



October 23, 2020

Via Email

Ms. Debra A. Howland
Executive Director
New Hampshire Public Utilities Commission
21 South Fruit Street, Suite 10
Concord, New Hampshire 03301
ExecutiveDirector@puc.nh.gov

**Re: Docket No. DE 19-197,
Prepared Rebuttal Testimony of Michael Murray on Behalf of Mission:data
Coalition, and Exhibits**

Please find enclosed the rebuttal testimony of Michael Murray on behalf of Mission:data Coalition, including Exhibits in the above-referenced docket.

Pursuant to the Commission's emergency directive relating to the ongoing pandemic, cover letter and testimony are being filed in electronic form only, and no hard copies are being submitted.

Respectfully submitted,

/s/
Michael Murray, President
Mission:data Coalition
1752 NW Market St #1513
Seattle, WA 98107
(510) 910-2281 (phone)
michael@missiondata.io

email cc: Parties to Docket No. DE 19-197

1 **BEFORE THE NEW HAMPSHIRE**
2 **PUBLIC UTILITIES COMMISSION**

3
4
5
6 DOCKET NO. DE 19-197

7
8 DEVELOPMENT OF A STATEWIDE, MULTI-USE ONLINE ENERGY DATA
9 PLATFORM

10
11
12
13
14 **PREPARED REBUTTAL TESTIMONY OF**
15 **MICHAEL MURRAY**
16 **ON BEHALF OF MISSION:DATA COALITION**

17
18
19
20
21
22
23
24
25
26
27
28 October 23, 2020

1
2
3
4
5
6
7
8
9
10
11

TABLE OF CONTENTS

I.	INTRODUCTION	3
II.	RESPONSE TO JUNH	3
A.	OVERVIEW OF THE JUNH'S PROPOSALS.....	3
B.	CYBERSECURITY AND PRIVACY REQUIREMENTS.....	9
C.	THE DOUBLE STANDARD OF CYBERSECURITY REQUIREMENTS	14
III.	GOVERNANCE	22
IV.	CONCLUSION	23

1

I. INTRODUCTION**2 Q. WHAT IS THE PURPOSE OF THIS REBUTTAL TESTIMONY?**

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

11

12

II. RESPONSE TO JUNH**13 A. OVERVIEW OF THE JUNH’S PROPOSALS****14 Q. WHAT OPTIONS FOR A DATA PLATFORM WERE PROPOSED BY THE
15 JUNH?**

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

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

9 Option 3 involves GBC but implemented with an "API of APIs," meaning that third
10 parties could access a single API endpoint for all New Hampshire utilities.

11 Eversource/Unitil note that multi-site commercial customers would likely benefit from
12 this approach because web-based authorizations could occur once instead of multiple
13 times.³ Option 3 also includes a centralized web portal for New Hampshire that provides
14 aggregated data by municipality.

15 For Options 2 and 3, Eversource/Unitil state that a cost-benefit analysis should
16 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.

1 Finally, Liberty states that its proposal “is essentially the same as that of the other
2 New Hampshire utilities.”⁵

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

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

16 As for Option 2, I think it should be dismissed for the following reasons. First,
17 Option 2 would require customers served by multiple utilities to grant multiple, separate
18 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.

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

9 Second, Option 2 should be discarded because, despite Eversource/Unitil's
10 commitment that "the interface for these APIs, as well as the data formats returned will
11 be exactly the same for each implementing utility,"⁹ experience has shown that when
12 each utility implements their own GBC APIs, there are several ways that these
13 implementations can diverge, creating significant unnecessary costs to third parties and
14 undermining the objective of state-wide consistency. For example, the California utilities
15 have different requirements for third parties' Secure Socket Layers ("SSL") certificates
16 that are a prerequisite to interact with GBC. Three GBC implementations in New
17 Hampshire – even if the APIs are "identical" – could nonetheless triple the
18 administrative back-and-forth between utilities and third parties due to management of
19 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.

