

STATE OF NEW HAMPSHIRE  
BEFORE THE  
PUBLIC UTILITIES COMMISSION

Docket No. DE 23-039

Liberty Utilities (Granite State Electric) Corp. d/b/a Liberty  
Distribution Service Rate Case  
Cybersecurity

DIRECT TESTIMONY

OF

SHAWN ECK

May 5, 2023



THIS PAGE INTENTIONALLY LEFT BLANK

**TABLE OF CONTENTS**

| <u>TITLE</u>                                 | <u>PAGE</u> |
|--|-------------|
| LIST OF FIGURES .....                        | iii         |
| LIST OF TABLES.....                          | iii         |
| I. INTRODUCTION.....                         | 1           |
| II. CURRENT LANDSCAPE.....                   | 4           |
| III. CRITICAL INFRASTRUCTURE .....           | 8           |
| IV. CYBERSECURITY REGULATORY LANDSCAPE ..... | 13          |
| V. PROGRAM COMPONENTS AND COSTS.....         | 17          |
| A. Program Configuration .....               | 17          |
| B. Cost Uncertainty .....                    | 19          |
| VI. CONCLUSIONS.....                         | 21          |

**LIST OF FIGURES**

|  |    |
|--|----|
| FIGURE 1. CRITICAL INFRASTRUCTURE SECTORS..... | 9  |
| FIGURE 2. NIST’S CYBERSECURITY FRAMEWORK.....  | 14 |

**LIST OF TABLES**

|  |    |
|--|----|
| TABLE 1. COMPANY CYBERSECURITY PROGRAM SPENDING BY RATE YEAR ..... | 18 |
|--|----|

THIS PAGE INTENTIONALLY LEFT BLANK

1 **I. INTRODUCTION**

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

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

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

9 A. I am testifying on behalf of Liberty Utilities (Granite State Electric) Corp. d/b/a Liberty  
10 (“Liberty” or the “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 career  
13 in cybersecurity through service in the United States Air Force in 1997. Following my  
14 service, I served as a government contractor supporting cybersecurity missions under the  
15 United States Air Force. I was employed by Iowa Park Consolidated Independent School  
16 District in 2003 as the Director of Information Technology. Beginning in late 2003 to  
17 2006, I worked for The Empire District Electric Company (“Empire”) supporting the  
18 corporate and control system networks. From 2006 to 2013, I was employed by Freeman  
19 Health Systems supporting the health system cybersecurity and Health Insurance  
20 Portability and Accountability (“HIPAA”) Compliance. In 2013, I returned to Empire and  
21 served in several cybersecurity roles until September 2020 when I began my current role

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

8 **Q. Have you previously testified in a proceeding before the New Hampshire Public**  
9 **Service Commission (“Commission”)?**

10 A. No, I have not.

11 **Q. Do you have significant experience representing Liberty and its affiliates in**  
12 **collaborations with regulators, their staff, and other stakeholders on matters related**  
13 **to cybersecurity?**

14 A. Yes. In New Hampshire, and in the other states where the utilities owned by Algonquin  
15 Power and Utilities Corporation (“APUC”), Liberty’s parent company, do business, I am  
16 engaged with our regulators and their staff and with other stakeholders on matters related  
17 to cybersecurity. I am responsible for developing and preparing the Company’s annual  
18 cybersecurity plan which is filed annually with the Commission. In addition, I regularly  
19 meet with senior government officials in the states where the APUC utilities operate to  
20 coordinate on initiatives related to cybersecurity and I frequently accept invitations to  
21 participate in industry conferences focused on cybersecurity in the utility space.

1 **Q. What is the purpose of your testimony?**

2 A. The purpose of my testimony is to explain Liberty’s proposed cybersecurity program (the  
3 “Program”) and describe the investments it will make to ensure the continuation of the  
4 safe, secure, and reliable operation of its electric distribution system. I also describe the  
5 environment in which the Company’s proposed spending will take place. In particular, I  
6 explain the need for continued investments in cybersecurity, that the cybersecurity space  
7 is changing rapidly and unpredictably, and that because of these factors, electric utilities  
8 can neither reasonably predict nor reliably control their future cybersecurity spending.  
9 These findings support my primary conclusion that the Commission should approve the  
10 Company’s proposed Program and authorize it to adjust its spending as necessary to  
11 prudently invest in cybersecurity to protect the Company’s critical infrastructure.

