STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

CASE 18-M-0376 - Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place.

CASE 15-M-0180 - In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products.

CASE 98-M-1343 - In the Matter of Retail Access Business Rules.

ORDER ESTABLISHING MINIMUM CYBERSECURITY AND PRIVACY PROTECTIONS AND MAKING OTHER FINDINGS

Issued and Effective: October 17, 2019

TABLE OF CONTENTS

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

At a session of the Public Service Commission held in the City of Albany on October 17, 2019

COMMISSIONERS PRESENT:

John B. Rhodes, Chair
Diane X. Burman, concurring
James S. Alesi
Tracey A. Edwards
John B. Howard

CASE 18-M-0376 - Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place.

CASE 15-M-0180 - In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products.

CASE 98-M-1343 - In the Matter of Retail Access Business Rules.

ORDER ESTABLISHING MINIMUM CYBERSECURITY AND PRIVACY PROTECTIONS AND MAKING OTHER FINDINGS

(Issued and Effective October 17, 2019)

BY THE COMMISSION:

INTRODUCTION

In a petition filed on February 4, 2019 (Petition), Consolidated Edison Company of New York, Inc., Orange and Rockland Utilities, Inc., Central Hudson Gas & Electric Corporation, National Fuel Gas Distribution Corporation, The Brooklyn Union Gas Company d/b/a National Grid NY, KeySpan Gas East Corporation d/b/a National Grid, and Niagara Mohawk Power Corporation d/b/a National Grid, New York State Electric & Gas Corporation, and Rochester Gas and Electric Corporation (collectively, Joint Utilities or JU) request an order: (1) approving the business-to-business process

used to develop the Data Security Agreement (DSA);[1] (2) approving continued use of the business-to-business process to amend the DSA; (3) adopting minimum standard requirements to be included in a DSA; and, (4) affirming the existing authority of the Joint Utilities to require the execution of a DSA by entities seeking access to utility customer data or the distribution utility's Information Technology (IT) systems and, if they fail to do so, disconnect them from the utility IT systems and remove their access to customer information. The Joint Utilities seek to protect customer data and distribution utility IT systems by requiring entities seeking access to utility customer data or utility IT systems to execute a DSA. These entities include, inter alia, Energy Service Companies (ESCOs), Distributed Energy Resource Suppliers (DERS), Direct Customers, and their applicable contractors (collectively referred to as Energy Service Entities (ESEs)).[2]

By this Order, the Commission grants, in part, and denies, in part, the relief requested by the Joint Utilities. This Order does not specifically adopt the terms of the DSA, but instead adopts minimum cybersecurity and data privacy requirements for entities that receive from, or exchange customer data with, the utilities on an electronic basis other than by email. As discussed below, this current approach will provide a universal foundation of cybersecurity and data privacy requirements, while the Commission will continue to develop such requirements and may modify or expand upon them in the future, as appropriate.

---

[1] For the purposes of this Order, the DSA is defined as including both data privacy protections and cybersecurity protections.

[2] The Public Service Commission's (Commission) Order Instituting Proceeding, issued on June 18, 2018 in this Case, adopted a narrower definition of ESE focusing on the retail energy market. For purposes of this Order, the Commission adopts the broader definition.

Ensuring that cybersecurity protections remain current and that the appropriate balance is struck between data privacy and promoting consented data access will require ongoing Commission attention.

Related to this Petition are two petitions for declaratory rulings and one request for clarification, which are also addressed by this Order. The first is a petition for a declaratory ruling filed by the Joint Utilities on November 9, 2018, in Cases 98-M-1343 and 18-M-0376 (JU Declaratory Ruling Petition).[3] The JU Declaratory Ruling Petition seeks confirmation that a distribution utility may discontinue an ESCO's participation in the utility's retail access program pursuant to Section 2.F. of the Uniform Business Practices (UBP) if the ESCO fails to meet minimum data security standards, including execution of a DSA.

The second related petition is a petition for a declaratory ruling filed by Mission:data Coalition on November 30, 2018 in Case 18-M-0376 (Mission:data Declaratory Ruling Petition).[4] The Mission:data Declaratory Ruling Petition seeks a

[3] Case 18-M-0376, et al., Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place, Petition of the Joint Utilities for Declaratory Ruling Regarding Their Authority to Discontinue Utility Access to Energy Service Companies in Violation of the Uniform Business Practices (filed November 9, 2018).

[4] Case 18-M-0376, supra, Petition of Mission:data Coalition for Declaratory Ruling Regarding the DER Oversight Order's Exemption of DER Suppliers from Certain Cyber Security Requirements (filed November 30, 2018).

ruling that the Commission's DER Oversight Order[5] prohibits the utilities from requiring DERS that utilize Green Button Connect (GBC) to sign a DSA as a prerequisite to receive customer data.

