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)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**

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

I. INTRODUCTION

Q. Please state your full name and business address.

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

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

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

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

A. I am testifying on behalf of The Empire District Electric Company ("Empire" or the "Company").

Q. Please describe your educational and professional background.

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

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

Q. Have you previously testified before the Missouri Public Service Commission ("Commission") or before any other utility regulatory agency?

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

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

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

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

Q. How is the remainder of your testimony organized?

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

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

II. CURRENT LANDSCAPE

Q. Please summarize this section of your testimony.

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

Q. What is the current cyber threat landscape?

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

of known ransomware attacks in the United States increased by 47 percent between January 2020 and December 2022.[1] From attacks aimed at disrupting services to espionage focused on gaining access to networks and stealing sensitive information, domestic and foreign adversaries continue to adapt their techniques to gain access to and potentially compromise the integrity of critical US infrastructure with intent to negatively impact US industries and the American way of life.

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

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

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

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

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

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

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

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

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

III. CRITICAL INFRASTRUCTURE

Q. Please summarize this section of your testimony.

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

Q. What is critical infrastructure?

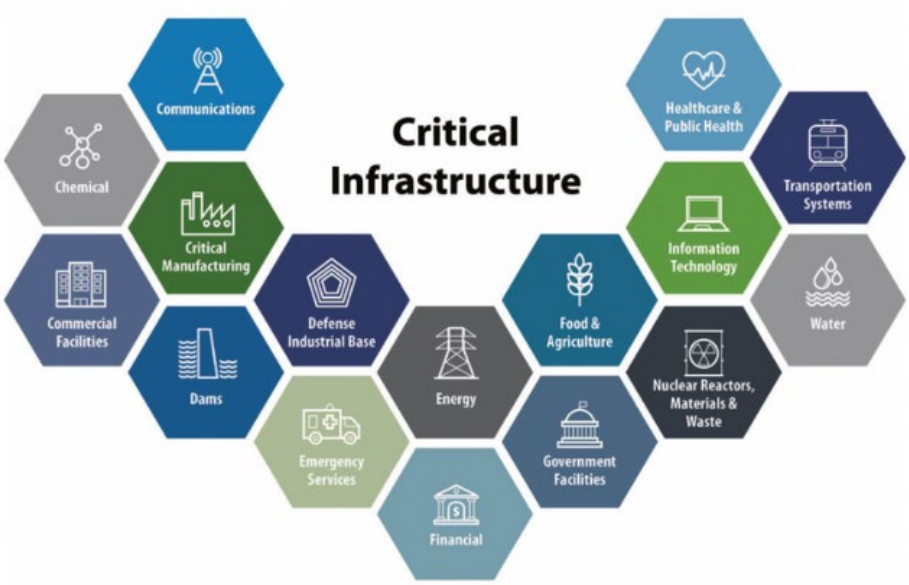
A. The Cybersecurity & Infrastructure Security Agency ("CISA"), a division of the Department of Homeland Security, defines critical infrastructure as "…assets, systems, and networks, whether physical or virtual, [that] are considered so vital to the United States that their incapacitation or destruction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

Q. Which sectors of the economy include critical infrastructure?

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



Q. Are Empire's generation, transmission, and distribution systems critical infrastructure?

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

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

A. Yes.

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

A. The Company's data, its Operational Technology ("OT"), and its Information Technology ("IT") used to support its utility operations and business functions.

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

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

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

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

Q. Please describe Empire's OT.

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

Q. Please describe the Company's IT.

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

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

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

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

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

Q. Will implementing the Cybersecurity Program support the Company's ability to mitigate these threats?

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

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

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

IV. THE PROGRAM AND THE NEED TO INVEST

Q. Please summarize this section of your testimony.

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

Q. Please describe the Cybersecurity Program.

A. **[redacted]**

Confidential Direct Schedule SE-1 provides a description of the workstreams and projects. Program Capital and operating costs are allocated to Empire, as I describe 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).

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

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

Figure 2. NIST's Cybersecurity Framework

Q. Briefly describe these five functions.

A. Each function can be briefly described as follows:

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

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

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

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

A. **[redacted]**

Q. What benefits to Empire's customers are realized from making these investments?

A. **[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.

Q. Are there recurring annual operating and maintenance ("O&M") costs related to the Cybersecurity Program?

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

Q. How are these costs allocated to Empire?

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

VI. CONCLUSIONS

Q. Please summarize your direct testimony.

A. My testimony supports four conclusions.

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

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

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

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

Q. What are your recommendations?

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

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

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