12 **Q. How is the remainder of your testimony organized:**

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

- 14 • *Section II* summarizes the current landscape that the Company faces.
- 15 • *Section III* describes the concept of critical infrastructure and explains how the  
16 term is applicable to Liberty’s assets.
- 17 • *Section IV* describes the various cybersecurity-related regulations and guidelines  
18 to which the Company must adhere and explains why the cost of doing so is  
19 increasing.
- 20 • *Section V* describes the financial and operating characteristics of the components  
21 that comprise the Program. In that same section, I also explain that the Company's

1 spending plans are necessarily subject to tremendous uncertainty and recommend  
2 that the Commission adopt policies that will allow Liberty to adjust its spending  
3 in response to events in the market between the end of this case and the beginning  
4 of the Company's next one.

- 5 • *Section VI* contains my conclusions.

## 6 **II. CURRENT LANDSCAPE**

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

8 A. In this section of my testimony, I provide a high-level explanation of the Program and its  
9 basic components and conduct a more extensive discussion of the cybersecurity  
10 environment in which Liberty does business. In particular, the highly uncertain and  
11 rapidly evolving nature of the cybersecurity threats that the Company must mitigate while  
12 doing business in New Hampshire.

13 **Q. Please describe the Program**

14 A. APUC invests in cybersecurity across the organization on a consolidated basis wherein  
15 APUC makes investments in infrastructure and incurs operational expenses to provide for  
16 cybersecurity for its operating companies. Program capital and operating costs are  
17 allocated to APUC's operating utilities, including the Company, as I describe in detail  
18 later in my testimony.

19 **Q. Please state how APUC's Cybersecurity strategy has evolved.**

20 A. Protecting critical infrastructure has always been a priority for APUC and the Company.  
21 However, the landscape in which we operate as a utility has evolved and is in constant



1 flux. In the past, utilities typically viewed cybersecurity as a one-time investment, with  
2 the primary focus on purchasing and implementing technology solutions that met most  
3 threats. Today, cybersecurity is an ongoing concern, requiring ongoing attention,  
4 maintenance, and updates to meet and anticipate the evolving landscape.

5 **Q. Please summarize the ways in which the Company's approach is changing in this**  
6 **increasingly dynamic environment?**

7 A. Liberty has always recognized the need to secure its system as an important part of its  
8 business, but new technologies and the increased interdependence of critical systems  
9 increasingly require it to adapt its practices and devote more resources to security while,  
10 simultaneously, reporting and compliance requirements are becoming more stringent,  
11 increasing burdens further. The impact on Liberty is typical of electric utilities  
12 everywhere: cybersecurity is becoming more complex and more expensive at the same  
13 time it becomes an increasingly critical function.

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

16 A. The proliferation of new technologies has created new risks. One of the most significant  
17 changes in the energy sector is the increased adoption of digital technologies. From smart  
18 grid systems to interconnected energy management systems using Internet of Things  
19 ("IoT"), these technologies are becoming more prevalent in the industry. As a result,  
20 utilities are facing increased exposure and vulnerability to cyberattacks that can cause  
21 widespread damage and disruption. I will provide a simple example. Traditionally, a

1 power plant or small generator produced only electrons that were consumed by an end  
2 user. The meter was the point at which the utility and the end user interacted, and  
3 information exchanged. Now, however, an end user (commercial or residential) may use  
4 technology, like solar panels, battery storage, and wired or wireless monitoring devices,  
5 that in addition to producing electrons, also transmit and receive electronic signals that  
6 contain customer information, usage information, time of use information, and other  
7 personal data that adds a layer of complexity to the data the Company is required to  
8 protect.