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

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

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

1 minimal” as compared with Option 2.¹⁰ However, Eversource/Unitil provide no evidence
2 behind this assertion. In discovery, Eversource/Unitil admitted that they made no effort
3 to analyze or quantify the incremental value of Option 3 over Option 2.¹¹ This is in
4 contrast with my direct testimony, in which I provided several qualitative and quantitative
5 assessments demonstrating that the imposition of unnecessary “hurdles” for customers,
6 such as additional online logins, will significantly diminish the value of the data platform
7 in New Hampshire. Testifying that “Usability considerations can impact customer
8 utilization rates by literally an order of magnitude,” I cited as evidence a study by
9 demand response firm EnergyHub that found a streamlined, online customer enrollment
10 process saw 42% participation rates as compared to 3% when the process was clumsy,
11 difficult, and required many steps.¹² I also mentioned SMT. Although it is more closely
12 related to Option 3 in its overall design, an unnecessary requirement for customers to
13 create a login and password at smartmetertexas.com was a large contributing factor to
14 SMT’s low utilization rate and the subject of substantial, years-long litigation.¹³
15 Eversource/Unitil underappreciate the value of the customer experience in granting an
16 authorization, and this is evidenced by the fact that they did not conduct any
17 assessment of how multiple authorization processes for each utility would impose
18 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.

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

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

9 **B. CYBERSECURITY AND PRIVACY REQUIREMENTS**

10 **Q. REGARDING OPTION 3, WHAT PRIVACY OR CYBERSECURITY** 11 **REQUIREMENTS DO EVERSOURCE/UNITIL PROPOSE FOR THIRD PARTIES?**

12 A. Eversource/Unitil discuss numerous cybersecurity and privacy requirements.
13 Some are vague, while some are specific. For example, Eversource/Unitil state that the
14 data platform should be subject to the U.S. Department of Energy's DataGuard privacy
15 standard ("DataGuard");¹⁵ federal regulations governing records retention;¹⁶ state
16 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.

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

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

12 **Q. ARE THESE PROPOSED REQUIREMENTS FOR THIRD PARTIES DEFINED?**

13 A. No. Regarding the cybersecurity assessment, Eversource/Unitil stated in a
14 discovery response that “There are various industry standard questionnaires that are
15 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.

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

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

15 A. Liberty proposes that third parties must “satisfy utility review of compliance with
16 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.

1 378:51, II. This will include a vendor cyber security review by utilities using a common
2 questionnaire.”³⁰

3 **Q. IS THAT PROPOSED REQUIREMENT FOR THIRD PARTIES DEFINED?**

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

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

11 A. I have two serious concerns with the JUNH’s eligibility proposals. First, it would
12 be wholly inappropriate for the Commission to approve third party eligibility
13 requirements that are unknown or unspecified. When the Commission issues an order,
14 such orders have the force of law. A law that requires third parties to adhere to the
15 JUNH’s unknown or unspecified requirements is inherently unfair: It is a moving target,
16 impossible to satisfy, and subject to change at any moment, based upon a utility’s whim.
17 Indeed, Liberty admitted in discovery that its cybersecurity requirements are not
18 “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.

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

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

12 Second, as a corollary to the above, the Commission should never approve third
13 party eligibility criteria that are not stated on the record as a result of confidentiality
14 claims. When asked in discovery to provide a copy of any documents detailing Liberty’s
15 “utility review of [third party’s] compliance with privacy standards,” Liberty refused to do
16 so, stating that its enterprise-wide cybersecurity plan is confidential.³³ Similarly,
17 Eversource/Unitil refused to provide its information technology cybersecurity policies
18 and guidelines due to confidentiality.³⁴ If the JUNH wanted the Commission to consider
19 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

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

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

15

16 **C. THE DOUBLE STANDARD OF CYBERSECURITY REQUIREMENTS**

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

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

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

15 I note other double standards as well. Both Eversource/Unitil³⁷ and Liberty³⁸ state
16 that they provide interval usage data to various entities by email today. And yet they do
17 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.

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

6 In addition, Eversource/Unitil do not require retail suppliers, who directly interact
7 with the utilities' IT systems, to abide by cybersecurity requirements. When asked in
8 discovery, "Please confirm that retail suppliers accessing Unitil's EDI system(s) must
9 agree to abide by Attachment E pages 1-3, 'Unitil Vendor Security Requirements'," Unitil
10 responded: "At this time, retail suppliers are not required to abide by the Unitil Vendor
11 Security Requirements."³⁹ Similarly, when asked in discovery, "Please confirm that
12 Eversource does not have any cybersecurity requirements that apply to retail
13 suppliers using EDI," Eversource responded: "Eversource does not have cybersecurity
14 requirements for retail suppliers because we do not have a contractual relationship with
15 them."⁴⁰ Even though retailers have direct interactions with utilities' IT systems –
16 supposedly the basis of their argument to impose cybersecurity requirements upon third
17 parties using GBC – Eversource/Unitil have transmitted thousands of customers' energy
18 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.*

