BEFORE THE NEW HAMPSHIRE
PUBLIC UTILITIES COMMISSION

DOCKET NO. DE 19-197

DEVELOPMENT OF A STATEWIDE, MULTI-USE ONLINE ENERGY DATA PLATFORM

PREPARED REBUTTAL TESTIMONY OF

MICHAEL MURRAY

ON BEHALF OF MISSION:DATA COALITION

October 23, 2020

TABLE OF CONTENTS

I. INTRODUCTION

Q. WHAT IS THE PURPOSE OF THIS REBUTTAL TESTIMONY?

A. The purpose of my rebuttal testimony is to respond to the testimony of Eversource/Until, who filed joint direct testimony, and Liberty Utilities (together, the "JUNH") filed on August 17, 2020. Specifically, I address the following points: (1) the JUNH's proposal of "Option 3" provides a basis for moving forward, but numerous implementation details and third party requirements must be modified; (2) the JUNH's cybersecurity requirements for third parties should be rejected; (3) the JUNH's conception of third parties as their vendors and not as co-equal market participants is flawed; and (4) I make one modification to my proposal regarding governance.

II. RESPONSE TO JUNH

A. OVERVIEW OF THE JUNH'S PROPOSALS

Q. WHAT OPTIONS FOR A DATA PLATFORM WERE PROPOSED BY THE JUNH?

A. Eversource/Unitil proposed three options for a data platform. Option 1 is the application of Green Button Download My Data ("DMD") to each utility's web portal, allowing customers to download their usage data in a standardized format.

Option 2, described as Eversource/Unitil's "preferred option,"[1] is GBC implemented by each utility individually. Eversource/Unitil state that application programming interfaces ("APIs") will be standardized, with the formats of data received from these APIs will be "exactly the same for each implementing utility."[2] However, each third party DER would need to complete a separate integration with each utility in New Hampshire in this case. Furthermore, customers served by two different utilities – one for electricity, and another for natural gas service – would need to complete two authorizations in order to share their total energy usage, adding some inconvenience.

Option 3 involves GBC but implemented with an "API of APIs," meaning that third parties could access a single API endpoint for all New Hampshire utilities. Eversource/Unitil note that multi-site commercial customers would likely benefit from this approach because web-based authorizations could occur once instead of multiple times.[3] Option 3 also includes a centralized web portal for New Hampshire that provides aggregated data by municipality.

For Options 2 and 3, Eversource/Unitil state that a cost-benefit analysis should performed prior to implementation.[4]

[1] *Joint Testimony of Thomas Belair, Riley Hastings, and Dennis Moore for Eversource And Justin Eisfeller, Kimberly Hood, and Jeremy Haynes for Unitil* (hereafter "*Eversource/Unitil Direct*"). August 17, 2020 at 25:11.

[2] *Id.* at 27:3.

[3] *Id.* at 30:1-2.

[4] See, e.g., *Eversource/Unitil Direct* at 30:17-19.

Finally, Liberty states that its proposal "is essentially the same as that of the other New Hampshire utilities."[5]

Q. WHICH OPTIONS PROPOSED BY THE JUNH SHOULD BE CONSIDERED IN YOUR VIEW AND WHY?

A. Option 1 should be dismissed from consideration. Eversource/Unitil acknowledge that Option 1 "does not provide any automated data sharing."[6] Option 1 does not satisfy the requirements of RSA 378:53, which states that the data platform must "support the Energy Service Provider Interface of the North American Energy Standards Board and the Green Button 'Connect My Data' initiative of the Green Button Alliance." DMD is not Green Button Connect My Data ("GBC") and therefore does not meet the requirements. DMD provides only minimal value to customers and their authorized distributed energy resources ("DERs"), which I also refer to as "third parties." Moreover, Eversource/Unitil acknowledged that they already provide DMD to customers on each utility's respective web portal,[7] so it is unclear why Eversource/Unitil would propose something that does not appear to be different from the status quo.