9 **Q. What steps are being taken in response?**

10 A. The Company must maintain robust cybersecurity measures that address both the  
11 increasing complexity of technology and the inherent characteristics of the dynamic  
12 resource mix. This includes developing comprehensive cybersecurity policies and  
13 procedures, implementing effective access controls and authentication measures,  
14 conducting regular risk assessments, and investing in cybersecurity training and  
15 awareness programs for employees.

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

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

1 **Q. Is the cybersecurity landscape evolving?**

2 A. Yes, rapidly.

3 **Q. Does that make it more difficult to develop cybersecurity spending plans?**

4 A. Yes, considerably. It is impossible to precisely know years in advance the nature of the  
5 investment needed or the response that will be required of the Company to maintain or  
6 recover system security, making it difficult to predict the level of investment needed for  
7 cybersecurity. APUC strives ensure it has adequate capabilities to holistically defend and  
8 protect our critical infrastructure enabling us to reliably provide critical services in the  
9 communities we serve.

10 **Q. Please explain how oversight and reporting requirements have changed.**

11 A. Critical infrastructure is often subject to government oversight, aimed at ensuring the  
12 safety, reliability, and security of these essential services. Because of the change in the  
13 technology used to provide critical services, the threats posed to them, and evolving and  
14 increasing demands from end users for more services, regulations have multiplied and  
15 continued to grow- creating a legislative, regulatory, and legal lag. By legislative,  
16 regulatory, and legal lag, I mean the legislative, regulatory, or legal provisions intended  
17 to ensure compliance may be inadequate to deal with technological or commercial  
18 contexts created by rapid advances in business models, information, and communication  
19 technology. Compliance can be described as the actions an organization takes to follow a  
20 set of standards established by a third party, like a governmental regulator. Compliance is  
21 different from security. Security or cybersecurity refers to the “real-time” people,

1 processes, systems, and technology, both hardware and software, that protect a  
2 company's assets from being affected by a bad actor, through a breach, leak, or  
3 cyberattack, for example. The lag occurs when the laws or rules that govern compliance  
4 are not keeping pace with live or "real-world" security threats. Despite the lag, however,  
5 the Company must protect its critical infrastructure now. It does not have the luxury of  
6 waiting to protect its critical assets once the law or rules are clear, or "catch up" to the  
7 current environment or technology. APUC's challenge becomes more complex when  
8 industrial best practices, and legislative, legal, and regulatory regimes governing assets  
9 vary from state to state, region to region, or by asset type.

10 **III. CRITICAL INFRASTRUCTURE**

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

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

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

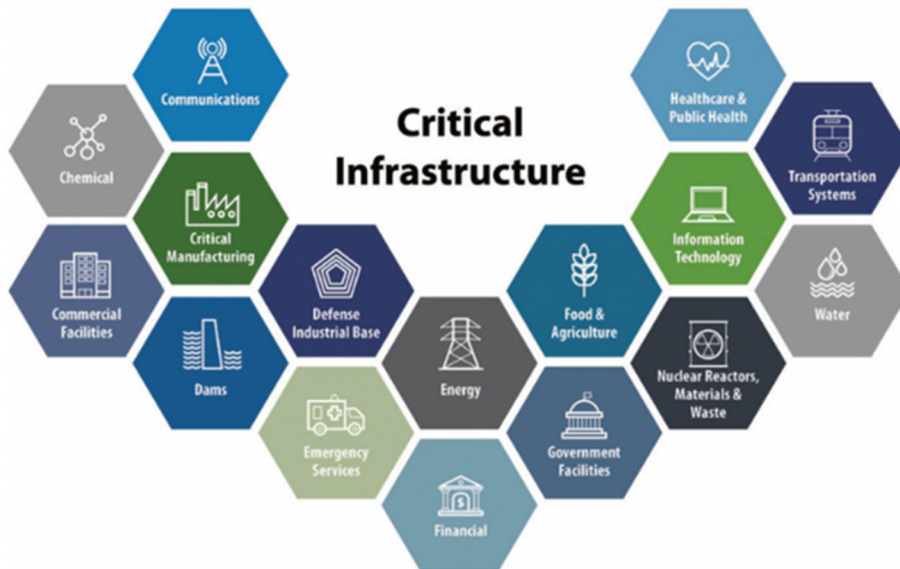
16 A. The Cybersecurity & Infrastructure Security Agency defines critical infrastructure as  
17 "...assets, systems, and networks, whether physical or virtual, [that] are considered so  
18 vital to the United States that their incapacitation or destruction would have a debilitating