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

3 **Q. ARE YOU ARGUING THAT ALL CYBERSECURITY REQUIREMENTS ARE**
4 **INAPPROPRIATE?**

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

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

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

6 A. Unfortunately, the cybersecurity requirements for third parties proposed by the
7 JUNH demonstrate that the JUNH view third parties as their vendors, and not co-equal
8 market actors. I believe this understanding is deeply flawed. The JUNH wish to treat
9 third parties as subservient; the number and type of cybersecurity requirements
10 proposed by the JUNH sound remarkably similar to those imposed on the JUNH's IT
11 vendors, such as Customer Information System providers Oracle and SAP. In fact,
12 Eversource/Unitil's testimony reveals that they perceive no distinction between third
13 parties and their own vendors. Eversource/Unitil cite a Ponemon Institute study, "Data
14 Risk in the Third-Party Ecosystem," stating that 56% of enterprises were involved with
15 third parties who experienced some form of breach. The key point is "third party," which
16 is defined very differently in the Ponemon Institute study than the definition I use here.
17 In the study's key findings, the authors state that the survey applies to "organizations'
18 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.

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

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

9 **Q. PLEASE EXPLAIN “SYSTEM RISK” AND “DATA MISUSE RISK.”**

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

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

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

13 **Q. HOW SHOULD DATA MISUSE RISK BE ADDRESSED?**

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

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

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

9 **Q. DO YOU OBJECT TO MFA?**

10 A. I do not have an inherent objection to MFA itself. However, I object to
11 inconsistencies between the authentication practices of the utilities' customer web
12 portals and the data platform. As I stated in direct testimony, one of the lessons learned
13 from GBC implementations in other jurisdictions is the "no more onerous" principle,
14 which states that the customer authorization process should be no more onerous than
15 the process a utility requires for a similar online transaction. The JUNH do not require
16 MFA on their existing web portals. In a discovery response, Eversource/Unitil stated,
17 "The Utilities do not currently require two-factor or multi-factor authentication (MFA)."⁴²
18 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.

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

10

III. GOVERNANCE

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

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

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

1

IV. CONCLUSION

2 **Q. WHAT IS YOUR CONCLUSION?**

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

7 **Q. DOES THIS CONCLUDE YOUR REBUTTAL TESTIMONY?**

8 A. Yes.

**Public Service of New Hampshire d/b/a Eversource Energy
Unitil Energy Systems, Inc. and Northern Utilities, Inc. (together
Unitil)**

Docket No. DE 19-197

Date Request Received: 08/31/2020

Request No. MISSION 1-002

Request from: Mission:Data Coalition

Date of Response: 09/15/2020

Page 1 of 1

Witness: Justin Eisfeller, Christine Riley Hastings

Request:

See 29:26-27, discussing Option 3: "For individual residential customers, the incremental benefit would likely be minimal."

- a. Why do the Joint Utilities believe the incremental benefit of Option 3 would be "minimal"? Please explain.
- b. Did the Joint Utilities make any effort to analyze or quantify the incremental value of Option 3 over Option 2 to residential customers? If so, please provide copies of all relevant documents.

Response:

- a. Individual residential customers in New Hampshire are generally served by a single utility (for electric service), and a subset of those customers may have a second utility if they also have gas service. In that the incremental benefit referenced in the testimony is the ability to aggregate data sets across utilities, and that most residential customers have service from a single utility, for those customers with a single utility's service there would be little or no incremental benefit to them from Option 3. For the subset of customers with two utilities, there would be some incremental benefit in aggregating data, but much of the same benefit of aggregation could be accomplished through manual or programmatic means, likely at lower cost than implementing Option 3.
- b. No. The Utilities expect that an incremental benefit/cost analysis will be done prior to a final decision. Much work needs to be done by all the stakeholders to establish a model for this analysis before it can be performed.

