ECKERT SEAMANS
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
213 Market Street
8th Floor
Harrisburg, PA 17101

TEL: 717 237 6000
FAX: 717 237 6019

Deanne M. O'Dell, Esq.
717.255.3744
dodell@eckertseamans.com

February 8, 2023

Via Electronic Filing
Rosemary Chiavetta, Secretary
PA Public Utility Commission
P.O. Box 3265
Harrisburg, PA 17105-3265

Re: Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting – Docket No. L-2022-3034353

Dear Secretary Chiavetta:

Enclosed for electronic filing please find Comments of NRG Energy, Inc. with regard to the above-referenced matter.

Sincerely,

Deanne M. O'Dell

DMO/lww
Enclosure

Colin Scott, Assistant Counsel, colinscott@pa.gov
Chris Van de Verg, Assistant Counsel, cvandeverg@pa.gov
Daniel Searfoorce, Manager – Water, Reliability and Emergency Preparedness Division
dsearfoorc@pa.gov
Michael Holko, Director, Office of Cybersecurity Compliance and Oversight, miholko@pa.gov
Karen Thorne, Regulatory Review Assistant, kathorne@pa.gov

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

Rulemaking to Review Cyber Security Self-Certification Requirements and the Criteria for Cyber Attack Reporting	:	Docket No. L-2022-3034353
	:	

COMMENTS OF NRG ENERGY, INC.

Deanne M. O'Dell, Esquire
Eckert Seamans Cherin & Mellot, LLC
213 Market Street, 8th Fl.
Harrisburg, PA 17108-1248
717 237 6000
dodell@eckertseamans.com

Date: February 8, 2023

TABLE OF CONTENTS

I. INTRODUCTION

By Advanced Notice of Proposed Rulemaking Order ("ANOPR") entered on November 10, 2022, the Commission invited comments to assist in its consideration of whether and how its existing regulations regarding cyber attack reporting and self-certification filings[1] ("Regulations") should be revised to ensure that they address public utility fitness in the current and anticipated future cybersecurity threat landscape.[2]

In the ANOPR, the Commission also describes entities which are subject to the Regulations as those outlined in 52 Pa Code § 101.2 defined as a "jurisdictional utility." The Commission noted that certain categories of entities under its supervision do not fall within the definition of a jurisdictional utility, including licensed entities such as electric generation suppliers ("EGS") and natural gas suppliers ("NGS"), and in Appendix A, the Commission asks whether the self-certification regulations should be applied to such entities as EGSs and NGSs.

NRG Energy, Inc. ("NRG") is one of the largest competitive retailers of electricity and natural gas supply in the United States by customer count and by volume. Subsidiaries of NRG are licensed as EGSs[3] by the Commission pursuant to the Electricity Generation Customer

---

1 52 Pa Code §§ 57.11 (relating to accidents for electricity public utilities); 59.11 (relating to accidents for gas public utilities); 61.11 (relating to accidents for steam utilities): 65.2 (relating to accidents for water public utilities); 101/1-101.7 (relating to public utility preparedness through self certification for jurisdictional utilities); and, 61.45 (relating to security planning and emergency contact list for steam utilities).

2 ANOPR at 1-2.

3 As EGSs in Pennsylvania, NRG subsidiaries hold licenses as follows: Direct Energy Business, LLC – Docket No. A-11025; Direct Energy Business Marketing, LLC – Docket No. A-2013-2368464; Direct Energy Services, LLC – Docket No. A-110164; Energy Plus Holdings LLC – Docket No. A-2009-2139745; Gateway Energy Services Corporation – Docket No. A-200902137275; Independence Energy Group LLC d/b/a Cirro Energy – Docket No. A-2011-2262337; Reliant Energy Northeast LLC d/b/a NRG Home/NRG Business/NRG Retail Solutions – Docket No. A-2010-2192350; Green Mountain Energy Company – Docket No. A-2009-2139745; Stream Energy Pennsylvania, LLC – Docket No. A-2010-2181867; XOOM Energy Pennsylvania, LLC – Docket No. A-2012-2283821, Bounce Energy, Inc. – Docket No. A-2020-3020380.

