

CONFIDENTIAL DESIGNATIONS

The Empire District Electric Company d/b/a Liberty

ER-2024-0261

RE: All confidential testimony (portions of pp. 10, 12-13) and schedules (portions of Direct Schedule SE-1) of Shawn Eck

The information provided is designated “Confidential” in accordance with Commission Rule 20 CSR 4240-2.135(2)(A)7 and 8 due to the nature of the material regarding the safety and security of Liberty’s critical infrastructure and other utility facilities. Schedule SE-1 identifies, by vendor and specific project, the scope and contents of Empire’s cybersecurity and asset security protections. Liberty recognizes the importance of providing transparent and accurate testimony and information in response to regulatory inquiries. We must emphasize the potential risks associated with disclosing the sensitive information included in the testimony that could inadvertently expose critical infrastructure or systems to cybersecurity threats. Public disclosure of this information would allow adversarial parties and bad actors to develop an attack profile, as the bad actor would know (1) the specific vendors Liberty has engaged, (2) the extent of the security protections, and (3) vulnerabilities that Liberty or the vendors may have. Likewise, the level of a company’s investment in cybersecurity is a relevant data point to building an attack profile. The confidential information in Liberty’s testimony refers to and provides a holistic description of the threats that Liberty is seeking to avoid. Cumulatively, the confidential testimony provides a detailed description of Liberty’s cybersecurity efforts and protections, falling squarely within the category of “(r)elating to the security of a company's facilities” in 20 CSR 4240-2.135(2)(A)7 and trade sections under subsection 8. The confidentiality shall be maintained consistent with that Rule and/or Section 386.480 RSMo., as the case may be. This confidential designation is made in recognition of the ongoing responsibility to protect public safety and national security and to ensure the continued reliability of critical infrastructure. Liberty trusts that all relevant parties will respect the need for such safeguards and will work with Liberty to establish the necessary protections to preserve confidentiality through the regulatory process.

Exhibit No.: _____
Issue: Cyber-Security Programs
Witness: Shawn Eck
Type of Exhibit: Direct Testimony
Sponsoring Party: The Empire District
Electric Company d/b/a Liberty
Case No.: ER-2024-0261
Date Testimony Prepared: November 2024

**Before the Public Service Commission
of the State of Missouri**

Direct Testimony

of

Shawn Eck

on behalf of

The Empire District Electric Company d/b/a Liberty

November 6, 2024



****DENOTES CONFIDENTIAL****
20 CSR 4240-2.135(2)(A)7, 8

PUBLIC VERSION

TABLE OF CONTENTS
FOR THE DIRECT TESTIMONY OF SHAWN ECK
THE EMPIRE DISTRICT ELECTRIC COMPANY D/B/A LIBERTY
BEFORE THE MISSOURI PUBLIC SERVICE COMMISSION
CASE NO. ER-2024-0261

SUBJECT	PAGE
I. INTRODUCTION.....	1
II. CURRENT LANDSCAPE.....	3
III. CRITICAL INFRASTRUCTURE	6
IV. THE PROGRAM AND THE NEED TO INVEST	10
V. CYBERSECURITY PROGRAM COMPONENTS AND COSTS	13
VI. CONCLUSIONS	14

DIRECT TESTIMONY OF SHAWN ECK
THE EMPIRE DISTRICT ELECTRIC COMPANY D/B/A LIBERTY
BEFORE THE MISSOURI PUBLIC SERVICE COMMISSION
CASE NO. ER-2024-0261

