



Filing Receipt

Filing Date - 2025-03-26 02:28:00 PM

Control Number - 57579

Item Number - 119

**SOAH DOCKET NO. 473-25-11558
PUC DOCKET NO. 57579**

APPLICATION OF CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC FOR APPROVAL OF ITS 2026-2028 TRANSMISSION AND DISTRIBUTION SYSTEM RESILIENCY PLAN	§ § § § §	BEFORE THE STATE OFFICE OF ADMINISTRATIVE HEARINGS
---	-----------------------	---

March 26, 2025

**Contact: Stacey Murphree
CenterPoint Energy Service Company, LLC
1111 Louisiana Street
Houston, Texas 77002
Telephone No: (713) 207-6537
Fax: (713) 454-7197
stacey.murphree@centerpointenergy.com**

TABLE OF CONTENTS

<u>Description</u>	<u>Page</u>
CenterPoint Energy Houston Electric, LLC's Responses to Office of Public Utility Counsel Fourth Set of RFIs.....	2-19
Certificate of Service	20

**CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558**

**OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RFI04-01**

QUESTION:

Please explain whether Presidential Policy Directive 21 ("PPD-21 ") enumerates specific hazards that should be protected against

ANSWER:

PPD-21, superseded by National Security Memorandum 22 (NSM-22), establishes new policy positions and objectives for federal agencies to protect US critical infrastructure, including calls for the creation of sector-specific minimum security and resilience requirements. However, it did not specifically identify new hazards for critical infrastructure operators/owners or impose any additional requirements or responsibilities on operators/owners.

SPONSOR:

Chris Ford

RESPONSIVE DOCUMENTS:

None

CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558

OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RF104-02

QUESTION:

For the following cyber attack categories, please explain whether the Company has experienced specific attacks utilizing that specific attack vector over the past five years:

- a. Ransomware;
- b. Distributed Denial of Service;
- c. Malware;
- d. Phishing;
- e. Exploitation of known but unpatched vulnerabilities;
- f. Social Engineering;
- g. Supply Chain Attacks;
- h. System misconfigurations;
- i. Missing or Poor encryption practices;
- j. Insider threats; and
- k. External actor threats via physical or cyber attacks.

Based on an agreement with OPUC, the Company is answering the revised question below.

What are the Company's processes and practices as it relates to:

- a. Responding to cyber attacks;
- b. Monitoring cyber attack vectors; and
- c. Assessing emerging cyber attack vectors.

ANSWER:

- a. The company's position on responding to cyber attacks is centered around minimizing the business impact through early detection and remediation. The Cyber Security Operations Center (CSOC) is dedicated to monitoring and responding to cybersecurity events that could threaten the confidentiality, integrity, or availability of company data or systems.

In terms of practical measures, the company is implementing a standardized security stack across sites to detect operational technology (OT) cybersecurity threats. This includes passive sensors and firewalls, integration of security operations centers to include IT, OT, and physical security, and functional testing of equipment and software within the security stack before deployment.

- b. The Cyber Security Operations Center (CSOC) plays a crucial role in monitoring and responding to cybersecurity threats. CSOC's monitoring is informed by the company's membership in various Information Sharing and Analyst Centers (ISACs) and private threat intelligence sources. Using this threat intelligence, user behavioral analytics and pattern analysis, the CSOC analyzes various attack vectors for threats to the company's assets.
- c. The company's process for assessing emerging cyber attack vectors includes threat modeling, threat landscape monitoring and collaboration with industry peers via ISACs.

SPONSOR:
Chris Ford

RESPONSIVE DOCUMENTS:
None

**CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558**

**OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RFI04-03**

QUESTION:

For any cyber attacks that occurred in the past five years, please explain whether a detailed forensic evaluation of the attack, including a dissection of the methodology of the attack and determination of damage potentially caused was completed. Additionally, if answering in the affirmative please provide an example of a full forensic report and please answer the following questions:

- a. Has Dr. Joseph B. Baugh ("Dr. Baugh") personally examined the forensic reports of the various incidents to gain a perspective on the typical vector used for the specific attack, the methodology used to conduct the attack, and the damage caused, as well as corrective actions taken by the company to prevent the same type of attack in the future?
- b. Are overarching metrics and trend curves (time, duration, cause, impact, etc.) of the specific cyber attack categories available demonstrating the need for the specific metrics detailed in Dr. Baugh's testimony?