As for Option 2, I think it should be dismissed for the following reasons. First, Option 2 would require customers served by multiple utilities to grant multiple, separate authorizations in order to share their whole-home or whole-building energy information.

[5] *Direct Testimony of Heather M. Tebbetts and Melissa B. Samenfeld on behalf of Liberty Utilities* (hereafter "*Liberty Direct*"). August 17, 2020 at 14:9.

[6] *Eversource/Unitil Direct* at 24:1.

[7] *Scoping Comments of Eversource, Unitil and Liberty*. Docket No. 19-197. March 11, 2020 at 3.

For example, an energy efficiency consultant may require both electricity and natural gas usage in order to accurately evaluate the cost-effectiveness of switching to heat pumps. Requiring a customer to create a login and password on two utilities' websites before they can consummate a data-sharing authorization will be a significant barrier to adoption and will reduce the utilization of, and ratepayer value derived from, the data platform. As I stated in direct testimony, one of the key lessons learned from Smart Meter Texas ("SMT") is that requiring customers to create an unnecessary login and password led to slow consumer uptake.[8]

Second, Option 2 should be discarded because, despite Eversource/Unitil's commitment that "the interface for these APIs, as well as the data formats returned will be exactly the same for each implementing utility,"[9] experience has shown that when each utility implements their own GBC APIs, there are several ways that these implementations can diverge, creating significant unnecessary costs to third parties and undermining the objective of state-wide consistency. For example, the California utilities have different requirements for third parties' Secure Socket Layers ("SSL") certificates that are a prerequisite to interact with GBC. Three GBC implementations in New Hampshire – even if the APIs are "identical" – could nonetheless triple the administrative back-and-forth between utilities and third parties due to management of SSL certificates. Managing a single API and SSL certificate is much more streamlined

[8] *Direct Testimony of Michael Murray on Behalf of Mission:data Coalition* (hereafter "*Murray Direct*"). August 17, 2020 at 35:3-18.

[9] *Eversource/Unitil Direct* at 27:2-3.

and efficient than managing three. In addition, the customer experience during the authorization process could be dramatically different between utilities – even if the APIs are consistent – meaning that third parties' customer education materials would need to be customized for each utility, increasing costs. Finally, there are certain "degrees of freedom" in the GBC standard itself. Even if certified as GBC compliant by the Green Button Alliance, three implementations in New Hampshire could still have differences that would require third parties to develop and maintain bespoke software for each. For example, OAuth flows and token exchanges; PUSH vs. PULL configurations; and whether "bulk" historic data are compressed and transmitted over FTP or HTTP can all vary, despite attaining Green Button Alliance certification. Option 2 adds unnecessary and costly limitations on the DER market in New Hampshire.

Third, Option 2 should be dismissed because New Hampshire's small size means that third party DERs will be unlikely to justify the investment in three GBC software integrations. This is particularly true for Liberty and Unitil, who have small customer bases of only a few tens of thousands of customers. There is a cost to DERs of maintaining software for each API endpoint. Economic necessity requires DERs to make investments according to perceived potential returns, and the reality is that it will be harder for DERs to economically justify supporting Liberty and Unitil's GBC implementations when only small customer bases can be reached with that investment.

Finally, Eversource/Unitil misapprehend Option 2's detrimental effects; my experience in other jurisdictions demonstrates the shortfalls and drawbacks of Option 2. Eversource/Unitil testify that "the incremental benefit [of Option 3] would likely be