1 effect on security, national economic security, national public health or safety, or any  
2 combination thereof.”<sup>1</sup>

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

4 A. There are sixteen, according to the Cybersecurity and Infrastructure Security Agency, a  
5 division of the Department of Homeland Security. The sectors are shown in Figure 1.

6 *Figure 1. Critical Infrastructure Sectors*



7

8 **Q. Is the Company’s distribution system critical infrastructure?**

9 A. Yes, as are the assets and systems that support the distribution system’s operation.

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

11 A. Yes.

---

<sup>1</sup> <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>

1 **Q. What are the specific assets and systems that comprise the Company's critical**  
2 **infrastructure?**

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

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

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

9 **Q. Can you provide examples?**

10 A. The Company collects, generates, and analyzes a great many types of data while doing  
11 business. Among these, load data, equipment data, outage data, weather data, data that  
12 describes the physical configuration of the Company's distribution network, and  
13 customer data are the types whose protection are most critical.

14 **Q. Please describe Liberty's OT.**

15 A. OT includes the Company's technology supporting physical infrastructure and  
16 distribution operations. Distribution physical infrastructure includes, for example,  
17 distribution lines, switches, and the myriad other assets that Liberty owns and operates on  
18 behalf of its customers.

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

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

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

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

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

10 Malware attacks: Malware is a type of software designed to damage or disable computers  
11 and computer systems. It can infect computers through email attachments, infected  
12 software, or even through social engineering techniques.

13 Ransomware attacks: Ransomware is a type of malware that encrypts a victim's files and  
14 demands payment to restore access. It can be delivered through phishing emails,  
15 malicious downloads, or compromised websites.

16 Denial of Service (DoS) attacks: These attacks overload a company's servers or network  
17 with traffic, rendering it inaccessible to legitimate users.

18 Insider threats: Insider threats are posed by internal accounts which have access to  
19 sensitive data and can intentionally or unintentionally leak, steal, or misuse it.

1           Advanced Persistent Threats (APTs): APTs are sophisticated, long-term cyber-attacks  
2           that are designed to infiltrate a company's network and extract sensitive data without  
3           being detected.

4           Zero-day exploits: Zero-day exploits are vulnerabilities in software that are unknown to  
5           the vendor and can be exploited by hackers to gain access to a company's systems.

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

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

10 **Q.    Is it important that Liberty protect each of the different types of its critical**  
11 **infrastructure?**

12 A.    Yes, very.

13 **Q.    Why?**

14 A.    As stated in Presidential Policy Directive 21, the Energy Sector is uniquely critical  
15    because it provides an "enabling function" across all critical infrastructure sectors (i.e.,  
16    "Energy Critical Infrastructure"). APUC is an owner and operator of Critical  
17    Infrastructure such as electric, gas, water, and wastewater utilities, dams, and  
18    communications critical infrastructure. Specific to New Hampshire, the Company owns  
19    and operates Energy Critical Infrastructure including electric and gas.



1 **IV. CYBERSECURITY REGULATORY LANDSCAPE**

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

3 A. In this section, I describe the various ways in which government agencies and other  
4 governance bodies provide oversight and guidance to the electric industry on matters of  
5 cybersecurity and explain that increasingly onerous compliance and reporting  
6 requirements that those entities impose are increasing utilities' costs of meeting their  
7 obligations.

8 **Q. Who regulates the Company's cybersecurity?**

9 A. There is no single set of regulatory regimes that applies simultaneously to every single  
10 critical asset that we own in every single state and across every single function. There are  
11 multiple regulatory regimes, Authorities Having Jurisdiction ("AHJs"), and operational  
12 frameworks holding oversight mandates.