ANSWER:

- a. No, a detailed forensic analysis of each cyberattack that occurred during the past five years was beyond the scope of the CNP engagement and was not performed. I did not personally examine forensic reports of the various incidents. In general, cybersecurity attacks tend to take a common set of attack vectors, depending on the specific category of attack, and specific mitigation and preventive activities are dictated by organization-specific cybersecurity incident response plans. In addition, specific information on cyberattacks is classified by organizations as highly sensitive and confidential to avoid publically sharing system vulnerabilities with those who may wish to attempt to infiltrate and or penetrate and is typically not shared beyond an extremely limited distribution range required by regulatory bodies. I prepared the threat landscape assessment based on publicly available information from credible sources, as cited in the GH SRP report (exhibit ELS-2).
- b. No. Specific cybersecurity performance metrics reflect a company's adaptability and preparedness in a dynamic digital threat landscape and highlight the importance of tracking performance and continuous improvement in cybersecurity strategies. The performance metrics identified for each technology and situational awareness resiliency measure were derived through consultation with CNP Subject Matter Experts (SMEs), based on best cybersecurity practices and integrated SME knowledge of the CNP operating environment and specific cyber system characteristics.

SPONSOR:

Dr. Joseph Baugh

RESPONSIVE DOCUMENTS:

None

**CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558**

**OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RFI04-04**

QUESTION:

Admit or deny that every cyber attack within a specific category of cyber attacks (Ransomware, Malware, etc.) all follow common attack vector methodologies. If deny, please explain.

ANSWER:

Deny. It is common knowledge in the cyber security field that cyber attack within a specific category of cyber attacks can follow multiple attack vector methodologies.

SPONSOR:

Chris Ford

RESPONSIVE DOCUMENTS:

None

**CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558**

**OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RF104-05**

QUESTION:

Admit or deny that cyber attacks continually evolve and use differing strategies, methodologies, and techniques to accomplish the specific goal of the attack vector. If deny, please explain.

ANSWER:

Admit.

SPONSOR:

Chris Ford

RESPONSIVE DOCUMENTS:

None

**CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558**

**OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RFI04-06**

QUESTION:

Admit or deny that every cyber attack must be examined for a uniqueness or evolution which enables the attack vector itself to evolve and potentially defeat existing cyber defenses. If deny, please explain.

ANSWER:

Admit. Cyber attack tactics, techniques and procedures are examined during incident response. Relevant lessons learned from each attack are used to improve the company's incident response procedure.

SPONSOR:

Chris Ford

RESPONSIVE DOCUMENTS:

None

**CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558**

**OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RFI04-07**

QUESTION:

In situations where the Company has instituted cyber practices and measures after the installation of systems and devices, please explain if it is the policy of the Company to develop a plan to re-examine those installed systems and devices for proper configuration, potential installed malware, or other threats.

ANSWER:

Yes, it is the policy of the Company to re-examine installed systems and devices for proper configuration, potential installed malware, or other threats after deployment. The company has a comprehensive approach to cybersecurity that includes regular vulnerability scanning, and post-deployment scanning of new solutions.

SPONSOR:

Chris Ford

RESPONSIVE DOCUMENTS:

None

**CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558**

**OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RF104-08**

QUESTION:

Please explain whether the Company takes the position that all electric systems are generally the same.

Based on an agreement with OPUC, the Company is answering the revised question below.

Please explain whether the Company takes the position that all information technology systems are generally the same.

ANSWER:

The company does not take the position that all information technology systems are generally the same. In fact, the company recognizes the distinct differences between Information Technology (IT) and Operational Technology (OT) systems and has tailored its cybersecurity program to address these differences. Systems also have varying degrees of risk depending on factors such as application criticality, interconnectivity and position in the network.