minimal" as compared with Option 2.[10] However, Eversource/Unitil provide no evidence behind this assertion. In discovery, Eversource/Unitil admitted that they made no effort to analyze or quantify the incremental value of Option 3 over Option 2.[11] This is in contrast with my direct testimony, in which I provided several qualitative and quantitative assessments demonstrating that the imposition of unnecessary "hurdles" for customers, such as additional online logins, will significantly diminish the value of the data platform in New Hampshire. Testifying that "Usability considerations can impact customer utilization rates by literally an order of magnitude," I cited as evidence a study by demand response firm EnergyHub that found a streamlined, online customer enrollment process saw 42% participation rates as compared to 3% when the process was clumsy, difficult, and required many steps.[12] I also mentioned SMT. Although it is more closely related to Option 3 in its overall design, an unnecessary requirement for customers to create a login and password at smartmetertexas.com was a large contributing factor to SMT's low utilization rate and the subject of substantial, years-long litigation.[13] Eversource/Unitil underappreciate the value of the customer experience in granting an authorization, and this is evidenced by the fact that they did not conduct any assessment of how multiple authorization processes for each utility would impose burdens on customers served by multiple utilities. I further noted that only 20%-30% of

[10] *Eversource/Unitil Direct* at 29:26-27.

[11] Exhibit 1. Response of Eversource/Unitil to Mission:data 1-002, dated September 15, 2020.

[12] *Murray Direct* at 48:13 – 49:7.

[13] *Id.* at 34:19 – 35:18, 48:9-12.

JUNH customers appear to have an online account established at their utility.[14] Requiring many customers to create *two* logins and passwords at the utilities' websites serving them is unnecessary and would diminish the overall value of the data platform in New Hampshire.

As for Option 3, I believe that the "API of APIs" is the best overall approach and, generally speaking, it comports with the recommendations I provided in direct testimony. However, I disagree with several aspects of the JUNH's proposal and claims made by the JUNH, as I describe below.

B. CYBERSECURITY AND PRIVACY REQUIREMENTS

Q. REGARDING OPTION 3, WHAT PRIVACY OR CYBERSECURITY REQUIREMENTS DO EVERSOURCE/UNITIL PROPOSE FOR THIRD PARTIES?

A. Eversource/Unitil discuss numerous cybersecurity and privacy requirements. Some are vague, while some are specific. For example, Eversource/Unitil state that the data platform should be subject to the U.S. Department of Energy's DataGuard privacy standard ("DataGuard");[15] federal regulations governing records retention;[16] state breach notification law;[17] the NIST Cybersecurity Framework;[18] NIST guidelines for

[14] *Murray Direct* at 35, footnote #32.

[15] *Eversource/Unitil Direct* at 36:16-17.

[16] *Id.* at 40:24-25.

[17] *Id.* at 40:26.

[18] *Id.* at 46:9-10.

smart grid cybersecurity (NISTIR 7628);[19] an unspecified governance policy;[20] an unspecified set of data protection controls;[21] and a vaguely-defined change management process.[22] I note that the aforementioned requirements apply to the utilities, not third parties.

As for third parties specifically, Eversource/Unitil propose several requirements. First, third parties must complete an as-yet-unspecified cybersecurity assessment. Second, according to Eversource/Unitil, third parties must sign a mutual non-disclosure agreement ("NDA"). Third, Eversource/Unitil state vaguely that additional NDAs from different departments may be required: "Additional NDAs from departments such as purchasing or IT may also be required, as appropriate."[23] Fourth, third parties should be subject to "external assessment and audit for security management controls."[24]

Q. ARE THESE PROPOSED REQUIREMENTS FOR THIRD PARTIES DEFINED?

A. No. Regarding the cybersecurity assessment, Eversource/Unitil stated in a discovery response that "There are various industry standard questionnaires that are designed to assess third party controls in place for the protection of information," but

[19] *Id.* at 40:18-20.

[20] *Id.* at 44:3-24 ("Policies must be developed to define the data governance structure, secure data access and usage, and to ensure data integrity for successful integration").

[21] *Id.* at 40:17 – 42:16 ("The Utilities plan to incorporate process and system controls into the platform, commensurate with the risk to customer privacy as well as critical infrastructure").

[22] *Id.* at 45:21 – 46:7.

[23] *Id.* at 42:25-26.

[24] *Id.* at 45:5-6.