13 **Q. What is a regulatory regime, as you have used the term above?**

14 A. A system of regulations and the means to enforce them, usually established by a  
15 governmental authority to regulate a specific activity and/or assets.

16 **Q. Does different oversight apply to transmission and distribution systems?**

17 A. Yes. The electric transmission system is regulated by federal and regional AHJs that  
18 include the Federal Energy Regulatory Commission ("FERC"), the U.S. Department of  
19 Energy ("DOE"), and the North American Electric Reliability Corporation ("NERC").  
20 Northeast Power Coordinating Council ("NPCC"), ISO New England, etc. Various state,  
21 city, and county AHJs impose additional requirements. As a result, rules and regulations

1 can be complex and considerable care must be taken to ensure compliance with the  
2 various federal, state, and local requirements on an ongoing basis.

3 **Q. In addition to the requirements imposed by these entities, are there overarching**  
4 **frameworks, common controls, rules, or organizations that guide the Company’s**  
5 **and APUC’s cybersecurity strategies?**

6 A. Yes. Included among them are the NERC Reliability Standards, Sarbanes-Oxley Act  
7 (“SOX”), International Organization Standardization (“ISO”), NIST, and New  
8 Hampshire’s own Puc 306.10 Physical and Cyber Security Plans, Procedures and  
9 Reporting requirements which incorporate five functions encapsulated by NIST’s  
10 Cybersecurity Framework: identify, protect, detect, respond, and recover (i.e., Figure 3  
11 below). These are the highest levels of abstraction and act as the core elements around  
12 which we take actions related to our cybersecurity obligations and investments in people,  
13 processes, and technologies.

14 *Figure 2. NIST’s Cybersecurity Framework*



15

1 **Q. Briefly describe these five functions.**

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

- 3 1. Identify: Assess and manage risks by identifying assets, systems, and threats to  
4 prioritize cybersecurity needs.
- 5 2. Protect: Implement safeguards to limit the impact of potential cybersecurity  
6 incidents on critical infrastructure and services.
- 7 3. Detect: Continuously monitor systems for signs of breaches or vulnerabilities to  
8 swiftly identify and analyze potential threats, both internally and externally.
- 9 4. Respond: Develop and execute response strategies to contain, mitigate, and  
10 eliminate the impact of detected incidents.
- 11 5. Recover: Implement plans to restore normal operations after an incident, ensuring  
12 the organization's resilience and adaptation to evolving threats.

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

15 **Q. Can you please summarize the requirements imposed by the state of New  
16 Hampshire regarding cybersecurity, including physical security?**

17 A. The New Hampshire Division of Enforcement inspects the physical plant of energy  
18 providers to review physical security systems employed by electric utilities, such as  
19 facility perimeters, controlled spaces, production spaces, and restricted spaces. They  
20 evaluate areas such as lighting, hardware, control systems, access systems, and entry  
21 points. Additionally, the Division of Enforcement monitors cybersecurity plans for

1 completeness and best practices. The Division of Enforcement also works with FERC's  
2 Office of Energy Infrastructure Security in sharing strategic frameworks and assessment  
3 techniques.

4 To be compliant with the New Hampshire Commission's Puc 300 rules related to  
5 cybersecurity obligations, the Company generally is required to:

- 6 • Develop, maintain, and follow a written physical security plan and a written  
7 information cybersecurity plan, both of which are risk-based and incorporate a  
8 threat level assessment, defined security measures for critical equipment and  
9 facilities, response procedures, and notifications upon discovering a breach,  
10 defined processes to track events, and employee awareness training programs.
- 11 • Notify the Commission of any accident or event that involves a breach of security  
12 or threat against utility facilities.
- 13 • File a quarterly report of equipment theft, sabotage, and breaches of security with  
14 the commission using Form E-37.
- 15 • Establish procedures for the confidential treatment of documents submitted in  
16 routine filings, including cybersecurity and physical security plans.