SPONSOR:

Chris Ford

RESPONSIVE DOCUMENTS:

None

**CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558**

**OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RFI04-09**

QUESTION:

Please explain the methodology that the Company believes would be employed in an AI-based cyberattack.

ANSWER:

The company believes the methodology employed in AI-based cyber attacks would include characteristics such as automation and speed, sophistication and adaptability and personalization.

SPONSOR:

Chris Ford

RESPONSIVE DOCUMENTS:

None

**CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558**

**OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RFI04-10**

QUESTION:

Please explain whether every electric system operator utilizes the same configurations and operating methodologies when using the same equipment.

Based on an agreement with OPUC, the Company is answering the revised question below.

Please explain whether every information technology system utilizes the same configurations and operating methodologies when using the same equipment.

ANSWER:

Configurations and operating methodology differ between Information Technology (IT) and Operational Technology (OT) systems that use the same equipment.

SPONSOR:

Chris Ford

RESPONSIVE DOCUMENTS:

None

CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558

OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RF104-11

QUESTION:

Admit or deny that a system installed in one part of the country will function exactly the same when installed identically in another part of the country. If deny, please explain. Additionally, please answer the following questions:

- a. Is it Dr. Baugh's experience that the same systems are always installed identically in every part of the country and experience the same operating factors;
- b. Is it Dr. Baugh's experience that all companies abide by the same operating methodologies with regard to their systems; and
- c. Is it Dr. Baugh's experience that data obtained from one system should be identical to data from an identical system installed identically in another part of the country?

ANSWER:

No, as each organization is different and has unique operating characteristics, personnel capabilities, organizational risk tolerance levels, and divergent threat landscapes specific to the organization's service territory and its business goals and objectives.

- a. No, while there will be numerous similarities between identical energy management systems (EMS) from the same vendor and supporting cyber system installations, sufficient variation in operating conditions exists that an absolute response either way is misleading. Organizations operating similar EMS generally face similar operating factors, but responses to cyberattacks can vary significantly for the same reasons listed in the 4-11 root response above.
- b. In general, it is my experience that electrical utilities tend to be risk-averse and adhere to cybersecurity best practices, where specific regulatory requirements do not come into play. For example, CNP's transmission EMS is regulated by the NERC CIP reliability standards, but its distribution management system (DMS) is not. Speaking specifically to CNP, the technology and situational awareness resiliency measures in its SRP are intended to apply cybersecurity best practices to ensure a defense-in-depth strategy is developed that will protect its DMS and associated cyber systems.
- c. This is another case where an absolute response may be misleading. While it is true that electrical utilities will collect similar types of data from remote sites (e.g., operational data, situational awareness data, and metering data), individual utility characteristics prevent a characterization of identical data drawn from identical systems installed in an identical manner in another part of the country. However, similar systems do face common threat vectors and systems from common manufacturers may share common-mode vulnerabilities depending on the specific system. This is the rationale for performing site-specific threat and vulnerability assessments and developing specific protective measures and controls to ensure the utility's cyber systems are protected from identified risks, threats, and vulnerabilities commensurate with the utility's cybersecurity policies, operational characteristics, and risk tolerance levels. Performing such site-specific assessments were beyond the scope of the Guidehouse engagement.

SPONSOR:

Dr. Joseph Baugh

RESPONSIVE DOCUMENTS:
None

CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558

OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RF104-12

QUESTION:

For physical ballistic damage to the Company's systems and assets in the past five years, please provide a breakdown, by year, of such incidents. Additionally, for each of the physical ballistic attacks, has Dr. Baugh or the Company examined the forensic report for each to gain perspective on the attack style, methodology, and other factors that could offer trend and specific metric information?

Based on an agreement with OPUC, the Company is answering the revised question below.

What are the Company's processes and practices as it relates to preventing, mitigating the likelihood of, monitoring, and responding to ballistic attacks?