Eversource/Unitil did not specify which assessment they proposed to use.[25] Regarding the NDA, Eversource/Unitil admitted in discovery that "NDAs have not been developed for use with the data platform."[26] As for additional NDAs from purchasing or IT departments, Eversource/Unitil provided three different NDAs in a discovery response but did not specify which NDA would apply under which circumstances ("The Utilities expect the NDA process to be delineated with the rollout of the platform").[27] With regard to "external assessment and audit," Eversource/Unitil's direct testimony is vague, stating only that "Platform users that utilize and store customer data should be subject to external assessment and audit for security management controls."[28] When asked in discovery "Exactly what kind of 'external assessment' or 'audit' are the Joint Utilities proposing?", Eversource/Unitil answered only tentatively, stating "The most common audit type is a SOC 3 audit."[29]

Q. WHAT PRIVACY OR CYBERSECURITY REQUIREMENTS DOES LIBERTY PROPOSE FOR THIRD PARTIES?

A. Liberty proposes that third parties must "satisfy utility review of compliance with privacy standards relative to RSA 363:38, and requirements as established in RSA

[25] Exhibit 2. Response of Eversource/Unitil to Mission:data 1-011, dated September 15, 2020.

[26] Exhibit 3. Response of Eversource/Unitil to Mission:data 1-010(a), dated September 15, 2020

[27] *Id.*, Response of Eversource/Unitil to Mission:data 1-010(b), dated September 15, 2020.

[28] *Eversource/Unitil Direct* at 45:5-6.

[29] Exhibit 4. Response of Eversource/Unitil to Mission:data 1-012, dated September 15, 2020.

378:51, II. This will include a vendor cyber security review by utilities using a common questionnaire."[30]

Q. IS THAT PROPOSED REQUIREMENT FOR THIRD PARTIES DEFINED?

A. No. What would "satisfy" Liberty with regard to privacy requirements pursuant to RSA 363:38 and RSA 378:51, II is not articulated. Furthermore, while third parties would be required to adhere to Liberty's cybersecurity requirements, Liberty admitted in discovery that "The Company does not have a formal cybersecurity proposal at this time."[31]

Q. WHAT CONCERNS YOU ABOUT THESE REQUIREMENTS FOR THIRD PARTIES PROPOSED BY THE JUNH?

A. I have two serious concerns with the JUNH's eligibility proposals. First, it would be wholly inappropriate for the Commission to approve third party eligibility requirements that are unknown or unspecified. When the Commission issues an order, such orders have the force of law. A law that requires third parties to adhere to the JUNH's unknown or unspecified requirements is inherently unfair: It is a moving target, impossible to satisfy, and subject to change at any moment, based upon a utility's whim. Indeed, Liberty admitted in discovery that its cybersecurity requirements are not "pass/fail" and cannot be objectively determined because "there will always be some

[30] *Liberty Direct* at 27:9-11.

[31] Exhibit 5. Response of Liberty Utilities to Mission:data 1-4, dated September 15, 2020.

level of judgment in reviewing control environments."[32] The net result of Commission approval of the JUNH's proposal would be for the utilities to have virtually unlimited power over third parties to restrict access to information on fabricated grounds that are arbitrary, discriminatory or capricious. Such an approval would be an abdication of the Commission's responsibility to restrain utilities' monopoly power.

Instead, I argued in my direct testimony for a much fairer and more transparent approach. Any third party eligibility criteria must be specific and articulable. I proposed these eligibility criteria: third parties must (i) provide contact information to the JUNH, (ii) demonstrate technical interoperability with the GBC platform, (iii) accept certain terms and conditions, to be approved by the Commission, including adherence to DataGuard; and (iv) not be on the Commission's list of "banned" or prohibited third parties.

Second, as a corollary to the above, the Commission should never approve third party eligibility criteria that are not stated on the record as a result of confidentiality claims. When asked in discovery to provide a copy of any documents detailing Liberty's "utility review of [third party's] compliance with privacy standards," Liberty refused to do so, stating that its enterprise-wide cybersecurity plan is confidential.[33] Similarly, Eversource/Unitil refused to provide its information technology cybersecurity policies and guidelines due to confidentiality.[34] If the JUNH wanted the Commission to consider its eligibility proposals, it should have defined them clearly and put them in testimony.