1 **I. INTRODUCTION**

2 **Q. Please state your full name and business address.**

3 A. My name is Shawn Eck. My business address is 602 South Joplin Avenue, Joplin,
4 Missouri.

5 **Q. By whom are you employed and in what capacity?**

6 I am employed by Liberty Utilities Service Corp. (“LUSC”) as Director of IT Security,
7 Risk, and Compliance.

8 **Q. On whose behalf are you testifying in this proceeding?**

9 A. I am testifying on behalf of The Empire District Electric Company (“Empire” or the
10 “Company”).

11 **Q. Please describe your educational and professional background.**

12 A. I have been working in the cybersecurity space for more than 20 years. I began my
13 career in cybersecurity through service in the United States Air Force in 1997.
14 Following my service, I served as a government contractor supporting cybersecurity
15 missions under the United States Air Force. I was employed by Iowa Park Consolidated
16 Independent School District in 2003 as the Director of Information Technology.
17 Beginning in late 2003 to 2006, I worked for Empire supporting the corporate and
18 control system networks. From 2006 to 2013, I was employed by Freeman Health
19 Systems supporting the health system cybersecurity and Health Insurance Portability
20 and Accountability (“HIPAA”) Compliance. In 2013, I returned to Empire and served
21 in several cybersecurity roles until September 2020 when I began my current role as
22 Director of IT Security, Risk, and Compliance. In addition to my experience, I’ve

1 pursued additional education and certifications in cybersecurity, including Certified
2 Information Systems Security Professional and the Certification in Risk and
3 Information Systems Control, among other certifications. I maintain these certifications
4 through ongoing professional education. Overall, my educational and professional
5 background as a cybersecurity professional is extensive and includes a combination of
6 formal education, military training, accreditations, certifications, and on-the-job
7 experience.

8 **Q. Have you previously testified before the Missouri Public Service Commission**
9 **(“Commission”) or before any other utility regulatory agency?**

10 A. Although I have not testified before this Commission, I have provided written
11 testimony before the New Hampshire Public Utilities Commission and the New York
12 Public Service Commission. Additionally, in Missouri, and in the other states where
13 Empire affiliates own and operates utilities, I engage with regulators and their staff and
14 other stakeholders on matters related to cybersecurity. More specifically, I am
15 responsible for developing and preparing annual cybersecurity plans filed with
16 regulatory agencies that govern our business.

17 **Q. What is the purpose of your direct testimony in this proceeding before the**
18 **Commission?**

19 A. The purpose of my direct testimony is to describe Empire’s Cybersecurity Program
20 (“Cybersecurity Program”) and the investments it will make for the continuation of the
21 safe, secure, and reliable operation of its electric distribution system. I also describe the
22 environment in which Empire’s proposed spending will take place, how the
23 cybersecurity space is changing rapidly and becoming more complex, and I will explain
24 the need for continued investments in cybersecurity. These findings support my

1 primary conclusion that the Commission should approve Empire’s Cybersecurity
2 Program to protect Empire’s critical infrastructure and provide secure and reliable
3 utility service to its customers.

4 **Q. How is the remainder of your testimony organized?**

5 A. The remainder of my testimony is organized as follows:

- 6 • *Section II* summarizes the current landscape Empire faces.
- 7 • *Section III* describes the concept of critical infrastructure and explains how the
8 term is applicable to Empire’s assets.
- 9 • *Section IV* describes the components of the Cybersecurity Program and the need
10 to make these investments to address cyber risk.
- 11 • *Section V* describes the financial and operating characteristics of the
12 components that comprise the Cybersecurity Program.
- 13 • *Section VI* contains my conclusions.

14 **II. CURRENT LANDSCAPE**

15 **Q. Please summarize this section of your testimony.**

16 A. In this section of my testimony, I provide an explanation of the evolving cybersecurity
17 environment in which Empire operates. I define the cybersecurity threats that pose risks
18 to Empire and its customers and therefore must be mitigated while doing business.