Choice and Competition Act.[4] Subsidiaries of NRG are also licensed NGS[5] by the Commission pursuant to the Natural Gas Choice and Competition Act.[6] Through these licensed subsidiaries, NRG sells competitive electric generation and natural gas supply to retail consumers in the Commonwealth. As licensed NGSs and EGSs, these subsidiaries of NRG are expressly excluded from the definition of "public utility" in the Public Utility Code[7] "except for limited purposes"[8] and, therefore, the Commission's Regulations under consideration here do not impose cyberattack reporting or self-certification filings on the NGSs or EGSs.

As explained more fully below, NRG understands and supports the need for data security to protect the utility infrastructure and network and to safeguard the confidentiality of customer information. However, NRG does not support imposing new Commission designed cyber security obligations on NGSs and EGSs for two overarching reasons. First, an NGS or EGS which accesses and/or is in possession of personal information related to an electricity or gas customer is already subject to an existing subset of laws and regulations relating to data privacy, confidentiality, and cybersecurity, and additional regulations will not enhance or expand any cybersecurity benefit.

Second, as a commercial entity, an NGS or EGS must address cybersecurity and

---

4 66 Pa.C.S. §§ 2801 et seq. ("Natural Gas Competition Act")

5 Independence Energy Group LLC d/b/a Cirro Energy PUC Docket No. A-2013-23964409; Reliant Energy Northeast, LLC (PUC Docket No. A-2015-2478293; PUC Utility Code No. 1217605); Green Mountain Energy Company (PUC Docket No. A-2017-2583732; PUC Utility Code No. 1219483); Xoom Energy Pennsylvania, LLC (PUC Docket No. A-2012-2283967; PUC Utility Code No. 1214189); Gateway Energy Services Corporation (PUC Docket No. A-2009-2138725); Bounce Energy, Inc. (A-2020-3023412); Direct Energy Business, LLC (PUC Docket No. A-125072) and Direct Energy Business Marketing, LLC (PUC Docket No. -2013-2365792; PUC Utility Code No. 1215776).

6 66 Pa. C.S. §§ 2201 et seq. ("Electric Competition Act")

7 66 Pa. C.S. §102 (definition of "public utility").

8 *See HIKO Energy, LLC v. Pa. Pub. Util. Comm'n*, 163 A.3d 1079, 1082 n.1 (Pa. Cmwlth. 2017) (en banc), aff'd, 209A.3d 246 (Pa. 2019); *Indep. Oil & Gas Ass'n v. Pa. PUC*, 804 A.2d 693, 697 (Pa. Cmwlth. 2002)

protection of personal information in order to successfully operate in the commercial marketplace, as well as to protect its own information assets. As such, an NGS or EGS has strong incentives to self-regulate and ensure it employs industry standard cybersecurity practices.

NRG appreciates the opportunity to submit these comments on this important topic and looks forward to continuing to provide feedback as may be useful for the Commission in this proceeding.

II. COMMENTS

In Appendix A, the Commission identifies nine "Topics for Comment" with questions for each topic and invites interested stakeholders to provide their response. Given that NRG as an EGS and NGS is not currently subject to the Commission's Regulations, NRG will focus these comments on Question Number 6 regarding whether self-certification regulations should be extended to NGSs and EGSs. For the reasons discussed below, NRG submits that imposing cybersecurity reporting or other obligations on its competitive supplier entities is unnecessary as it would "replicate regulations that were already in place and required by the Federal government or other agencies…."[9] As a result, imposing additional regulations offers no significant benefit regarding the Commission's goal of ensuring the security of the energy infrastructure and/or customer information, but may instead serve to divert critical resources, funds and time from the primary focus of enhancing and perhaps redesigning the cybersecurity practices and architecture of the infrastructure of jurisdictional utilities' networks and systems providing and delivering electricity and natural gas. In addition, doing so could also negatively impact the competitive suppliers by imposing additional time-consuming and potentially new obligations on their

---

[9] ANOPR at 2.

operations that could divert resources better used by being able to keep abreast of developments in cybersecurity as well as to offer competitive products and service to retail end users.

A. Additional Cybersecurity Obligations For NRG Are Unnecessary Given The Existing Landscape Of Federal And State Data Privacy And Cybersecurity Regulations

NRG understands that regulations relating to cybersecurity are beneficial in setting standards for compliance, but, as the Commission noted, its existing cybersecurity regulations are part of a network of cybersecurity and privacy laws and regulation which "have proliferated over the last decade or more since the PUC's regulations were first promulgated."[10] Of course, any future Commission regulations will also become part of that growing and complex network.