[32] Exhibit 2. Response of Liberty to Mission:data 1-11, dated September 15, 2020

[33] Exhibit 5.

[34] Exhibit 6. Response of Eversource/Unitil to Mission:data 1-005, dated September 15, 2020

However, the JUNH did not take that opportunity and are instead hiding behind a veil of secrecy.

For the Commission to approve the JUNH's proposals for cybersecurity requirements of third parties would inappropriately surrender the Commission's authority to the JUNH. It would throw wide open a door for the utilities to discriminate against certain third parties that the utilities do not like, or that the utilities perceive as a competitor, without any objective, reasonable or consistent basis. By way of analogy, approval of the JUNH's proposals for third party cybersecurity requirements would be akin to rescinding the Commission's interconnection requirements for rooftop solar in New Hampshire and appointing the JUNH as the sole authority regarding interconnection matters. I also note that no other jurisdiction in the United States permits utilities to create their own cybersecurity requirements or modify them over time. For these reasons, the JUNH's cybersecurity proposals in this regard should be dismissed.

C. THE DOUBLE STANDARD OF CYBERSECURITY REQUIREMENTS

Q. DO YOU HAVE OTHER OBJECTIONS TO THE JUNH'S PROPOSAL REGARDING THIRD PARTY CYBERSECURITY REQUIREMENTS?

A. Yes. The JUNH's cybersecurity requirements represent a double standard. This is true in several respects. First, the JUNH's cybersecurity requirements are far outside the norm as compared with other jurisdictions. As I described in direct testimony, the

JUNH dedicate pages upon pages of their testimony to the threats posed by third parties accessing customer energy usage data, arguing that the JUNH must have the ability to conduct cybersecurity audits and disqualify third parties who fail to meet standards for encryption and access controls. And yet, at the same time, Eversource acknowledges that the radio broadcasts from its automated meter reading ("AMR") meters are *unencrypted*. This means that anyone can purchase a $60 mini-computer such as a Raspberry Pi, configure its software-defined radio, and drive around neighborhoods in New Hampshire reading customers' AMR meters every few seconds *without any limitation whatsoever*. I note that free and open-source software tools already exist that can be downloaded from the internet for precisely this purpose.[35] The JUNH claim that privacy and security are of "paramount" importance,[36] and yet Eversource has chosen not to employ basic encryption on their AMR meters. Put simply, this is rank hypocrisy. The JUNH's cybersecurity concerns are being selectively applied to third parties without any rational basis.

I note other double standards as well. Both Eversource/Unitil[37] and Liberty[38] state that they provide interval usage data to various entities by email today. And yet they do not require email recipients to adhere to cybersecurity requirements, audits and non-

[35] A free and open-source software library for reading Itron's AMR broadcasts on the 900MHz band can be found at https://github.com/bemasher/rtlamr.

[36] *Eversource/Unitil Direct* at 19:4.

[37] Exhibit 7. Response of Eversource/Unitil to Local Government Coalition LGC2-004(a), dated October 2, 2020

[38] *Liberty Direct* at 10:16-17.

disclosure agreements. If the JUNH sincerely believed that third party possession of customer interval energy usage data was their responsibility to police, they would immediately cease the practice of emailing usage data and demand that recipients adhere to the JUNH's stated cybersecurity requirements. Of course, this has not happened.

In addition, Eversource/Unitil do not require retail suppliers, who directly interact with the utilities' IT systems, to abide by cybersecurity requirements. When asked in discovery, "Please confirm that retail suppliers accessing Unitil's EDI system(s) must agree to abide by Attachment E pages 1-3, 'Unitil Vendor Security Requirements'," Unitil responded: "At this time, retail suppliers are not required to abide by the Unitil Vendor Security Requirements."[39] Similarly, when asked in discovery, "Please confirm that Eversource does not have any cybersecurity requirements that apply to retail suppliers using EDI," Eversource responded: "Eversource does not have cybersecurity requirements for retail suppliers because we do not have a contractual relationship with them."[40] Even though retailers have direct interactions with utilities' IT systems – supposedly the basis of their argument to impose cybersecurity requirements upon third parties using GBC – Eversource/Unitil have transmitted thousands of customers' energy usage and account information to outside entities via automated, electronic

[39] Exhibit 8. Response of Eversource/Unitil to Mission:data 2-005, dated October 2, 2020.