19 **Q. What is the current cyber threat landscape?**

20 A. As Empire’s business landscape grows and matures, so does its exposure to an
21 increasingly complex and dangerous threat landscape. Sophisticated threat actors
22 continue to target utility’s daily operations, business administration, and its ability to
23 provide high quality services to its customers. For example, according to the 2024
24 Department of Homeland Security (DHS) Homeland Threat Assessment, the number

1 of known ransomware attacks in the United States increased by 47 percent between
2 January 2020 and December 2022.¹ From attacks aimed at disrupting services to
3 espionage focused on gaining access to networks and stealing sensitive information,
4 domestic and foreign adversaries continue to adapt their techniques to gain access to
5 and potentially compromise the integrity of critical US infrastructure with intent to
6 negatively impact US industries and the American way of life.

7 **Q. Please explain how new technologies are changing the nature of the cybersecurity**
8 **threat.**

9 A. The proliferation of new technologies creates new risks. One of the most significant
10 changes in the energy sector is the increased adoption of digital technologies. From
11 smart grid systems to interconnected energy management systems using Internet of
12 Things (“IoT”), these technologies are becoming more prevalent in the industry. As a
13 result, utilities are facing increased exposure and vulnerability to cyberattacks that can
14 cause widespread damage and disruption. For example, traditionally a power plant or
15 small generator produced only electrons that were consumed by an end user. The meter
16 was the point at which the utility and the end user interacted, and information
17 exchanged. Now, however, an end user (commercial or residential) may use
18 technology, like solar panels, battery storage, and wired or wireless monitoring devices,
19 that in addition to producing electrons, also transmit and receive electronic signals that
20 contain customer information, usage information, time of use information, and other
21 personal data, which adds a layer of complexity to the data the Company is required to
22 protect.

¹ https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf, at p. 26.

1 **Q. Please state how cybersecurity strategy has evolved in this increasingly dynamic**
2 **environment.**

3 A. In the past, utilities typically viewed cybersecurity as a one-time investment, with the
4 primary focus on purchasing and implementing technology solutions that met
5 perceived threats. Today, cybersecurity is an ongoing concern, requiring continuous
6 attention, maintenance, and updates to meet and anticipate the evolving landscape.
7 Empire recognizes that both new technologies and the increased interdependence of
8 critical systems increasingly require adaptation and commitment of more resources to
9 security. Simultaneously, reporting and compliance requirements are becoming more
10 stringent, further increasing burdens especially with regards to protecting critical
11 infrastructure. Protecting critical infrastructure has always been a priority, but now our
12 strategy requires a diverse set of solutions and an ability to adapt to changing threats in
13 this increasingly dynamic environment.

14 **Q. Please explain increased interdependence and its effect on cybersecurity.**

15 A. Many critical infrastructure sectors are increasingly interconnected and reliant on one
16 another. For example, the energy sector powers the information and communication
17 technology sector with electrons that make them run. The communication technology
18 sector in turn supports other key sectors like water, electricity monitoring and security,
19 etc. One cannot function properly without the other.

20 **Q. Specifically, what steps are being taken in response to the ongoing risks**
21 **surrounding cybersecurity?**

22 A. The Company must maintain robust cybersecurity measures that addresses both the
23 increasing complexity of technology and the inherent characteristics of the dynamic
24 resource mix. This includes developing comprehensive cybersecurity policies and

1 procedures, implementing effective access controls and authentication measures,
2 conducting regular risk assessments, and investing in cybersecurity training and
3 awareness programs for employees.

4 **III. CRITICAL INFRASTRUCTURE**

5 **Q. Please summarize this section of your testimony.**

6 A. In this section of my testimony, I introduce and explain the concept of critical
7 infrastructure and describe the critical infrastructure the Company owns and operates.
8 I then describe how implementing the Cybersecurity Program protects those critical
9 assets.