17 **Q. Has New Hampshire recognized the need for companies to invest in cybersecurity?**

18 A. Yes. In July 2022 the New Hampshire Department of Energy published the "New  
19 Hampshire 10-Year State Energy Strategy" recommending that "New Hampshire  
20 stakeholders need to "make cybersecurity a priority and should continue to pursue  
21 available synergies with regional and national partners to identify and respond to cyber

1 threats in real time.” As I discuss in my testimony, APUC’s Program and cybersecurity  
2 strategy is in line with this recommendation.

3 **V. PROGRAM COMPONENTS AND COSTS**

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

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

7 **A. Program Configuration**

8 **Q. Please briefly summarize the investments that comprise the Program.**

9 A. The Program is comprised of a mix of resources that includes hardware, software, and  
10 services. The Program investments include capital and operating expenditures that are  
11 used on software or technology platforms that provide security controls and capabilities.  
12 All Program investments provide security control for critical operations and business  
13 functions (e.g., SCADA system, substations operations, enterprise solution, etc.). The  
14 Program and its costs will be centrally procured and allocated across APUC’s  
15 subsidiaries.

16 **Q. What is the current outlook for the capital cost of the Program for the period over  
17 which the Company is proposing to set rates?**

18 A. \$4.93 million.

19 **Q. Can you please provide the total Program spending on an annual basis?**

20 A. Yes. Table 1 shows the Capital Expense (“CapEx”) for the Rate Years (“RYs”) that  
21 comprise the period over which the Company is proposing to make rates.

1 **Q. Please summarize the current outlook for Program OpEx and CapEx that will be**  
2 **allocated to the Company.**

3 A. The current outlook for Program spending by type for the rate period is shown in Table 1  
4 below.

5 *Table 1. Company Cybersecurity Program Spending by Rate Year*

|              | <b>Rate Years</b>     | <b>Capex (\$M)</b> | <b>Opex (\$M)</b> |
|--------------|-----------------------|--------------------|-------------------|
| Rate Year 1  | July 2023 - June 2024 | \$ 2.04            | \$ -              |
| Rate Year 2  | July 2024 – June 2025 | \$ 1.25            | \$ -              |
| Rate Year 3  | July 2025 - June 2026 | \$ 1.65            | \$ 0.22           |
| <b>Total</b> |                       | <u>\$ 4.93</u>     | <u>\$ 0.22</u>    |

6

7 **Q. Are these amounts already included in the Company’s cost of service?**

8 A. Yes. The rates proposed by Company witnesses Dane and Jardin include the Company’s  
9 cost of the cybersecurity program, including the costs to recover the capital investment  
10 and operating expenses.<sup>2</sup>.

11 **Q. Are any of the assets associated with the capital spending shown in Table 1 already**  
12 **in service?**

13 A. Yes. Spending on the Program has already begun, and a small amount of capital has  
14 already been placed into service. The RY1 CapEx value shown in Table 1 includes  
15 approximately \$0.7M in CapEx that was or will be placed into service between January

---

<sup>2</sup>Dane-Jardin Direct Testimony, p. 23

1 2023 and June 2023. I understand that this approach is consistent with past practice in  
2 New Hampshire.

3 **Q. Why is there no OpEx before RY3?**

4 A. The Program is capital-intensive in the earlier years. After which the Program will be  
5 maintained and sustained through operating costs.

6 **Q. How are these costs allocated to the Company?**

7 A. The costs are allocated to the operating companies using the same approach as applies to  
8 other costs incurred by APUC on behalf of the operating companies.

9 **B. Cost Uncertainty**

10 **Q. Are you confident in the accuracy of the spending outlook shown in the tables  
11 above?**

12 A. No, not very. As I explain in several instances earlier in my testimony, the dynamic  
13 nature of the cybersecurity space necessarily introduces significant uncertainty in any  
14 spending forecast. Put simply, the changing landscape and required investment result in  
15 the need to constantly adapt program requirements. Changes in Program requirements  
16 and configuration will inevitably create changes in costs.