[40] *Id.*

transactions. I therefore conclude that the JUNH's proposed cybersecurity requirements of third parties in this docket are being selectively applied without basis.

Q. ARE YOU ARGUING THAT ALL CYBERSECURITY REQUIREMENTS ARE INAPPROPRIATE?

A. No. The JUNH should employ reasonable cybersecurity standards in *their* implementation of the GBC platform, but the JUNH should not impose cybersecurity requirements *on third parties* beyond DataGuard, as I have proposed. As for the JUNH's responsibility to manage its own IT systems, the GBC standard requires encryption in transit using SSL and, perhaps most importantly, refuses to send any customer information to a third party without the customer's consent. As for third parties, I proposed in direct testimony a requirement that third parties should adhere to the U.S. Department of Energy's DataGuard standard. The DataGuard standard requires third parties to adhere to numerous privacy protections and security controls, and is enforceable by the Federal Trade Commission. Together, I believe these requirements are reasonable, and they are consistent with other jurisdictions' requirements. I note that requiring DataGuard of third parties even goes beyond some jurisdictions' requirements for third parties in terms of privacy and security protection, such as California's and Colorado's. My point is that the JUNH's cybersecurity requirements proposed *for third parties* are arbitrary and excessive. This is particularly true when compared with Eversource's practice of declining to encrypt AMR meter radio

broadcasts, and sending interval usage data to various entities via unencrypted email without audit or adherence to cybersecurity standards.

Q. WHAT DOES THE JUNH'S CYBERSECURITY REQUIREMENTS FOR THIRD PARTIES SAY ABOUT THE RELATIONSHIP BETWEEN UTILITIES AND THIRD PARTIES?

A. Unfortunately, the cybersecurity requirements for third parties proposed by the JUNH demonstrate that the JUNH view third parties as their vendors, and not co-equal market actors. I believe this understanding is deeply flawed. The JUNH wish to treat third parties as subservient; the number and type of cybersecurity requirements proposed by the JUNH sound remarkably similar to those imposed on the JUNH's IT vendors, such as Customer Information System providers Oracle and SAP. In fact, Eversource/Unitil's testimony reveals that they perceive no distinction between third parties and their own vendors. Eversource/Unitil cite a Ponemon Institute study, "Data Risk in the Third-Party Ecosystem," stating that 56% of enterprises were involved with third parties who experienced some form of breach. The key point is "third party," which is defined very differently in the Ponemon Institute study than the definition I use here. In the study's key findings, the authors state that the survey applies to "organizations' approach to managing data risks created through outsourcing."[41] However, third party

[41] Ponemon Institute study at 5. https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/sep2017/cs2017_0340.pdf.

DERs are not "outsourced" vendors to utilities. Third party DERs do not exist to meet the JUNH's operational or business needs. Instead, third party DERs are serving *customers* and their energy management and cost management needs, and may have only an incidental relationship with a utility.

I believe the JUNH's fundamental misunderstanding can be addressed by limiting the JUNH's liability for data misuse risks as I discussed in direct testimony. The JUNH's proposals assume that the JUNH are responsible for the acts of third parties, when that should not be the case.

Q. PLEASE EXPLAIN "SYSTEM RISK" AND "DATA MISUSE RISK."

A. Based on the JUNH's direct testimony, I believe the JUNH have conflated two cybersecurity and privacy risks: "system risk" and "data misuse risk." System risk is the risk that a third party or "bad actor" will infiltrate the utilities' IT systems simply as a result of having some level of access. Put simply, the mere existence of a GBC platform creates some level of system risk. In contrast, data misuse risk is the risk that a third party will misuse a customer's data after it has received legitimate permission from a customer to access his or her data. It is absolutely essential that the Commission understand the distinctions between these two risks and how to address them.