ANSWER:

CEHE Response:

The company uses advanced modeling to prepare for physical attack events, including ballistic attacks. Additionally, the company has technology in place to detect ballistic events in real time. Any such event would active the incident response process that includes real-time operational support. This involves the use of camera and imagery tools, system and scenario modeling, advanced analytics/AI, centralized event command, and hardened service centers. To mitigate against ballistic attacks the Company employs a risk assessment process to accurately identify/determine asset criticality and the proper security posture. The Company employs concrete ballistic-resistant barriers around the control house, a Boomerang gunshot detection system, intrusion detection technology and advanced video surveillance for enhanced security countermeasures.

Guidehouse Response:

Similar to my response to item 4-3 subpart A, a detailed forensic analysis of each physical security attack that occurred during the past five years was beyond the scope of the CNP engagement and was not performed. I did not personally examine forensic reports of the various incidents. Just as with forensic analyses developed for significant cybersecurity attacks, organizations who have experienced such attacks tend to share details only as required by regulatory bodies and these details are not typically available for public consumption. However, based on my experiences auditing NERC reliability standard CIP-014, I am familiar with the characteristics of reported physical security attacks in the transmission sector of the North American electrical grid and subsequent protective measures and controls developed in response to those attacks. I applied this experience and my professional judgement to evaluate the physical security aspects of the technology and situational awareness resiliency measures to gain a reasonable assurance (see OPUC 4-13) that each such resiliency measure would provide benefits to CNP's system operations and its customers.

SPONSOR:

Chris Ford and Joseph Baugh

RESPONSIVE DOCUMENTS:

None

**CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558**

**OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RFI04-13**

QUESTION:

Referring to the Direct Testimony of Dr. Joseph B. Baugh at 34 ("Baugh Direct"), please define "reasonable assurance" as it is used to describe how a resiliency measure is required to support a grid modernization project

ANSWER:

"Reasonable assurance" is a common term used by auditors or inspectors, often associated with sampling, because gaining an absolute level of confidence may be impossible given time and resource constraints for a specific engagement. Reasonable assurance is a high level of assurance but is not a guarantee of complete accuracy or freedom from errors or fraud. Developing reasonable assurance involves a process identifying, assessing, and mitigating risks to achieve a high, but not absolute, level of confidence in a report or system, typically through an audit or risk assessment.

In this case, Guidehouse was engaged to perform qualitative comparative analyses to confirm or reject the technology and situational awareness resiliency measures proposed by CNP. Based on the documentation provided, interviews with CNP SMEs, and professional judgement, I gained a reasonable assurance that the combined set of resiliency measures would support more resilient electrical operations from a cybersecurity perspective by collectively developing a defense-in-depth strategy.

SPONSOR:

Dr. Joseph Baugh

RESPONSIVE DOCUMENTS:

None

CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558

OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RF104-14

QUESTION:

What historic trend analysis, if any, was conducted to determine both a present and future need for the Spectrum Acquisition resiliency measure? Additionally, please answer the following questions:

- a. What factors or indicators were used to determine that a demonstrated need exists for higher bandwidth;
- b. Why are lower latency rates required for grid modernization and what specific modernizations mandate the latency rates advocated in this filing;
- c. Referring to Baugh Direct at 34, wherein Dr. Baugh states that 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," please specifically list which projects Dr. Baugh refers to by Project Title, Case or Cause No, and specific regulatory jurisdiction where that project is under review or has been approved.

ANSWER:

- a. There was a formal engagement with Burns & McDonnell to perform a future (Field Area Network) FAN assessment that was provided in March 2024. There were the different networks (700MHz FAN, commercial cellular, unlicensed 900 MHz radios, land mobile radio, 900MHz paging transmitter) that were reviewed along with use cases for each network. A gap analysis was performed based on use cases forecasts for distribution automation, advanced metering infrastructure, mobile workforce, gas metering and distributed generation). The device forecasts indicate a growing number of grid devices and more use cases with some of those with higher bandwidth and reliability needs. There is no one, single existing CenterPoint Energy owned communication network solution that will support the demand of future field devices (~60,000 devices). The analysis indicates there is a device density impact that creates network challenges in handling increased data traffic, maintain reliable connectivity and provide adequate bandwidth for devices. Further, as the end-device density grows, the network planning and management becomes more difficult related to capacity constraints, especially in areas with higher end-device density. There was extrapolation based on the anticipated devices and capacity needs. The studies determined that existing CNP owned spectrum will reach capacity in 2030. Spectrum bandwidth depends on the spectrum, and current CNP spectrum will not support expected growth.
- b. Modernizations that mandate the latency rates advocated in this filing pertain to capacity constraints. Examples of devices where latency issues need to be addressed include perimeter surveillance and vegetation management, direct transfer trip and IGSD – reclosers/sectionalizer. The GenX mesh transition and the meter reading software requirements are likely to raise in the next 5-6 years. There will be more devices that require network support driven by significant new investments in the Greater Houston Resiliency Initiative. There are currently approximately 14 sites identified that have the potential for radio sector overloading in the future. While there are several utilities leveraging the narrowband 700 MHz today, there is a risk that vendor support for devices on the narrowband spectrum reduces as vendors focus investment on devices support pLTE-capable spectrum. 700Mhz will not support transfer trip due to latency potential at more than 80 milliseconds is the maximum latency for DTT (direct transfer trip) for communications. The type of spectrum and that spectrum's capabilities can impact the latency. CenterPoint Energy is looking for spectrum that is capable of meeting the business requirements to meet our customers needs in a cost effective manner.
- c. Guidehouse benchmarking data relative to the Spectrum Acquisition and other resiliency measures was obtained from a proprietary survey report from First Quartile, which highlighted

the types of system resiliency measures where utilities place the highest investment focus (see Exhibit ELS-2, Appendix A, Figure A2, pp. 266-267). This information was provided to Guidehouse at a high-level based on the survey results. The general locations of the North American utilities represented in the report are indicated in Figure A1 (Ibid, p. 265). Other specific information requested in Q4-14.c is not currently available as Guidehouse is not permitted to release an unredacted version of the survey or individual participant details as the First Quartile survey was conducted on a "blind" basis to protect respondent confidentiality.

Guidehouse provided a table that contains relevant legislation and docket numbers for general resiliency filings including Texas (Exhibit ELS-2, Appendix B, Table B3, pp. 276-279) from a Guidehouse benchmarking report, however these filings may not align perfectly with the utilities included in the First Quartile survey.

SPONSOR:

Ron Bahr and Dr. Joseph Baugh

RESPONSIVE DOCUMENTS:

None

**CENTERPOINT ENERGY HOUSTON ELECTRIC, LLC
PUC DOCKET NO. 57579
SOAH DOCKET NO. 473-25-11558**

**OFFICE OF PUBLIC UTILITY COUNSEL
REQUEST NO.: OPUC-RFI04-15**

QUESTION:

Please refer to Baugh Direct at 35, wherein Dr. Baugh states, "Guidehouse determined the proposed Data Center Modernization resiliency measure is consistent with resiliency practices deployed at other utilities ... " please list the other utilities referenced and the resiliency practices deployed at those utilities by name of utility, location, and practice which are consistent with the Data Center Modernization proposed in this case.

ANSWER:

Guidehouse benchmarking data relative to the Data Center Modernization and other resiliency measures was obtained from a proprietary survey report from First Quartile, which highlighted the types of system resiliency measures where utilities place the highest investment focus (see Exhibit ELS-2, Appendix A, Figure A2, pp. 266-267). This information was provided to Guidehouse at a high-level based on the survey results. The general locations of the North American utilities represented in the report are indicated in Figure A1 (Ibid, p. 265). Other specific information requested in Q4-15 is not currently available as Guidehouse is not permitted to release an unredacted version of the survey or individual participant details as the First Quartile survey was conducted on a "blind" basis to protect respondent confidentiality.

SPONSOR:

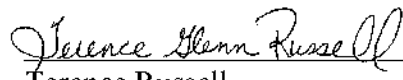
Dr. Joseph Baugh

RESPONSIVE DOCUMENTS:

None

CERTIFICATE OF SERVICE

I hereby certify that on March 26, 2025, notice of the filing of this document was provided to all parties of record via electronic mail in accordance with the Second Order Suspending Rules, filed in Project No. 50664.


Terence Russell