BEFORE THE
NEW YORK PUBLIC SERVICE COMMISSION

Proceeding on Motion of the Commission Regarding Strategic Use of Energy Related Data	)	**Case 20-M-0082**
Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place	)	**Case 18-M-0376**

COMMENTS OF NRG ENERGY, INC. IN RESPONSE TO THE JOINT UTILITIES' PETITION TO MODIFY THE DATA SECURITY AGREEMENT SELF-ATTESTATION REQUIREMENTS AND IMPLEMENT A GOVERNANCE REVIEW PROCESS FOR REGULAR SELF-ATTESTATION UPDATES

I. INTRODUCTION AND SUMMARY OF POSITION

On May 3, 2022, the Joint Utilities[1] in the above proceedings filed a Petition to Modify the Data Security Agreement Self Attestation Requirements and Implement a Governance Review Process for Regular Self-Attestation Updates ("JU Petition"). NRG requests that the Commission deny the JU Petition as filed for the reasons set forth below.

Who We Are

Headquartered in Houston, Texas, NRG is a leading integrated energy and home services company in the U.S. A Fortune 500 company, NRG is at the forefront of changing how people use, buy, and think about energy. We strive to empower our residential, commercial, and industrial

[1] The Joint Utilities are comprised of Central Hudson Gas and Electric Corporation (Central Hudson), Consolidated Edison Company of New York, Inc., National Fuel Gas Distribution Corporation, New York State Electric & Gas Corporation, Niagara Mohawk Power Corporation d/b/a National Grid, KeySpan Gas East Corporation d/b/a National Grid and The Brooklyn Union Gas Company d/b/a National Grid NY, Orange and Rockland Utilities, Inc., and Rochester Gas and Electric Corporation.

customers with reliable and cost-effective energy solutions. We draw on our deep industry experience to provide products and services that suit our customer's needs with the consistency and innovation expected from the nation's leading integrated energy and home services provider. NRG has numerous licensed Energy Service Companies ("ESCOs") that are actively serving electricity and natural gas customers throughout New York.[2] NRG also serves customers in twenty-four (24) other states across the U.S. Together, NRG is creating a sustainable energy future by fostering smarter energy choices and providing reliable, cleaner power. NRG's retail brands maintained one of the largest combined competitive retail energy portfolios in the U.S. with 157 TWhs of electricity and 1,877 MMDth of natural gas sold in 2021 and approximately six (6) million customers served. Our roughly 7,300 employees provide a range of products and services including demand response and energy efficiency, 100% renewable energy, energy plans bundled with energy efficiency technology, such as Nest thermostats, as well as loyalty rewards and charitable giving products through "Choose to Give" plans.

Summary of Position

NRG urges the Commission to not approve the JU Petition as proposed. The JU Petition does not evaluate cyber security concerns using a risk based approach, distinguishing between the risk to utility IT systems and the risk of improper access to customer data,[3] along with consideration of classifying the sensitivity of such data and aligning appropriate levels of

---

[2] The NRG Energy Inc. retail companies operating in New York include Direct Energy Business, LLC ("DEB"), Direct Energy Business Marketing, LLC, Direct Energy Services, LLC, and Gateway Energy Services Company in addition to Green Mountain Energy Company, Reliant Energy Northeast LLC d/b/a NRG Home and d/b/a NRG Business Solutions, Energy Plus Holdings LLC, Energy Plus Natural Gas LLC, Independence Energy Group LLC d/b/a Cirro Energy, XOOM Energy New York, LLC, and Stream Energy New York, LLC.

[3] Cases 18-M-0376 et al., Proceeding on the Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place, *Order Establishing Minimum Cyber Security and Privacy Protections and Making Other Findings* (Cyber Security Proceeding), Order Establishing Minimum Cyber Security and Privacy Protections and Making Other Findings (issued October 17, 2019) (DSA Order), p. 35.

protection.[4] Instead, the JU Petition opts to overly burden energy service entities ("ESEs")[5] and customers by requiring cyber security and encryption methods normally reserved for highly sensitive data at the highest levels of government. Further, NRG believes that ESEs need more input on cyber security changes, and as such, should be a member of the proposed Governance Committee to ensure all stakeholders are represented in future cyber security discussions. Finally, NRG also believes that if the Commission approves some or all of the JU Petition, there should be a phased-in compliance period so that ESEs like NRG would be provided adequate time to undertake the necessary reviews of their systems to determine compliance and, as necessary, implement any new requirements.