Q. HOW SHOULD SYSTEM RISK AND DATA MISUSE RISK BE ADDRESSED?

A. I believe system risks can be successfully mitigated. It can be accomplished through careful implementation and adherence to the GBC standard. The GBC standard requires that data transmitted be encrypted using Transport Layer Security (TLS) version 1.2 and, most importantly, it only permits data to be exchanged if a customer has granted opt-in consent to the utility. When the customer grants consent to the utility, a secure token is generated. It is only with the correct token that a third party can access customer information. If a third party fabricates a token or submits a false token with a data request, it is the utility's obligation to reject it. System risk must be addressed solely by the utilities; it would be inappropriate to make third parties responsible for the GBC platform. All of this is to say that if the GBC platform is vulnerable to attack by a third party, that is due to the utilities' imprudent management.

Q. HOW SHOULD DATA MISUSE RISK BE ADDRESSED?

A. As I described in my direct testimony, data misuse risk can be addressed with the Commission establishing third party eligibility criteria, including adherence to DataGuard, and the enforcement procedures I outlined.

Q. WHAT IS MULTI-FACTOR AUTHENTICATION (MFA)?

A. MFA is the practice of verifying customer identity by using more than one piece of information. For example, instead of merely a login/password combination, MFA could involve sending a code to the email address of a registered customer account or in a text message to the customer's cell phone. The customer would enter that code into a website as additional "factors" to verify their identity. Both Eversource/Unitil and Liberty have testified that the data platform should require customers to complete MFA prior to directing the exchange of any customer information.

Q. DO YOU OBJECT TO MFA?

A. I do not have an inherent objection to MFA itself. However, I object to inconsistencies between the authentication practices of the utilities' customer web portals and the data platform. As I stated in direct testimony, one of the lessons learned from GBC implementations in other jurisdictions is the "no more onerous" principle, which states that the customer authorization process should be no more onerous than the process a utility requires for a similar online transaction. The JUNH do not require MFA on their existing web portals. In a discovery response, Eversource/Unitil stated, "The Utilities do not currently require two-factor or multi-factor authentication (MFA)."[42] Similarly, Liberty stated in a discovery response that "Liberty does not currently require

[42] Exhibit 9. Response of Eversource/Unitil to Mission:data 1-004, dated September 15, 2020.

two-factor or multi-factor authentication."[43] Failure to adopt this principle in New Hampshire will result in inadvertently creating an incentive for third parties to use credential-sharing to access customer information, rather than use the data platform. I therefore reiterate my proposal from direct testimony that the authorization process should not involve any steps that deviate from the JUNH's existing authentication practices. If the JUNH ultimately implement MFA for their web portals, then data-sharing authentication practices should be symmetrical. However, the asymmetry proposed by the JUNH is unnecessary, confusing to customers, and would diminish the utilization of, and ratepayer value derived from, the data platform.

III. GOVERNANCE

Q. DO YOU HAVE ANY CHANGES TO YOUR RECOMMENDATIONS PROVIDED IN DIRECT TESTIMONY REGARDING GOVERNANCE?

A. Yes. I neglected to mention that the Office of the Consumer Advocate ("OCA") should act as chair of the Governance Committee. Aside from this, all of my previous recommendations remain unchanged.

[43] Exhibit 10. Response of Liberty to Mission:data 1-3, dated September 15, 2020.

IV. CONCLUSION

Q. WHAT IS YOUR CONCLUSION?

A. The JUNH propose several elements of a data platform (including MFA and cybersecurity requirements for third parties) that have been shown to deviate from best practices as learned in other jurisdictions. If Option 3 is approved by the Commission as proposed, the data platform will not be a success in New Hampshire.

Q. DOES THIS CONCLUDE YOUR REBUTTAL TESTIMONY?

A. Yes.