10 **Q. What is critical infrastructure?**

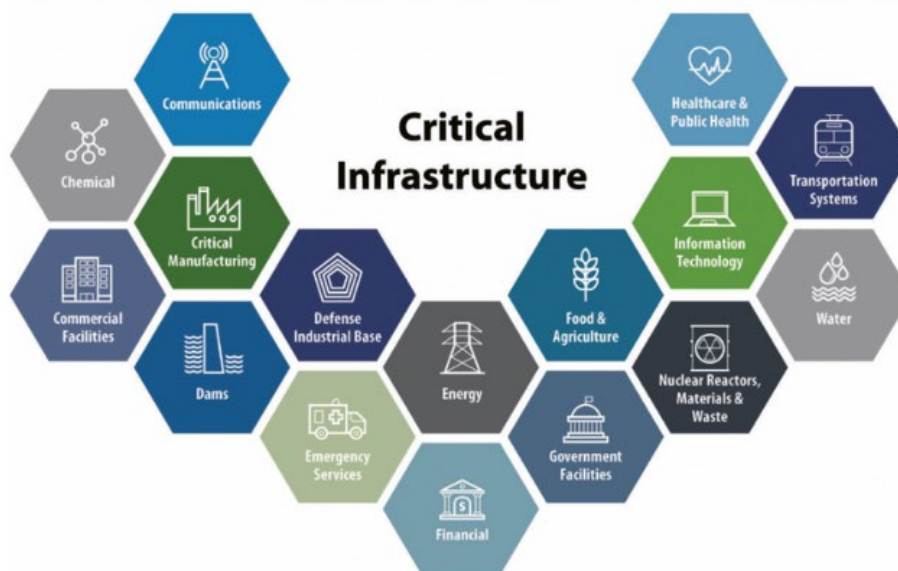
11 A. The Cybersecurity & Infrastructure Security Agency (“CISA”), a division of the
12 Department of Homeland Security, defines critical infrastructure as “...assets, systems,
13 and networks, whether physical or virtual, [that] are considered so vital to the United
14 States that their incapacitation or destruction would have a debilitating effect on
15 security, national economic security, national public health or safety, or any
16 combination thereof.”²

17 **Q. Which sectors of the economy include critical infrastructure?**

18 There are sixteen, according to CISA. The sectors are shown in Figure 1.

² <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>.

Figure 1. Critical Infrastructure Sectors



1 Q. Are Empire’s generation, transmission, and distribution systems critical
2 infrastructure?

3 A. Yes, the assets and systems that support generation, transmission, and distribution
4 operations constitute critical infrastructure.

5 Q. Is the primary goal of the Cybersecurity Program to protect these assets and
6 systems?

7 A. Yes.

8 Q. What are the specific data, assets and systems that comprise the Company’s
9 critical infrastructure?

10 A. The Company’s data, its Operational Technology (“OT”), and its Information
11 Technology (“IT”) used to support its utility operations and business functions.

12 Q. Within this context, can you please define the term data?

13 A. Data refers to the information generated, collected, processed, stored, and transmitted
14 by the various systems and assets within the essential sectors. Data is vital for the
15 efficient operation and management of an electric utility.

1 **Q. Please provide some examples of the Company's data.**

2 A. The Company collects, generates, and analyzes many types of data while doing
3 business. Among these are load data, equipment data, outage data, weather data, data
4 that describes the physical configuration of Empire's generation, transmission, and
5 distribution networks, and customer data which are the types of data whose protection
6 are most critical.

7 **Q. Please describe Empire's OT.**

8 A. OT includes the Company's technology supporting physical infrastructure generation,
9 transmission, and distribution operations. Generation, transmission, and distribution
10 physical infrastructure includes, for example, SCADA, transmission/distribution lines,
11 switches, and the myriad other assets that Empire owns and operates on behalf of its
12 electric customers.

13 **Q. Please describe the Company's IT.**

14 A. IT is comprised of the systems the Company uses to store, process, analyze, and
15 exchange data. Specific types of IT assets include computer hardware, software, and
16 communication technologies.

17 **Q. What are common cybersecurity threats to the Company's data, IT, and OT**
18 **assets?**

19 A. Examples of common cybersecurity threats the Company faces are:

- 20 • Phishing attacks: These attacks involve sending fraudulent emails or messages
21 that trick users into providing sensitive information such as passwords or
22 confidential information or used to deliver malware.