**Public Service of New Hampshire d/b/a Eversource Energy
Unitil Energy Systems, Inc. and Northern Utilities, Inc. (together
Unitil)**

Docket No. DE 19-197

Date Request Received: 08/31/2020

Request No. MISSION 1-011

Request from: Mission:Data Coalition

Date of Response: 09/15/2020

Page 1 of 1

Witness: Kimberly Hood, Dennis E. Moore

Request:

See 42-43 concerning a common cyber security assessment process.

- a. Are the Joint Utilities proposing an assessment that can be objectively evaluated on a pass/fail basis?
- b. Are the Joint Utilities proposing that they use their discretion in determining a third party's eligibility?
- c. What did the Joint Utilities mean by "monitoring of third-parties for appropriate use of data"? How would this monitoring be conducted in practice?

Response:

- a. There are various industry standard questionnaires that are designed to assess third party controls in place for the protection of information. The Financial Services industry uses BASEL, for example, the electric industry has developed a standard questionnaire based on NIST controls, and the audit industry uses SOC 1, 2 and 3 type audits. None of these assessments are pass/fail. They assess the controls and their effectiveness. Then the user must determine if this is acceptable for the nature of the data.
- b. There will always be some level of judgement in reviewing control environments as every organization has different controls. Minimum expected control objectives can be established to ensure a consistent review process. However, the more structure and definition required, the less flexibility the third party has to meet the objective of protecting the information in a cost-effective manner.
- c. Monitoring could include either the Utilities or an independent party meeting with the data holder and auditing the use of the data. Monitoring could also include a service that monitors the Dark Web to identify customer data that may have been stolen or put out for sale.

**Public Service of New Hampshire d/b/a Eversource Energy
Unitil Energy Systems, Inc. and Northern Utilities, Inc. (together
Unitil)**

Docket No. DE 19-197

Date Request Received: 08/31/2020

Request No. MISSION 1-010

Request from: Mission:Data Coalition

Date of Response: 09/15/2020

Page 1 of 1

Witness: Justin Eisfeller, Christine Riley Hastings, Dennis E. Moore

Request:

See 42:22-26 regarding non-disclosure agreements (NDAs).

- a. Have the Joint Utilities developed an NDA that they propose? If so, please provide a copy.
- b. Under what circumstances would "additional NDAs from departments such as purchasing or IT" be required? Please explain in detail what the Joint Utilities meant by that sentence.
- c. Please provide copies of NDAs currently used by the Joint Utilities' respective departments such as purchasing or IT.

Response:

- a. No, NDAs have not been developed for use with the data platform. The contents of such an NDA will depend on roles and responsibilities of the various entities involved with the platform, to be determined by the Commission.
- b. This discussion refers to the internal procedural logistics. The Utilities expect the NDA process to be delineated with the rollout of the platform.
- c. Please see attached: MISSION 1-010c Attachment A, MISSION 1-010c Attachment B, and MISSION 1-010c Attachment C for the requested documents.

**Public Service of New Hampshire d/b/a Eversource Energy
Unitil Energy Systems, Inc. and Northern Utilities, Inc. (together
Unitil)**

Docket No. DE 19-197

Date Request Received: 08/31/2020

Request No. MISSION 1-012

Request from: Mission:Data Coalition

Date of Response: 09/15/2020

Page 1 of 1

Witness: Kimberly Hood, Dennis E. Moore

Request:

See 45:5-6: "Platform users that utilize and store customer data should be subject to external assessment and audit for security management controls." Exactly what kind of "external assessment" or "audit" are the Joint Utilities proposing? Please be specific, including whether the Joint Utilities or another entity would conduct such assessment/audit.

Response:

The most common audit type is an SOC 3 audit. This can be done either by an independent audit firm or by the Utilities.

Liberty Utilities (EnergyNorth Natural Gas) Corp. and
Liberty Utilities (Granite State Electric) Corp. both d/b/a Liberty Utilities

DE 19-197

Development of a Statewide, Multi-Use Online Energy Data Platform

Mission:data Coalition Data Requests - Set 1

Date Request Received: 8/31/20
Request No. MDC 1-4Date of Response: 9/15/20
Respondent: Heather Tebbetts**REQUEST:**

See 27:7-11: "The third party will be required to...satisfy utility review of compliance with privacy standards relative to RSA 363:38, and requirements as established in RSA 378:51, II. This will include a vendor cyber security review by utilities using a common questionnaire."