As will be discussed further below, NRG is already regulated in its data security practices as a result of a myriad of Federal and State laws, including for example, Pennsylvania's data breach statute[11] and, as licensed EGSs and NGSs, NRG is required to comply with the Commission's regulations at 52 Pa. Code §§ 54.8 (EGS) and 62.78 (NGSs).

1. <u>As Numerous Existing Privacy And Data Security Law Already Exist, Adding New Requirements On NGSs and EGSs Will Impose Another Layer of Regulatory Obligations</u>

As the Commission notes in the ANOPR, "the steady rise in the creativity, number and severity of cyber attacks" has led to "industry and government…continuously" reviewing, expanding, and improving cybersecurity standards for entities of all kinds.[12] The ANOPR details some of the broader guidance already developed. As recognized by the Commission, its proposed cybersecurity regulations will not operate in a vacuum and, if applied to licensed NGSs

---

10 ANOPR at 19.

11 73 P.S. §§ 2301 to 2308 and 2329 to 2330.

12 AnOPR at 11.

and EGSs, will impose another new layer of regulatory obligations. Importantly, NRG is not a one-dimensional company only operating as licensed NGSs and EGSs in Pennsylvania. It has a multitude of business arrangements and other obligations which must be addressed in order to operate the overall business. As such, NRG receives confidential data from a number of sources apart from its operations as an NGS and EGS. For example, NRG employees are required to provide confidential and sensitive information as part of their employment and, because NRG offers an employee sponsored health plan, it must comply with data privacy laws such as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as a covered entity. HIPAA places responsibilities on covered entities and their business associates to secure protected health information in electronic form. Organizations are expected to take the necessary steps to ensure privacy, protect against threats, ensure employee compliance, and protect against prohibited electronic uses or disclosures. Compliance with HIPAA requires companies to implement physical, technical, and administrative safeguards to protect individuals' health information.

In addition, NRG is required to comply with the Sarbanes-Oxley Act of 2002 ("SOX") which is intended to protect consumers and investors from fraudulent corporate accounting activities by establishing more transparent reporting and independent accounting requirements for corporations and their leaders.[13] SOX requires external auditors to audit and report on the internal control reports of management, in addition to the company's financial statement. A review of a company's internal controls is often the largest component of a SOX compliance audit. Internal controls include all IT assets, including any computers, network hardware, and

---

[13] *See* 29 U.S.C. §§ 1001 et. seq.

other electronic equipment that financial data passes through. A SOX IT audit will look at the following internal control items:

- IT security: Ensure that proper controls are in place to prevent data breaches and have tools ready to remediate incidents should they occur. Invest in services and equipment that will monitor and protect your financial database.

- Access controls: This refers to both the physical and electronic controls that prevent unauthorized users from viewing sensitive financial information. This includes keeping servers and data centers in secure locations, implementing effective password controls, and other measures.

- Data backup: Maintain backup systems to protect sensitive data. Data centers containing backed-up data, including those stored off-site or by a third-party are also subject to the same SOX compliance requirements as those hosted on-site.

- Change management: This involves the IT department process for adding new users and computers, updating and installing new software, and making any changes to databases or other data infrastructure components. Keep records of what was changed, in addition to when it was changed and who changed it.[14]

As noted above, NRG has an integrated digital footprint across many states for many different lines of business and is obligated to comply with a vast array of laws. NRG does not implement state-specific infrastructure, systems and networks. Instead, NRG's systems achieve economies of scale to support NRG's digital environment as well as to offer competitive products to NRG's customers by developing its system to address restrictive standards for data protection such as HIPPA and SOX, while ensuring that such standards address compliance

[14] *See* https://www.sarbanes-oxley-101.com/sarbanes-oxley-audits.htm for more information.

across many jurisdictions. An illustrative sampling of some of these other laws is provided below for broader context:

- Texas Business and Commerce Code - Section 521.001 et seq. - Identity Theft Enforcement and Protection Act (Breach Notification, Security) - United States

  > Businesses shall have ***reasonable procedures*** in place to protect and safeguard sensitive personal information, collected and stored in the regular course of business, from unlawful use or disclosure.[15]

- California Privacy Rights Act of 2020 (CPRA) - 1798.100 et seq. - California - United States