II. COMMENTS

There are three (3) overarching reasons why the Commission should not adopt the JU Petition as currently proposed: (1) the JU do not employ a balanced risk based approach to data security by considering the level of risk in contrast to the proposed requirements in their proposal instead opting for over burdensome cyber security requirements that in some cases are practically impossible to employ; (2) the JU's proposed Governance Committee does not provide ESEs like NRG, and their information technology experts, with a voice in future cyber security matters and potential changes to the Self-Attestation ("SA"); and (3) the JU Petition fails to provide ESEs a buffer period to assess their internal systems against any new requirements, identify any potential compliance issues and, as necessary, implement corrective actions.[6]

---

[4] *See* DSA Order, p. 45 (noting that "The Joint Utilities are charged with maintaining customer data and based upon the sensitivity of the specific data points, keeping it confidential.").

[5] Energy service entities (ESEs) refer to energy service companies (ESCOs), distributed energy resources (DERs) suppliers, direct customers, governmental agencies, and other entities as defined in the Data Security Agreement (DSA).

[6] It is also worth noting that the Petition uses terminology of "Confidential Customer and Non-Public Utility Information," neither of which is defined or recognized in the DSA or the DSA Order.

a) THE JU PETITION DOES NOT EMPLOY A RISK-BASED APPROACH TO CYBER SECURITY

As the JU state in their Petition, the ever changing cyber and data security landscape requires utilities "to examine their security posture and asses potential cyber resilience risks."[7] In turn, ESEs like NRG also need to assess their security posture and cyber resilience. Such assessments, however, must include risk-based assessments, which the JU Petition lacks. Indeed, the JU unilaterally call for rigid security standards that are amorphous, impractical, and detached from the real-world data security landscape and attempt to force "burdensome cyber hygiene requirements" on ESEs.[8]

Importantly, the Commission has already recognized the need to "strike[] the appropriate balance between protecting utility IT systems and customer information and facilitating the transfer of customer consented data."[9] In doing so, the Commission noted that:

> a balance must be struck between protecting utility IT systems and the privacy of customer data in a way that distributes the risks and responsibility amongst those entities electronically exchanging and/or receiving customer data with the utilities, and facilitating the dissemination of customer information to ESEs for which the customer consented to obtain their data. Ultimately, a market where all parties observe at least a minimum level of cybersecurity and privacy protections will reduce the risks associated with electronic communications of customer data between distribution utilities and ESEs, instilling customer confidence and promoting market development.[10]

The impractical and misguided nature of the JU Petition is evident in their six (6) proposed updates and three (3) new requirements to Appendix A. These comments specifically address the JU's new proposed requirements, Items 3, 7 and 8.

---

7 JU Petition at 2.

8 DSA Order, p. 13.

9 DSA Order, p. 23.

10 DSA Order, p. 13.

First, the JU Petition generally calls for implementation of cybersecurity standards issued by the United States Department of Commerce National Institute of Standards and Technology ("NIST"). This is evident in Items 3, 7 and 8. The JU's claim NIST standards are "industry-accepted" frameworks that "are considered current minimum protections and best practices."[11] However, NIST standards are not "current minimum protections"[12] nor are they the only security measures that are reasonable and appropriate. While some data may deserve this level of protection, not all data should be treated the same and the JU has not made any showing to the contrary. This is why it is important to focus on the type of data sought to be protected.

In addition, as the JU Petition acknowledges, the Commission understood that data privacy and security protections should be suitable for the scope of the business: "….the flexibility afforded by the DSA will allow ESEs to observe cyber security standards that are ***most appropriate for their businesses***….." [emphasis added].[13] The NIST standards are not appropriate for use in communicating retail customer data used in accordance with customer consent. This was true in 2019 as determined by the Commission:

> While the UBP-DERS requires DERS who obtain customer information from the distribution utility using EDI to have processes and procedures in place regarding cybersecurity consistent with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Commission declines to adopt this requirement for all ESEs. Instead, the flexibility afforded by the DSA will allow

---

11 JU Petition at 6.

12 *See e.g,*. New York's SHIELD Act data security protections which requires persons or businesses that own or license computerized data that includes New York residents' private information to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information." New York General Business Law § 899-bb. Data security protections (2020); The Health Insurance Portability and Accountability Act (HIPAA) also does not require fully implemented NIST standards. Department of Health and Human Services, Health Insurance Reform: Security Standards; Final Rule (HIPAA Security Rule), 45 C.F.R. Parts 160, 162 and 164 (2003); *see also* Department of Health and Human Services, HIPAA Security Series, *Security Standards: Technical Safeguards,* Vol. 2, Paper 4 (2007)("The Rule allows a covered entity *to use any security measures that allows it reasonable and appropriately to implement the standards and implementation specifications*. A covered entity must determine which security measures and specific technologies are reasonable and appropriate for implementation in its organization.") (emphasis added).