17 **Q. Are you aware of the Company's proposal to provide ratemaking flexibility that  
18 would accommodate this uncertainty?**

19 A. Yes, I am familiar with the proposal that Company Witnesses Matthew DeCoursey and  
20 Gregg Therrien make in their Direct Testimony regarding the reconciliation of variances  
21 from approved costs that will undoubtedly emerge over the course of the rate period.

1 While I am not an expert in utility ratemaking, the proposal that Messrs. DeCoursey and  
2 Therrien make appears to provide sufficient flexibility to account for the levels of  
3 spending uncertainty that I expect.

4 **Q. As an alternative to the proposal that Messrs. DeCoursey and Therrien make in**  
5 **their testimony, would it be possible for the Company to operate within the budgets**  
6 **set by the spending plans approved in this proceeding by deferring planned**  
7 **spending presently unanticipated cost increase require doing so?**

8 A. No. Under other circumstances, for other types of investments, I can see how deferring  
9 voluntary spending in response to cost increases elsewhere might be an effective way to  
10 control budgets, but the nature of the cybersecurity threat precludes that approach. The  
11 adverse impacts from any single breach have the potential to be profoundly adverse for  
12 our customers. Simply put, the Company cannot afford to fall behind on cybersecurity,  
13 even temporarily or by a small amount, even when the cost of keeping pace with threats  
14 jeopardizes budgets.

15 **Q. Is there any other alternative available?**

16 A. None that are good for our customers. Forcing the Company to operate within a set  
17 budget whose accuracy simply cannot be known in advance is inherently incompatible  
18 with the uncertain nature of the cybersecurity space and creates an unacceptable level of  
19 risk that Liberty would be unable to recover the costs of its investments and spending that  
20 were necessary to provide safe, reliable service. In the alternative, Liberty could add  
21 contingencies to its planned spending to account for potential variations in cost, but doing



1 so would create a different set of problems. The contingency would need to be large in  
2 order to ensure the Company's ability to recover its costs, but contingencies large enough  
3 to account for expected levels of uncertainty also create the risk of the rates being higher  
4 than actual costs. Based on my understanding of Messrs. DeCoursey and Therrien's  
5 Direct Testimony, their proposal would address that risk and protect customers from  
6 over-collections.

7 **Q. Do you agree with Messrs. DeCoursey and Therrien that the Company would be**  
8 **able to provide the Commission with sufficient information on its actual spending to**  
9 **demonstrate its prudence?**

10 A. Yes, I do. As I understand it, the Company proposes to provide the Commission with a  
11 reconciliation of its authorized and actual costs each year. To support the elements of that  
12 filing that related to cybersecurity, Liberty would expect to provide calculations of the  
13 variance and workpapers to support them; contracts, invoices, and other documentation  
14 of actual spending; the technical specifications of investments made; and narratives that  
15 explain why the variances were necessary and how they support the cybersecurity  
16 Program. Because of the nature of the investments, the Company would provide this  
17 information under confidential treatment.

18 **VI. CONCLUSIONS**

19 **Q. What conclusions have you drawn?**

20 A. My testimony supports five conclusions:

1        *First*, Liberty’s effective management of the cybersecurity threat is critical to its ability to  
2        provide safe, reliable service to its customers.

3        *Second*, the cybersecurity threat is likely to intensify over the next several years.

4        *Third*, the uncertain nature of the cybersecurity threat space means that utilities must be  
5        able to respond quickly to a changing environment.

6        *Fourth*, because needed investments cannot be predicted with certainty and program  
7        changes are likely, the cost of Liberty’s Program cannot be forecast with certainty.

8        *Fifth*, the specification of the Program described in Section V and whose costs are shown  
9        in Table 1 is expected to provide an adequate level of cybersecurity protection at a  
10       reasonable cost, given the information currently available.

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

12    A.    Based on these conclusions, I recommend that the Commission approve the Program  
13       based on the specifications I describe earlier in my testimony and that it approves the  
14       ratemaking proposal made by Messrs. DeCoursey and Therrien to create enough  
15       flexibility that the Company will be able to respond to changing threats.

16    **Q.    Does this conclude your testimony?**

17    A.    Yes.