  > Businesses must implement ***reasonable procedures and practices*** to protect personal information from unauthorized/illegal access, destruction, use, modification or disclosure in accordance with California Civil Code 1798.81.5. ***Protection measures must be appropriate to the nature of the personal information held.*** If a business implements reasonable security procedures and practices following a breach, it will not be considered a cure for the breach.[16]

- Illinois Complied Statutes - Section 815 ILCS 530/1 - Personal Information Protection Act (Breach Notification and Data Destruction) - United States

  > Data collectors must implement and maintain ***reasonable security measures*** to protect records containing personal information of Illinois residents from unauthorized access,

---

[15] *See* V.T.C.A., Bus. & C. § 521.052 ("(a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business. (b) A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by: (1) shredding; (2) erasing; or (3) otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means. (c) This section does not apply to a financial institution as defined by 15 U.S.C. Section 6809. (d) As used in this section, "business" includes a nonprofit athletic or sports association.")

[16] *See* Cal. Civ. Code § 1798.81.5 (West) ("(b) A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.(c) A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is not subject to subdivision (b) shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.")

acquisition, destruction, use, modification or disclosure. Contracts for disclosure of these records must require the recipient to implement and maintain reasonable security measures. Data collectors subject to and in compliance with the GLBA are deemed in compliance with these obligations.[17]

- New York - General Business Law Section 899-AA and Section 899-BB - Information Security Breach and Notification Act (Breach Notification) - United States

  This law requires any person or business that owns or licenses computerized data which includes private information of a resident of New York to ***develop, implement and maintain reasonable safeguards*** to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data. Compliance requires a data security program that includes ***reasonable administrative, technical, and physical safeguards*** (e.g. identifying and assessing risks, assessing effectiveness of safeguards, selecting appropriate service providers). A person or business shall be deemed in compliance with security requirements if they are subject to, and in compliance with Title V of the GLBA, HIPAA and HITECH Regulations, or the NY State Cybersecurity Requirements for Financial Services Companies. Violations can result in action by the AG to obtain injunctions and civil penalties. There is no private right of action.[18]

---

[17] *See* 815 Ill. Comp. Stat. Ann. 530/45 ("(a) A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. (b) A contract for the disclosure of personal information concerning an Illinois resident that is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. (c) If a state or federal law requires a data collector to provide greater protection to records that contain personal information concerning an Illinois resident that are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this Section. (d) A data collector that is subject to and in compliance with the standards established pursuant to Section 501(b) of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801, shall be deemed to be in compliance with the provisions of this Section.")

[18] *See* N.Y. Gen. Bus. Law § 899-bb (McKinney) ("2. Reasonable security requirement. (a) Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data. (b) A person or business shall be deemed to be in compliance with paragraph (a) of this subdivision if it either: (i) is a compliant regulated entity as defined in subdivision one of this section; or (ii) implements a data security

- Virginia - Consumer Data Protection Act of 2023- § 59.1-578 et seq.

> Data Controllers must establish, implement, and maintain ***reasonable administrative, technical, and physical data security practices*** to protect the confidentiality, integrity, and accessibility of personal data. ***Such data security practices shall be appropriate*** to the volume and nature of the personal data at issue.[19]

---

program that includes the following: (A) reasonable administrative safeguards such as the following, in which the person or business: (1) designates one or more employees to coordinate the security program; (2) identifies reasonably foreseeable internal and external risks; (3) assesses the sufficiency of safeguards in place to control the identified risks; (4) trains and manages employees in the security program practices and procedures; (5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and (6) adjusts the security program in light of business changes or new circumstances; and(B) reasonable technical safeguards such as the following, in which the person or business: (1) assesses risks in network and software design; (2) assesses risks in information processing, transmission and storage; (3) detects, prevents and responds to attacks or system failures; and (4) regularly tests and monitors the effectiveness of key controls, systems and procedures; and (C) reasonable physical safeguards such as the following, in which the person or business: (1) assesses risks of information storage and disposal; (2) detects, prevents and responds to intrusions; (3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and (4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed. (c) A small business as defined in paragraph (c) of subdivision one of this section complies with subparagraph (ii) of paragraph (b) of subdivision two of this section if the small business's security program contains reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers. (d) Any person or business that fails to comply with this subdivision shall be deemed to have violated section three hundred forty-nine of this chapter, and the attorney general may bring an action in the name and on behalf of the people of the state of New York to enjoin such violations and to obtain civil penalties under section three hundred fifty-d of this chapter. (e) Nothing in this section shall create a private right of action."_

[19] *See* Va. Code Ann. § 59.1-578 (West) ("A controller shall: (1) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer; (2) except as otherwise provided in this chapter, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent; (3) establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue;(4) not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to § 59.1-577 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and (5) not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known

- Massachusetts- 201 CMR 17.00: Standards for the Protection of Personal Information of MA Residents (Data Protection and Computer System Requirements)- United States

  This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer..[20]

---

child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.).")

