-2 Texas affordability metrics.xlsx
WP MA-3 Projection of Impact to Customer Bills.xlsx
WP MA-4 Storm Restoration Spend.xlsx
WP MA-5 Major storms impacting the greater Houston area.xlsx
WP MA-6 FPL Hurricane Savings.xlsx
WP MA-7 Estimation of Houston Diabetics.xlsx
WP MA-8 Cost of fast food vs cooking at home.xlsx
WP MA-9 Houston hourly workers information.xlsx
WP MA-10 Houston GDP and Jobs by sector.xlsx
WP MA-11 Port of Houston dollars and containers disrupted.xlsx
WP MA-12 Data center investment totals.xlsx
WP MA-13 Hydrogen projects tracker.xlsx

Please see the ZIP file for this Filing on the PUC Interchange in order to access these files.

Contact centralrecords@puc.texas.gov if you have any questions.