Finally, also related to the present Petition is a request for clarification filed by the Joint Utilities on November 21, 2017 in Case 15-M-0180 (JU Request for Clarification).[6] The JU Request for Clarification seeks clarification on the DER Oversight Order, specifically, whether Section 2.C. of the Uniform Business Practices for Distributed Energy Resource Suppliers (UBP-DERS) apply to DERS who are seeking to obtain customer data, regardless of the utility platform involved, so that the necessary rules for obtaining consent, among other things, apply across all platforms, not only to the Electronic Data Interchange (EDI) platform.

BACKGROUND

A cyber event in spring of 2018 involving an Electronic Data Interchange (EDI) provider prompted the distribution utilities and the Commission to reevaluate cybersecurity in the retail market. While already requiring a DSA with new ESCOs and other providers that interface electronically with the JU's IT

[5] Case 15-M-0180, In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products, Order Establishing Oversight Framework and Uniform Business Practices for Distributed Energy Resource Suppliers (issued October 19, 2017) (DER Oversight Order).

[6] Case 15-M-0180, supra, Joint Utilities' Request for Clarification (filed November 21, 2017).

systems, the Joint Utilities in March 2018 asked existing ESCOs to execute a DSA that included a Vendor Risk Assessment (VRA).[7]

Following numerous questions and concerns presented by the ESCO community, Department of Public Service Staff (Staff) held a stakeholder meeting on May 31, 2018, which included ESCO representatives, the Joint Utilities, EDI providers, and some DERS. This meeting was the first in a "business-to-business" process intended to collaboratively reach a DSA that addresses the Joint Utilities' and ESCO community concerns. The Commission's Order Instituting Proceeding, issued on June 14, 2018, supported the proposed collaborative process and underscored the importance of maintaining robust cybersecurity standards to "mitigate vulnerability of utility IT systems to cyber-attacks, and to ensure that confidential and sensitive customer information remains safeguarded from potential data breaches."[8]

The business-to-business process included two rounds of written comments, three days of in-person technical conferences,[9] as well as a teleconference meeting among interested stakeholders to discuss specific technical issues.[10] Additionally, during the business-to-business process, stakeholders and Staff urged the Joint Utilities to create uniformity between the various VRAs so that an ESE that undergoes an assessment in one distribution utility territory, would satisfy the assessment requirement in other territories and would not be subject to multiple lengthy

---

[7] The VRA is used by the Joint Utilities for determining a vendor's cybersecurity readiness before any system connection or data transfer. It includes 29 risk areas and requires the vendor to provide information on the controls they have in place to address this risk.

[8] Case 18-M-0376, supra, Order Instituting Proceeding, p. 3 (issued June 14, 2018) (June 2018 Order).

[9] May 31, 2018 and July 26-27, 2018.

[10] August 1, 2018.

VRAs. As a result, and in an effort to simplify the VRA process and create uniformity across the various distribution utilities, the Joint Utilities replaced the individual utility specific VRAs with a uniform Self-Attestation (SA). The SA contains 16 cybersecurity controls that are consistent with risk based frameworks, such as National Institute of Standards and Technology (NIST), and requests that ESEs attest that they observe these controls, or if the ESE is not already doing so, to implement these controls within a reasonable timeframe.

Following this collaborative process, the Joint Utilities circulated the DSA to all ESCOs, requesting that they be signed by August 18, 2018, and returned by August 31, 2018. As directed by the June 2018 Order, Staff filed a Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry on September 24, 2018 detailing the business-to-business process and its results.[11] At the time of filing the Staff Report, a vast majority of ESCOs had executed the DSA, representing approximately 90% of the retail market.

The June 2018 Order also directed parties to address these cybersecurity issues with respect to DERS in addition to retail market participants.[12] Staff conducted three additional collaborative meetings with the goal, inter alia, of engaging more DERS on these issues. The first of these meeting was held on November 14, 2018, and following that meeting, the JU again sought a round of comments on the DSA, which were received on or before December 17, 2018. Additionally, on December 13, 2018, the

[11] Case 18-M-0376, supra, Department of Public Service Staff Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry (September 24, 2018) (Staff Report).

[12] June 2018 Order, p. 3.

Commission issued its Order Adopting Accelerated Energy Efficiency Targets, which directed a collaborative process to develop GBC terms and conditions for third parties accessing data through GBC as well as the utilities' interaction with these third parties.[13] Following that Order, two working groups were held to develop the GBC terms and conditions; the first on February 21, 2019 in Albany, which began the process of identifying the necessary terms and conditions and the second on March 26, 2019 in New York City, which included discussion on the disputed provisions of the DSA – indemnification, cybersecurity insurance, language issues, and requirements for DERS third parties. On February 4, 2019, the Joint Utilities filed the instant Petition.