[20] See 201 CMR 17.03 Duty to Protect and Standards for Protecting Personal Information. (1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to: (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated. (2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to: (a) Designating one or more employees to maintain the comprehensive information security program; (b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: 1. ongoing employee (including temporary and contract employee) training; 2. employee compliance with policies and procedures; and 3. means for detecting and preventing security system failures. (c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises. (d) Imposing disciplinary measures for violations of the comprehensive information security program rules. (e) Preventing terminated employees from accessing records containing personal information. (f) Oversee service providers, by: 1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with 201 CMR 17.00 and any applicable federal regulations; and

2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 201 CMR 17.03(2)(f)2. even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010. (g) Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers. (h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized

If the Commission were to impose new Pennsylvania specific data security obligations for its licensed NGSs and EGSs, designed to accomplish similar goals as the foregoing referenced Federal and State laws, there may be a significant replication of standards and duplication of processes, which may not result in enhancements to cybersecurity over and above what is already required by existing laws. To the contrary, rather than enhance cybersecurity, it may detract from it because NRG would need to channel resources and time in ensuring compliance with the new and additional regulations instead of devoting those resources to the ongoing need to stay abreast of developments, enhancements and ever-evolving threats.

Furthermore, as the Commission noted, "The process of deconflicting regulations that duplicate, contradict or overlap each other has become an art unto itself."[21] The need to oversee, audit and manage the administration of duplicate regulations in a complex field of data security would impose on the Commission the obligation to invest substantial time, resources and financial expenditures in addition to developing and maintaining expertise in the complex world of data security and cybersecurity, all which may not result in an added benefit of enhancing the data security of NGS or EGS or be necessary to accomplish the Commission's stated goals. As the Commission noted, "…the administrative costs of maintaining self-certifications regulations may exceed any cybersecurity benefit the existing regulations may impart."[22] Certainly, to expand the scope of the existing regulations as well as the population to whom they may apply

---

use of personal information; and upgrading information safeguards as necessary to limit risks. (i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information. (j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

21 ANOPR at 19.

22 ANOPR at 15.

will only serve to exponentially increase the administrative costs of developing, implementing, overseeing and maintaining those new and expanded cybersecurity regulations.

2. Perceived Benefits Of Applying New Requirements To Suppliers Not Commensurate With Risks Such Entities May Pose

Furthermore, any perceived benefit of regulating an EGS or NGS may not be commensurate with the risk such entities pose, or whether such entities are even the ones who can control risk to the infrastructure and consumer data available from a utility.

Pursuant to Pennsylvania's data breach notification statute, protected "personal" information is defined as an individual's first name or initial with last name in combination with one or more of the following elements: (1) social security number, (2) driver's license or state identification card number; and/or (3) account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.[23] The customer information that the NRG subsidiaries access to provide services to end user customers does not include the data elements set forth in Pennsylvania's data breach statute but, rather, generally includes name, address, account number and usage history. Importantly, the Commission has directed and significantly limited what customer information is made available through the Eligible Customer Lists of the utilities[1] and, as noted previously, licensed EGSs and NGSs are required to comply with the Commission's privacy regulations at 52 Pa. Code §§ 54.8 (EGS) and 62.78 (NGSs) when in possession of such consumer information. Importantly, EGSs and NGSs do not need access to highly confidential customer information, including those data elements identified in Pennsylvania's data breach

---

[23] *See* 73 P.S. § 2302. Effective May 2, 2023, S.B. 696 amends the definition to include the following data elements: (1) medical information; (2) health insurance information; and, (3) a user name or email address in combination with a password or security question and answer that would permit access to an online account.

notification statute, in the normal course of providing retail end user supply services. Because the data they do access through the utility's billing system to provide service is already governed and limited by Commission regulations, there is not a need to impose new requirements on NGSs and EGSs intended to protect this information.[24] Rather, NRG respectfully submits that current regulatory obligations to maintain the confidentiality of the type of limited customer information the Commission permits an NGS or EGS to receive are sufficient to protect those elements of data an EGS or NGS is permitted to receive, and therefore adequately address risks associated with the loss of such data. Additional regulations are not needed because NGS and EGS do not obtain highly sensitive consumer data.