13 DSA Order, p. 49.

> ESEs to observe the cybersecurity standards that are most appropriate for their businesses.[14]

The JU Petition does not offer any justification or need to reverse course now. Every day large amounts of data are transferred between ESEs like NRG and customers. This includes confidential customer information such as a customer's account number, mailing address and energy usage. This type of data is important to safeguard which is why NRG vigilantly protects customer data. However, transmission by email of this category of data between NRG's customers, the utilities, the Commission, or other permissible third parties poses no risk to utility IT systems at large.

The JU Petition does not recognize differences in sensitivity of different types of data and instead is requesting encryption for all categories of customer data across the board. The JU Petition does not strike the appropriate balance as referred to in the Commission's 2019 Order. For example, if a customer emails NRG asking about their account information, high level encryption is not necessary to adequately protect the customer or the larger grid.[15] However, this is exactly what the JU has proposed in Item #7 which would now require "[encryption of] all Confidential Customer and Non-Public Information in transit using encryption methods compliance with NIST cryptographic standards and guidelines." Encryption of this nature, and the burden to implement and support NRG's customers with different email and computer systems, would require large amounts of money and time to implement and in some cases may not even be possible. As acknowledged by the Commission use of encryption for email would impede normal business practices:

---

[14] DSA Order, p. 49.

[15] The JU are also seeking to impose standards that they themselves do not comply with. For example, many utility customers in New York receive their billing information via physical mail, which can easily be intercepted. While the United States Postal Service does employ security standards, a bill placed in a private mailbox is not as secure as encrypted data.

> With respect to the requirement that Confidential Customer Utility Information be encrypted in transit, further refinement of this requirement is necessary so as to not impede normal business practices. Communicating via encrypted emails require the sender and recipient to have a pre-existing relationship with software to encrypt and decrypt the content of emails. Additionally, many ESEs utilize email to communicate with their customers, a vast majority of which will not have the ability to encrypt emails or receive encrypted emails from their chosen ESE. The Joint Utilities exclude email from the electronic communications with ESEs that trigger the need for a DSA. That same exception should be applied to the encryption in transit requirement. Thus, encryption of Confidential Customer Utility Information will not be required for email communications. This modification will allow ESEs to effectively communicate with customers and other entities without first establishing a process for mutual encryption and decryption.[16]

At the very least, it would be unduly burdensome and likely unworkable. An average customer using a Gmail account should not be required to employ NIST level encryption standards when communicating with NRG. The same is true for email communications with Commission staff. As noted in the above excerpt, this is precisely the reason this requirement (proposed SA Item #. 7) was rejected at the time the DSA was approved.

This is not to say that the data should not be protected. NRG recognizes the reality of dealing with average consumers as that is what the company does on a daily basis. Because of our wide-ranging clientele, NRG currently employs data security protections based on the sensitivity of the data at issue. This is the result of the company evaluating security processes and data through a risk-based lens. The JU have not performed this type of risk-based analysis and instead repeatedly cite to general security and encryption standards which do not take into account the sensitivity of the data at issue. Any re-evaluation of standards for email transmissions should be considered with the input of all stakeholders and not unilaterally imposed by the JU. Indeed, the JU Petition acknowledges the need for collective input:

> [t]o provide adequate cybersecurity for ESEs and appropriate protection for customer and system data, the SA requirements, first established in 2019 in the *Minimum Protections Order*, must keep pace with best practices, technology, and

[16] DSA Order, p. 52.

> industry requirements. This required regular updates of the SA controls through a structured process with participation from the Joint Utilities, Department of Public Service Staff (Staff) *and stakeholders*.[17]

The JU have provided no current examples of harm or pending threats to the privacy of customer data during email communications as permitted under the existing Commission-approved DSA and SA which would justify immediate imposition of new requirements in advance of the collaborative process anticipated in the Data Ready Certification Process.

Not only is this generic approach evident in the JU's proposed changes to data and communication encryption, but their proposals also lack minimum levels of specificity. The JU Petition proposes to change Item #7, Encryption in Transit, and Item #8, Encryption at Rest, so that all confidential customer and non-public utility information uses[18] "encryption methods compliant with NIST cryptographic standards and guidelines."[19] However, there is not one "NIST cryptographic standard" or one "NIST guideline" on encryption. Rather, NIST provides a number of cryptographic standards depending on circumstance. For example, under the large umbrella of NIST cryptographic standards and guidelines there are approved algorithms for block cipher techniques and guidelines for post-quantum cryptography for machines that exploit quantum mechanical phenomena.[20] However, the JU Petition does not provide ESEs with the needed level of specificity to know which standards and guidelines would or would not apply.