THE PETITION

In the Petition, the Joint Utilities request that the Commission: (1) confirm the business-to-business process used to develop the DSA was appropriate; (2) authorize the amendment of the DSA through continued use of the business-to-business process; (3) adopt minimum standard requirements to be included in a DSA; and (4) affirm the authority of the Joint Utilities to require execution of a DSA and to disconnect from the utility's IT systems entities that fail to execute a DSA. Regarding point (3), the Joint Utilities ask that minimum standard requirements: a) specify compliance with the UBP, UBP-DERS, or other applicable Commission rules; b) address the transfer of information; c) maintain confidentiality of Joint Utilities and ESEs information, including the protection of customer data; d) require the return and destruction of information; e) address each Party's responsibility

[13] Case 18-M-0084, In the Matter of a Comprehensive Energy Efficiency Initiative, Order Adopting Accelerated Energy Efficiency Targets (issued December 13, 2018).

and liability for data security incidents; f) require cybersecurity insurance; g) define minimum cybersecurity requirements; h) address how to determine whether ESEs have and maintain minimum levels of cybersecurity; and i) require ESE indemnification of the Joint Utilities.

The process by which the DSA was arrived at, the Joint Utilities continue, was a lengthy, publicly noticed proceeding that provided parties a full opportunity to participate. Moreover, the Joint Utilities assert that entities that either do business with utilities, have utility data, including customer information, or have any connection to the utility system should maintain adequate cybersecurity in order to protect both the utility IT systems, as well as to protect sensitive customer data from improper release.

The Joint Utilities ask, not that ESEs be required to maintain the same level of cybersecurity protections as vendors and contractors of the utility, but instead that these entities maintain minimum level cybersecurity protections as laid out in the DSA. According to the Joint Utilities, "each market participant must bear the cost responsibility of its IT systems and customers without shifting cost responsibility to nonparticipating customers or entities."[14]

The Joint Utilities claim that they currently have the authority under the UBP and UBP-DERS to protect their IT systems and disconnect third parties from those IT systems who pose a risk to system security. Thus, the Joint Utilities assert that they can already require any entity seeking to access customer data through the utility IT systems to execute a DSA, but that a formal decision from the Commission is sought to address the reluctance

[14] Petition, p. 4.

by some ESEs to comply with the terms of a DSA until such DSA is approved by the Commission.

The Joint Utilities state that they are supportive of the development of commodity, renewable, and energy efficiency markets, but assert that all market participants should bear the costs associated with doing business. The Joint Utilities oppose the assertion that entities looking to enter into nascent markets should not have to bear the costs of cybersecurity protections because those costs will act as a market barrier and stifle market development. This argument, the Joint Utilities emphasize, shifts those costs to other market participants, the utilities, and ultimately customers, whether or not they participate in retail or DER markets. The Joint Utilities argue that failing to address cybersecurity at the onset of market development will lead to cybersecurity issues, future compliance costs, and potentially substantial costs in the event of a cybersecurity incident.

NOTICE OF PROPOSED RULE MAKING

Pursuant to the State Administrative Procedure Act (SAPA) §202(1), a Notice of Proposed Rulemaking was published in the State Register on February 27, 2019 [SAPA No. 18-M-0376SP1]. The time for submission of comments pursuant to the SAPA Notice expired on April 29, 2019. Additionally, on February 20, 2019, a Notice Soliciting Comments on the Petition was issued by the Secretary. Fifteen entities submitted written comments pursuant to these notices and the Joint Utilities submitted reply comments. The comments received are addressed, as applicable, in the Discussion section below, and a full summary of the comments is attached to this Order as Appendix A. With respect to the JU Request for Clarification, a Notice of Proposed Rulemaking was published in the State Register on December 13, 2017 [SAPA No. 15-M-0180SP4]. No comments were received on the JU Request for

Clarification, but those comments that relate to both the instant Petition and the JU Request for Clarification are addressed below and in Appendix A.