- a. Has Liberty developed a document detailing "utility review of compliance with privacy standards"? If so, please provide a copy.
- b. Has Liberty developed a document detailing "cyber security review...using a common questionnaire?" If so, please provide a copy.
- c. Is Liberty proposing a cyber security review that can be objectively evaluated on a pass/fail basis?
- d. Is Liberty proposing a cyber security review in which Liberty uses its discretion in determining a third party's eligibility?

RESPONSE:

- a. The Company has a confidential enterprise-wide cybersecurity plan that includes policies and standards critical for compliance and consistent implementation of procedures. The minimum list of policies, standards, and frameworks align to NIST SP800-53rev3 policy controls and ISO 27001.
- b. The Company does not have a "common questionnaire" for cybersecurity as each review for security, such as the review for the Tesla Powerwall batteries, has its own set of security issues that need to be identified and reviewed.
- c. The Company does not have a formal cybersecurity proposal at this time.
- d. The third party's eligibility will be predicated on compliance with Liberty's cybersecurity plan and any other requirements that come about from this docket.

**Public Service of New Hampshire d/b/a Eversource Energy
Unitil Energy Systems, Inc. and Northern Utilities, Inc. (together
Unitil)**

Docket No. DE 19-197

Date Request Received: 08/31/2020

Request No. MISSION 1-005

Request from: Mission:Data Coalition

Date of Response: 09/15/2020

Page 1 of 1

Witness: Kimberly Hood, Justin Eisfeller, Dennis E. Moore

Request:

See 38:23-25: "Utilities would ensure that access to data is secured in a manner compliant with company policies, cyber security guidelines, Commission requirements, and all legal and regulatory mandates." Please provide copies of all company policies and cyber security guidelines referenced by the Joint Utilities.

Response:

Eversource and Unitil IT Security policies are confidential documents. Information regarding the Eversource and Unitil Cyber Security programs have been discussed with the PUC as part of NHPUC Rule 306.10.

The Utilities would also note that requests for data continue to increase in scope and volume, for both individual customer and aggregated information. This situation has continued to evolve over the past year and is anticipated to continue in the future. The Utilities continue to develop internal processes to receive, route, verify, respond, and send data in a matter that is secure, accurate, and timely and believe that the data platform may help to provide desired information to customers and third parties in an automated fashion upon implementation.

Public Service of New Hampshire d/b/a Eversource Energy
Docket No. DE 19-197**Date Request Received: 09/22/2020****Date of Response: 10/02/2020****Request No. LGC 2-004****Page 1 of 2****Request from: Local Government Coalition****Witness: Christine Riley Hastings, Christina S. Jamharian, Justin Eisfeller, Jeremy Haynes**

Request:

With regard to the responses to LGC 1-005:

- (a) Why does neither utility provide interval data via EDI? In light of the fact that other utilities have provided interval data via EDI for a number of years (e.g. in New Jersey, California, etc.), why do neither Eversource or Unitil do so? What would be the process of updating the EDI systems to do so? Has either utility evaluated this option, and if so, when was the evaluation conducted and why has it not been implemented? Please provide any supporting internal documentation to accompany this response.
- (b) Why is only 12 months of historic usage history available?
- (c) Where is customer usage history stored by the utility after 12 months? Is it stored in a database accessible within the utility through an internal server or is it placed onto a storage medium that must be reloaded onto a computer or server to access?
- (d) For how long does the utility store individual customer usage history in some form and for monthly data and hourly (or more frequent) interval meter data specifically?
- (e) Do the utilities have any written policies on how long customer usage data is retained?
- (f) Do the utilities believe there are any regulatory standards that pertain to how long they retain customer usage data, and if so, please cite?

Response:

- a. For Eversource, when the supplier data transfer process was designed for deregulation, a requirement was defined to standardize on the EDI-814 file format, one of many file formats available. Having a standard simplified the relationship between the utilities and the suppliers – all parties know to use the one file format instead of negotiating and defining a file format for each relationship. Interval data is not part of the EDI-814 standard, so another file format would need to be selected (EDI or some other standard) and then the utilities and suppliers would need to update their systems and processes to use it.

Currently, Unitil provides interval data via e-mail, consistent with the approach stipulated in the Terms and Conditions for Competitive Suppliers, Appendix B, Section II, which states that ‘Interval data is made available to Customers or their authorized agents through e-mail or through basic web access.’

