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

April 28, 2023

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

I. INTRODUCTION

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

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?

A. I am employed by Liberty Utilities Service Corp. as the Director of IT Security, Risk, and Compliance.

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

A. I am testifying on behalf of Liberty Utilities (Granite State Electric) Corp. d/b/a Liberty ("Liberty" 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 The Empire District Electric Company ("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, 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 in a proceeding before the New Hampshire Public Service Commission ("Commission")?

A. No, I have not.

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

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

Q. What is the purpose of your testimony?

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

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 that the Company faces.
- *Section III* describes the concept of critical infrastructure and explains how the term is applicable to Liberty's assets.
- *Section IV* describes the various cybersecurity-related regulations and guidelines to which the Company must adhere and explains why the cost of doing so is increasing.
- *Section* ***Error! Reference source not found.*** describes the financial and operating characteristics of the components that comprise the Program. In that same section,

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

- *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 a high-level explanation of the Program and its basic components and conduct a more extensive discussion of the cybersecurity environment in which Liberty does business. In particular, the highly uncertain and rapidly evolving nature of the cybersecurity threats that the Company must mitigate while doing business in New Hampshire.

Q. Please describe the Program

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

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

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

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

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

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

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

A. The proliferation of new technologies has created 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. I will provide a simple 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 that adds a layer of complexity to the data the Company is required to protect.

Q. What steps are being taken in response?

A. The Company must maintain robust cybersecurity measures that address 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.

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. Is the cybersecurity landscape evolving?

A. Yes, rapidly.

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

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

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

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

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

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 that the Company owns and operates. I then describe how implementing the Program protects those critical assets.

Q. What is critical infrastructure?

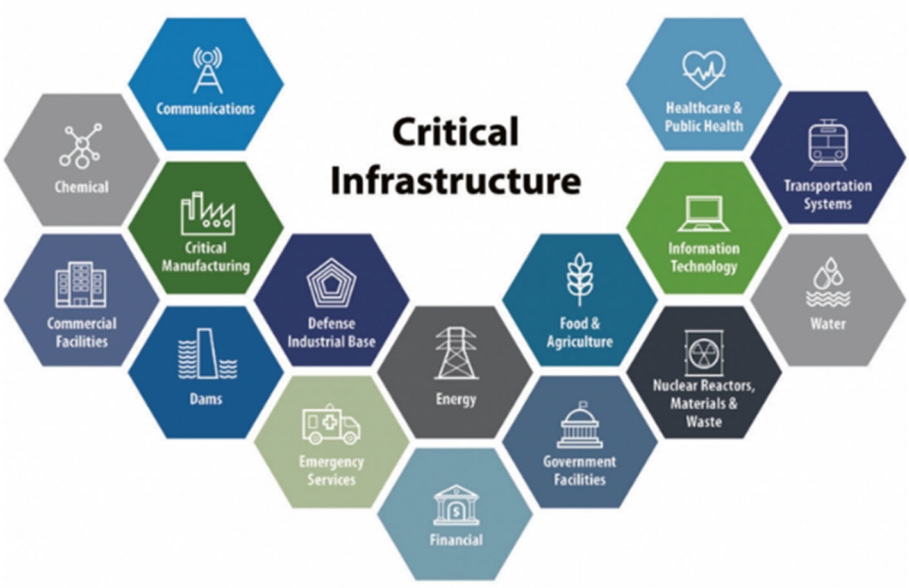
A. The Cybersecurity & Infrastructure Security Agency defines critical infrastructure as "…assets, systems, and networks, whether physical or virtual, [that] are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[1]

[1] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Q. Which sectors of the economy include critical infrastructure?

A. There are sixteen, according to the Cybersecurity and Infrastructure Security Agency, a division of the Department of Homeland Security. The sectors are shown in **Error! Reference source not found.**.

Figure 1. Critical Infrastructure Sectors



Q. Is the Company's distribution system critical infrastructure?

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

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

A. Yes.

Q. What are the specific 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 these essential sectors. Data is vital for the efficient operation and management, of an electrical utility.

Q. Can you provide examples?

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

Q. Please describe Liberty's OT.

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

Q. Please describe the Company's IT.

A. IT is comprised of the systems that 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 it.

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 Program support the Company's ability to mitigate these threats?

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

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

A. Yes, very.

Q. Why?

A. 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"). APUC is an owner and operator of Critical Infrastructure such as electric, gas, water, and wastewater utilities, dams, and communications critical infrastructure. Specific to New Hampshire, the Company owns and operates Energy Critical Infrastructure including electric and gas.

IV. CYBERSECURITY REGULATORY LANDSCAPE

Q. Please summarize this section of your testimony.

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

Q. Who regulates the Company's cybersecurity?

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

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

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

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

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

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

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

A. Yes. Included among them are the NERC Reliability Standards, Sarbanes-Oxley Act ("SOX"), International Organization Standardization ("ISO"), NIST, and New Hampshire's own Puc 306.10 Physical and Cyber Security Plans, Procedures and Reporting requirements 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:

1. Identify: Assess and manage risks by identifying assets, systems, and threats to prioritize cybersecurity needs.
2. Protect: Implement safeguards to limit the impact of potential cybersecurity incidents on critical infrastructure and services.
3. Detect: Continuously monitor systems for signs of breaches or vulnerabilities to swiftly identify and analyze potential threats, both internally and externally.
4. Respond: Develop and execute response strategies to contain, mitigate, and eliminate the impact of detected incidents.
5. 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. Can you please summarize the requirements imposed by the state of New Hampshire regarding cybersecurity, including physical security?

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

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

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

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

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

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

threats in real time." As I discuss in my testimony, APUC's Program and cybersecurity strategy is in line with this recommendation.

V. 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 Program, including the nature of the various investments being made and their costs.

A. Program Configuration

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

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

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

A. $4.93 million.

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

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

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

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

Table 1 Company Cybersecurity Program Spending by Rate Year

Rate Years		Capex ($M)	Opex ($M)
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
Total		$ 4.93	$ 0.22

Q. Are these amounts already included in the Company's cost of service?

A. Yes. The rates proposed by Company witnesses Dane and Jardin include the Company's cost of the cybersecurity program, including the costs to recover the capital investment and operating expenses.[2].

Q. Are any of the assets associated with the capital spending shown in Error! Reference source not found. already in service?

A. Yes. Spending on the Program has already begun, and a small amount of capital has already been placed into service. The RY1 CapEx value shown in **Error! Reference source not found.** includes approximately $0.7M in CapEx that was or will be placed

[2]Dane-Jardin Direct Testimony, p. 23

into service between January 2023 and June 2023. I understand that this approach is consistent with past practice in New Hampshire.

Q. Why is there no OpEx before RY3?

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

Q. How are these costs allocated to the Company?

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

B. Cost Uncertainty

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

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

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

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

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

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

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

Q. Is there any other alternative available?

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

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

Q. Do you agree with Messers. DeCourcey and Therrien that the Company would be able to provide the Commission with sufficient information on its actual spending to demonstrate its prudence?

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

VI. CONCLUSIONS

Q. What conclusions have you drawn?

A. My testimony supports five conclusions:

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

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

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

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

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

Q. What are your recommendations?

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

Q. Does this conclude your testimony?

A. Yes.