Whether regulating EGS/NGS will accomplish the Commission's stated goal of protecting the infrastructure may also be questioned in light of the fact that access to a utility's systems and the type of data made available are in the direct and sole control of the utility, and not the EGS or NGS. An NGS or EGS has no control or influence over the way it is granted access to customer information and the way the utilities allow communication of such data. So, for example, if an EGS or NGS meets or exceeds current industry standards over password protection, but the utility does not, then any purported regulations in that regard will not accomplish the stated goal. The appliable energy IT infrastructure, IT architecture and data access to consumer information is developed and maintained by the utilities. The security of that architecture is the primary responsibility and obligation of the utilities. The public interest may be better served by expending the Commission's time, resources and expenditures to ensure that utilities design and maintain their IT infrastructure, architecture, communication protocols and

---

[24] Pennsylvania also has a general data breach notification statute that applies to any entity that both: (1) conducts business in Pennsylvania; and, (2) owns, licenses, or maintains computerized data that includes personal information. *See* 73 P.S. §§ 2301 to 2308 and 2329 to 2330.

web portals pursuant to currently accepted industry standards in order to eliminate vulnerabilities in their own information security programs which will serve to enhance the integrity of the utility's systems and data protection and meet the Commission's goals.

3. Overly Prescriptive Requirements Should Be Avoided Due to Complexity Of Data Security Issues

While NRG's view is that no additional regulations are needed for its licensed suppliers, of particular interest to the Commission may be that upon review of the above-referenced laws and regulations (as emphasized in the above), they generally require the implementation of reasonable administrative, technical, and physical safeguards selected by the entity subject to the law, rather than adherence to specific set of data security standards proscribed by the regulator. Importantly, the entity subject to such laws has discretion to select which of the generally accepted industry standards it will adhere to, including for example, ISO 27001 and 27002, ISO 27017, NIST Cybersecurity Framework, AICPA Trust Services Principles, Information Technology Library (ITIL) standards, Control Objectives for Information and related Technology (COBIT) standards, Center for Internet Security (CIS) Controls.

As an alternative to expansive regulations and given that NGSs and EGSs as well as the Commission have a common goal of protecting Pennsylvania's energy infrastructure, NRG respectfully suggests a resolution posed by the Office of Cybersecurity, Energy Security, and Emergency Response ("CESER"):

> Because of the highly-dynamic technology and threat environment, effective cybersecurity practices require a continuous and comprehensive assessment of threats, identification of system vulnerabilities, strengthening and sharing of recognized security practices, and analysis of the impact of cyber events on the energy infrastructure. Timely bi-directional sharing of cyber threat information between the energy sector and government helps to determine the severity, scope, and nature of threats and

rapidly develop needed mitigations.[25]

Accordingly, in place of regulation, a public-private partnership could be established to among other things, foster communication and collaboration to facilitate sharing of data security enhancements and exchange threat information.

Participation In The Marketplace Requires Extensive Self-Regulation

A reality of conducting business in today's environment is that the lack of adequate cybersecurity is a significant risk which could be critical to the financial success and stability of the company. Today, cybersecurity risk is a component of the overall business risk environment and, as such, requires that an organization manage it through strong information security programs, data minimization, and informed decision-making processes.

The responsibility for cybersecurity is no longer relegated to the IT Department; rather it has risen to the board room. Companies both large and small have significant self-interest and commercial incentives to develop and maintain robust data security programs. These commitments and investments, which are apart from legal and regulatory requirements, should be considered by the Commission in considering limiting expansion of data security regulations to EGSs and NGSs, particularly with the limited role of an EGS and NGS in relation to the security of critical energy infrastructure, as well as their non-access to highly sensitive personal information in the possession of the jurisdictional entities.