- 1 • Malware attacks: Malware is a type of software designed to damage or disable
2 computers and computer systems. It can infect computers through email
3 attachments, infected software, or even through social engineering techniques.
- 4 • Ransomware attacks: Ransomware is a type of malware that encrypts a victim's
5 files and demands payment to restore access. It can be delivered through
6 phishing emails, malicious downloads, or compromised websites.
- 7 • Denial of Service (DoS) attacks: These attacks overload a company's servers or
8 network with traffic, rendering it inaccessible to legitimate users.
- 9 • Insider threats: Insider threats are posed by internal accounts which have access
10 to sensitive data and can intentionally or unintentionally leak, steal, or misuse
11 the data.
- 12 • Advanced Persistent Threats (“APTs”): APTs are sophisticated, long-term
13 cyber-attacks that are designed to infiltrate a company's network and extract
14 sensitive data without being detected.
- 15 • Zero-day exploits: Zero-day exploits are vulnerabilities in software that are
16 unknown to the vendor and can be exploited by hackers to gain access to a
17 company's systems.

18 **Q. Will implementing the Cybersecurity Program support the Company’s ability to**
19 **mitigate these threats?**

20 A. Yes. The Cybersecurity Program will improve capabilities, including people,
21 processes, and technology, to defend, detect, and respond to these threats.

1 **Q. Is it important that Empire protect each of the different types of critical**
2 **infrastructure?**

3 A. Yes, very. As stated in Presidential Policy Directive 21, the Energy Sector is uniquely
4 critical because it provides an “enabling function” across all critical infrastructure
5 sectors (i.e., “Energy Critical Infrastructure”).³ Empire owns and operates electric
6 critical infrastructure related to the generation, transmission, and distribution of
7 electricity.

8 **IV. THE PROGRAM AND THE NEED TO INVEST**

9 **Q. Please summarize this section of your testimony.**

10 A. In this section, I provide a high-level explanation of the Cybersecurity Program and its
11 basic components and conduct a more extensive discussion of the need to make these
12 investments to address the cybersecurity risks described in the sections above.

13 **Q. Please describe the Cybersecurity Program.**

14 A. ** [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED] **

20 **Confidential Direct Schedule SE-1** provides a description of the workstreams and
21 projects. Program Capital and operating costs are allocated to Empire, as I describe
22 later in my testimony.

³ https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf (last visited Aug. 21, 2024).

1 **Q. Are there overarching frameworks, common controls, rules, or organizations that**
2 **guide cybersecurity strategies?**

3 A. Yes. Included among them are the NERC Reliability Standards, Sarbanes-Oxley Act
4 (“SOX”), International Organization Standardization (“ISO”), and the National
5 Institute of Standards and Technology (“NIST) which incorporate five functions
6 encapsulated by NIST’s Cybersecurity Framework: identify, protect, detect, respond,
7 and recover (i.e., Figure 2 below). These are the highest levels of abstraction and act
8 as the core elements around which we take actions related to our cybersecurity
9 obligations and investments in people, processes, and technologies.

10 *Figure 2. NIST’s Cybersecurity Framework*



11
12 **Q. Briefly describe these five functions.**

13 A. Each function can be briefly described as follows:

- 14 • Identify: Assess and manage risks by identifying assets, systems, and threats to
15 prioritize cybersecurity needs.
- 16 • Protect: Implement safeguards to limit the impact of potential cybersecurity
17 incidents on critical infrastructure and services.

- 1 • Detect: Continuously monitor systems for signs of breaches or vulnerabilities
- 2 to swiftly identify and analyze potential threats, both internally and externally.
- 3 • Respond: Develop and execute response strategies to contain, mitigate, and
- 4 eliminate the impact of detected incidents.
- 5 • Recover: Implement plans to restore normal operations after an incident,
- 6 ensuring the organization’s resilience and adaptation to evolving threats.