In order to estimate the cost to update Unitil’s systems to allow for the processing of interval data transactions, specific EDI Standards related to interval data transactions would first need to be developed and agreed upon by NH stakeholders, including but not limited to which data elements would be provided, file formats, and protocols for data transfer.

Public Service of New Hampshire d/b/a Eversource Energy
Docket No. DE 19-197

Date Request Received: 09/22/2020

Request No. MISSION 2-005

Request from: Mission:Data Coalition

Date of Response: 10/02/2020

Page 1 of 2

Witness: Christine Riley Hastings, Christina S. Jamharian, Kimberly Hood, Justin Eisfeller

Request:

See the Joint Utilities' response to M:d1-15.

- a. 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."
- b. For Unitil, Attachments A, E and Attachment F appear to be the only requirements of retail suppliers that pertains to cybersecurity. Does Unitil require anything else pertaining to cybersecurity of retail suppliers using EDI?
- c. Was Unitil's "Competitive Energy Supplier Trading Partner Agreement" approved by the New Hampshire Public Utilities Commission? If so, please provide the proceeding number, order date and order number.
- d. Was Eversource's "Electric Supplier Services Master Agreement" approved by the New Hampshire Public Utilities Commission? If so, please provide the proceeding number, order date and order number.
- e. Please confirm that Eversource does not have any cybersecurity requirements that apply to retail suppliers using EDI.
- f. If Eversource does have cybersecurity requirements applicable to retail suppliers using EDI from (c) above, please update your response to M:d1-15 accordingly and provide copies of such cybersecurity requirements.

Response:

- a. At this time, retail suppliers are not required to abide by the Unitil Vendor Security Requirements. The continually changing landscape in regards to cyber threats and privacy legislation necessitates that the Utilities continually reassess and adjust our policies and practices regarding the sharing of sensitive and private customer data. Unitil initiated this process for its EDI vendor in 2019 and the Company will be expanding this requirement to include retail suppliers, as it is best practice and provides the best opportunity to protect our customer's data.
- b. No, Unitil does not currently have any other requirements related to cyber security of retail suppliers using EDI.
- c. Yes, the Competitive Energy Supplier Trading Partner Agreement was approved in proceeding number DE 05-178, effective 10/6/2006, in Order No. 24677.
- d. The agreement is not approved, or required to be approved, by the Commission.

**Public Service of New Hampshire d/b/a Eversource Energy
Unitil Energy Systems, Inc. and Northern Utilities, Inc. (together
Unitil)**

Docket No. DE 19-197

Date Request Received: 08/31/2020

Request No. MISSION 1-004

Request from: Mission:Data Coalition

Date of Response: 09/15/2020

Page 1 of 1

Witness: Kimberly Hood, Dennis E. Moore

Request:

Concerning the Joint Utilities's respective customer web portals:

- a. Does either utility require two-factor authentication or multi-factor authentication today?
- b. Can a residential customer start, stop or move their electric or gas service using only the web portal today?

Response:

- a. The Utilities do not currently require two-factor or multi-factor authentication (MFA). However, MFA has become standard for online transactions and is planned for new systems we intend to implement and added to existing systems in the future. Such controls are not static and the Utilities continue to add security to company systems, including MFA.
- b. Eversource customers must authenticate in order to start, stop or transfer service on our web site. Once logged in, customers can initiate their request electronically.
Unitil customers have the ability to start, stop and move their electric and/or gas service using only the web portal today.

Liberty Utilities (EnergyNorth Natural Gas) Corp. and
Liberty Utilities (Granite State Electric) Corp. both d/b/a Liberty Utilities

DE 19-197

Development of a Statewide, Multi-Use Online Energy Data Platform

Mission:data Coalition Data Requests - Set 1

Date Request Received: 8/31/20
Request No. MDC 1-3

Date of Response: 9/15/20
Respondent: Christine Downing

REQUEST:

Concerning Liberty's customer web portals:

- a. Does Liberty require two-factor authentication or multi-factor authentication today as a prerequisite to a customer logging in to Liberty's web portal?
- b. Can a residential customer start, stop or move their electric service using only the web portal today?

RESPONSE:

- a. Liberty does not currently require two-factor or multi-factor authentication.
- b. No, this is not an option at this time.