In managing commercial risk, NRG has recognized that cybersecurity is critical to its success and its stability. NRG manages cybersecurity risk at the executive level and also through

---

[25] See https://www.energy.gov/ceser/energy-sector-cybersecurity-preparedness. CESER addresses the emerging threats of tomorrow while protecting the reliable flow of energy to Americans today by improving energy infrastructure security and supporting the Department of Energy's (DOE) national security mission. CESER's focus is preparedness and response activities to natural and man-made threats, ensuring a stronger, more prosperous, and secure future for the Nation.

its information security team which oversees and implements best practices. NRG owes a duty to its stakeholders and its customers to ensure that it and its information assets are protected. Accordingly, NRG takes securing its systems from cyber and other attacks very seriously. NRG has a dedicated Information Technology Data Security ("IT") team which works to maintain the confidentiality, integrity, and availability of data systems and does this by designing and implementing various processes and procedures involving security strategies. The IT team also oversees security risk and management of incident response and stays up to date with the latest security threats and technologies. In addition, NRG engages outside third party evaluations of its security program and regularly tests its systems. NRG regularly performs tabletop exercises as part of its Business Continuity process in preparation for cyber events and requires on-line cyber security awareness and phishing training for all of its employees each year as part of its compliance program.

NRG also adheres to strong ethical standards in the performance of the services it provides and the products it delivers. These standards are spelled out in its Code of Conduct, which employees are required to review, acknowledge and comply. NRG's Code of Conduct expressly addresses the need to protect customer information as well as the requirement to protect information assets by setting forth specific principles to safeguard information and information assets: "We safeguard NRG' confidential and proprietary information and any

entrusted to us by others…" The Code of Conduct also expressly addresses the need for vigilance to cyber-attack prevention:

> We are all responsible for protecting our network and the security of our equipment…Our network and computer equipment help to drive our business. We depend on them for our everyday activities that involve valuable, confidential information about NRG, our colleagues and our customers…. [to] prevent cyber-attacks require[s] personal responsibility and diligence. Knowing how these breaches occur can help us prevent them. Listed below are various common examples:
>
> • Phishing
> • Click-bait
> • Spear-phishing
> • Catphishing
> • Malware
> • Man-in-the-Middle Attack (usually happens when using unsecured public Wi-Fi)

All NRG employees must participate in cybersecurity training which fully explains such attacks and identifies ways to spot, avoid and report them to the IT team for investigation. NRG employees are also required to comply with applicable NRG policies as well as applicable federal, state and local laws and regulations.

In addition to self-imposed cybersecurity risk management, to participate in the marketplace, many of our contractual relationships require NRG to represent and warrant that it maintains industry-standard data security practices and maintain cyber liability insurance. As part of acquiring cyber insurance, NRG is required to undergo a significant review process which includes a written application, a data security questionnaire, lengthy interviews with the underwriter, and a third party's assessment of NRG's data security program. Insurers review NRG's cyber controls at least annually prior to the insurance renewal date. If NRG's data security practices fail to meet required standards to purchase cyber insurance, then NRG might not be able to secure a policy, which could result loss of significant business relationships. In

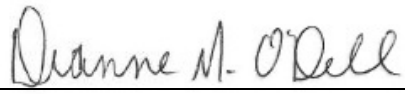
addition, if NRG's data security practices are not sufficiently robust, insurance premiums could be cost-prohibitive and negatively impact decisions for maintaining NRG's financial strength.

In sum, apart from the legal requirements, there are significant commercial pressures on NRG establish a robust cybersecurity program to ensure the protection of its information assets, confidential customer and other data which is a pre-requisite to the operation of a diverse, successful business.

III. CONCLUSION

NRG's view is that protecting its network and data systems from attacks, protecting the security and confidentiality of the customer information entrusted to it and complying with good data security practices and legal requirements are core functions to operating successfully. NRG recognizes the importance from the perspective of the Commission of ensuring that utilities and other regulated entities are incorporating and following reasonable data security practices. However, balancing the role of the NGSs and EGSs in the retail energy market sector, the data to which they have access, the existing array of cybersecurity regulations and commercial practices with the minimal benefit that may result from imposing new regulatory cybersecurity related regulatory requirements, does not support extending a revision of existing Commission regulations to NGSs and EGSs.

Respectfully Submitted,



Deanne M. O'Dell, Esquire
PA Attorney ID # 81064
Eckert Seamans Cherin & Mellot, LLC
213 Market Street, 8th Fl.
Harrisburg, PA 17108-1248
717 237 6000
dodell@eckertseamans.com

Attorneys for NRG Energy, Inc.

Dated: February 8, 2023