This issue is also present in the proposed changes to Item #3. The JU Petition calls for "[a]uthentication and password controls align with NIST Special Publications 800-63B: Digital

---

17 JU Petition at 2 (emphasis added).

18 *See* FN. 6 (noting that neither term is defined).

19 JU Petition at 8.

20 *See* The National Institute of Standards and Technology (NIST), *Cryptographic Standards and Guidelines*, available at https://csrc.nist.gov/Projects/cryptographic-standards-and-guidelines (linking to twelve (12) different standards and guidelines on a wide variety of cryptography topics).

Identity Guidelines."[21] However, Section 800-63B is only one part of the expansive four-volume "SP 800-63 Digital Identity Guidelines." The JU's complete disregard for this suggests that they failed to thoroughly analyze the actual standards they are proposing, let alone undertake the necessary risk-based analysis as to whether they are even necessary or appropriate to protect customer information. Further, as proposed, there is no way for an ESE to know what standards would and would not apply.

Overall, the JU Petition refers to the need for additional requirements because of sensational headlines and events which could have (but did not) impact any utility's IT systems and infrastructure. Here, however, many of the new requirements are not even directed at this risk and are focused primarily on protecting Confidential Customer Information and mere email communications between ESEs and permissible third parties such as their customers—with no direct connection to a utility during those communications.[22] The JU's proposed changes to the SA are therefore unnecessary. At a minimum, due to the lack of specificity in their proposed changes, the nature of the proposed changes, and the fact that the Commission has already commented on many of the issues the JU are trying to implement (such as the use of encryption for email), these changes should be directed to a more collaborative data-security process for consideration.

---

[21] JU Petition at 8.

[22] DSA Order, p. 35-36 ("Risk to the utility IT systems resulting from electronic communication with those systems are addressed by the cybersecurity protections primarily contained in the SA. Risk of data misuse or the improper access to confidential customer data is primarily addressed by the confidentiality terms and conditions of the DSA.").

b) THE JU PETITION DOES NOT PROVIDE ESEs LIKE NRG A SEAT ON THE GOVERNANCE COMMITTEE

The JU Petition also calls for the Commission to establish a Governance Committee to "provide a forum for regular reviews and updates of the SA."[23] NRG generally agrees with the JU that this would benefit all parties and allow for a collaborative process to identify new cyber risks to the industry. However, limiting Committee membership to only JU cyber security experts and Staff relegates ESEs to the background and would further perpetuate the already present disconnect between ESEs and the JU. ESEs like NRG need a seat at the table. Only with Staff, JU and ESE cyber security experts on the Governance Committee can robust discussions surrounding risk-based cyber security measures occur. The proposed Advisory Working group membership for ESEs does not ensure this communication will occur because, as proposed, the Governance Committee has no obligation to listen to Advisory Working Group recommendations. Instead, the Governance Committee submits its recommendations directly to the Commission. As such, ESEs need their own cyber security experts on the Governance Committee to ensure ESE concerns are heard.

c) THE JU PETITION DOES NOT PROVIDE ESEs ADEQUATE TIME TO IMPLEMENT THE PROPOSED CHANGES IN THE SA

Finally, the timing of the JU Petition, and request for parties to immediately sign an updated SA, is troublesome to NRG. If approved, ESEs would need time to review their existing systems to determine if any updates are required based on the new SA. This is a time intensive undertaking for a large company like NRG which employs complex data security systems across numerous platforms. As such, ESEs must be given time to come into compliance and not be obligated to sign a document they could immediately breach. NRG urges the Commission, if it chooses to adopt

[23] *Id.* at 10.

some or all of an updated SA, to provide ESEs sufficient time to assess their security systems and operational processes to develop or add systems and processes required to comply with any new requirements the Commission approves.

III. SUMMARY

For all of the foregoing reasons, NRG respectfully requests that the Commission deny the JU Petition as currently proposed and, instead, establish a Governance Committee as described herein to collaborate and propose appropriate risk-based cyber security measures.

Dated: July 25, 2022

Respectfully submitted,

Yvonne Hennessey
Barclay Damon LLP
80 State Street
Albany, New York 12207
Phone: (518) 429-4293
Email: yhennesey@barclaydamon.com
Counsel for NRG Energy, Inc.