7 Each of these functions is required for the Company to timely and adequately keep up
8 with ever-evolving threats.

9 **Q. How do the investments in the Cybersecurity Program address cybersecurity**
10 **threats and risk?**

11 A. ****** [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED] ******

18 **Q. What benefits to Empire’s customers are realized from making these**
19 **investments?**

20 A. ****** [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] **

V. CYBERSECURITY PROGRAM COMPONENTS AND COSTS

Q. What is the purpose of this section of your testimony?

A. In this section of my testimony, I describe the Cybersecurity Program, including the nature of the various investments being made and their costs.

Q. Please briefly summarize the investments that comprise the Cybersecurity Program.

A. The Cybersecurity Program is comprised of a mix of resources that includes hardware, software, and services. The investments include capital and operating expenditures that are used on software or technology platforms which provide security controls and capabilities. All investments provide security control for critical operations and business functions (e.g., SCADA system, substation operations, enterprise solution, etc.); costs will be centrally procured and allocated to Empire.

Q. What amount of capital costs for the Cybersecurity Program were operational in Empire’s update period in this case?

A. Through the end of Empire’s update period (i.e., September 2024), Total Cybersecurity Project costs are expected to be \$7.38 million at the Total Empire Electric level or \$6.42 million at the Missouri jurisdictional level. Refer to the direct testimony of Empire witness Charlotte T. Emery for further discussion on the plant additions adjustment, which includes the capital costs for the Cybersecurity Program.

1 **Q. Are there recurring annual operating and maintenance (“O&M”) costs related to**
2 **the Cybersecurity Program?**

3 A. Yes. O&M costs are comprised of added labor (FTEs) to support program operations
4 as well as licensing and software renewal costs. Annual non-labor O&M costs
5 associated with the Cybersecurity Program are estimated to be \$1.53 million for
6 calendar year 2024 with additional ongoing costs expected through 2027. We require
7 an incremental increase in headcount over the lifespan of the Cybersecurity Program
8 as capabilities become operational and in-service, with an estimated increase in
9 headcount of 20 FTEs by the year 2027.

10 **Q. How are these costs allocated to Empire?**

11 A. The costs are allocated using the same approach as applies to other costs incurred by
12 Empire as described in the Company’s Cost Allocation Manual (“CAM”). For further
13 discussion on the Company’s CAM, please refer to the direct testimony of Empire
14 witness Jill Schwartz.

15 **VI. CONCLUSIONS**

16 **Q. Please summarize your direct testimony.**

17 A. My testimony supports four conclusions.

18 (1) The current cyber threat landscape is evolving in both complexity and severity.
19 Empire’s effective management of the cybersecurity threat is critical to its ability to
20 provide safe, reliable service to its customers.

21 (2) Empire operates critical infrastructure that presents high risk from cyber threats that
22 must be addressed through a holistic cybersecurity solution, i.e. the Cybersecurity
23 Program.

1 (3) The Cybersecurity Program is designed to directly address the cyber threats & risks
2 by implementing capabilities focused on various domains of cybersecurity that
3 coincide to protect, detect, and respond to cybersecurity threats. The Cybersecurity
4 Program design follows industry best practices/frameworks and is able to adapt to
5 emerging threats in a dynamic and ever-changing environment.

6 (4) The Cybersecurity Program costs described in Section V are expected to provide an
7 adequate level of cybersecurity protection at a reasonable cost.

8 **Q. What are your recommendations?**

9 A. Based on these conclusions, I recommend the Commission support the recovery of the
10 Cybersecurity Program capital investment and operational expense to allow Empire to
11 maintain appropriate security that protects Critical Infrastructure.

12 **Q. Does this conclude your direct testimony at this time?**

13 A. Yes.

VERIFICATION

I, Shawn Eck, under penalty of perjury, on this 6th day of November, 2024, declare that the foregoing is true and correct to the best of my knowledge and belief.

/s/ Shawn Eck