LEGAL AUTHORITY

The Commission has the responsibility and the authority under the Public Service Law (PSL) to ensure that utilities carry out "their public service responsibilities with economy, efficiency, and care for the public safety, the preservation of environmental values and the conservation of natural resources."[15] Pursuant to the PSL, the Commission has "authority to condition ESCOs' eligibility to access utility [distribution IT systems] on such terms and conditions that the [Commission] determines to be just and reasonable."[16] The Commission's UBP were adopted pursuant to this authority and set forth various regulatory eligibility requirements for ESCOs to begin accessing, and to continue accessing, utility distribution IT systems for the purpose of selling energy services to customers. Thus, the Commission has authority over the tariffed rules and regulations of electric and gas distribution utilities, and has placed conditions on when the distribution utilities may allow ESCOs to use utility infrastructure to distribute electricity and natural gas to ESCO customers.[17] The Commission has jurisdiction and

---

[15] PSL §5(2).

[16] Matter of National Energy Marketers Assn. v. New York State Pub. Serv. Commn., ___ N.Y.3d ___, 2019 N.Y. Slip. Op. 03655, at 18 (2019); see Public Service Law §§ 5(1)(b), 65(1), 66(5), 66-d(2); see generally GBL § 349-d(11).

[17] Case 94-E-0952, In the Matter of Competitive Opportunities Regarding Electric Service, Opinion and Order Establishing Regulatory Policies for the Provision of Retail Energy Services (issued May 19, 1997) (Opinion 97-5); Opinion and Order Deciding Petitions for Clarification and Rehearing (issued November 18, 1997) (Opinion 97-17).

authority to establish and modify the conditions under which ESCOs may offer electric and gas commodity service to customers, and to impose consequences when ESCOs fail to abide by those conditions.

Moreover, as discussed in the REV Framework Order[18] and the DER Oversight Order,[19] the Commission's authority to impose rules and requirements on DERS stems from both its authority over electric corporations, as defined in PSL §§2(13) and 53, as well as its responsibility to ensure that participants in Commission-directed or -authorized programs, tariffs, or markets receive appropriate protections.

The Commission is authorized to issue a declaratory ruling with respect to: (i) the applicability of any rule or statute enforceable by it to any person, property, or state of facts; and (ii) whether any action by it should be taken pursuant to a rule. The Commission also may decline to issue such a declaratory ruling. This authority is expressly established by State Administrative Procedure Act §204 and governed by the Commission's Rules of Procedure, contained in 16 NYCRR Part 8, implementing that statute. Declaratory rulings involving interpretations of existing statutes, rules, or regulation are not "actions" within meaning of the State Environmental Quality Review Act (SEQRA) and its implementing regulations and, therefore, they may be issued without further SEQRA review.[20]

---

[18] Case 14-M-0101, Proceeding on Motion of the Commission in Regard to Reforming the Energy Vision, Order Adopting Regulatory Policy Framework and Implementation Plan (issued February 26, 2015).

[19] Case 15-M-0180, Regulation and Oversight of Distributed Energy Resource Providers and Products, Order Establishing Oversight Framework and Uniform Business Practices for Distributed Energy Resource Suppliers (issued October 19, 2017).

[20] See 6 NYCRR §617.5(c)(37) (defining "interpretation[s] of an existing code, rule or regulation," as Type II actions not subject to review under SEQRA).

DISCUSSION

While cybersecurity has long been a priority for the Commission and the industries it regulates, that priority has become even more pressing given the proliferation of digitalizing operations and reliance on electronic communications.[21] The Commission has consistently held that "[p]rotection of consumer information is a basic tenet of the Public Service Law and our policies."[22] The Commission again emphasized the need for cyber protections in opening the Reforming the Energy Vision proceeding, stating that "[c]yber security is highly important for reasons of privacy, reliability, resiliency and market confidence."[23] The Commission has also recently utilized a DSA as a means of establishing cyber protections for entities who receive customer information from the distribution utilities.[24]

In the CCA DSA Order, the Commission again recognized the need to protect customer data and adopted a DSA, with modifications, filed by the Joint Utilities intended for use in Community Choice Aggregation (CCA) programs. The DSA adopted in the CCA DSA Order served as a starting point for the discussions in the business-to-business process. Although the Commission declined to require cybersecurity insurance in the CCA DSA Order,

---

[21] See Case 14-M-0101, supra, Order Adopting Distributed System Implementation Plan Guidance, pp. 2-3, (issued April 20, 2016).

[22] Case 07-M-0548 et al., Proceeding on Motion of the Commission Regarding an Energy Efficiency Portfolio Standard, Order on Rehearing Granting Petition for Rehearing, p. 17 (issued December 3, 2010).

[23] Case 14-M-0101, supra, Order Adopting Regulatory Policy Framework and Implementation Plan (Issued February 26, 2015), p. 99.

[24] Case 14-M-0224, Proceeding on Motion of the Commission to Enable Community Choice Aggregation Program, Order Approving Community Choice Aggregation Program and Utility Data Security Agreement with Modifications (Issued October 19, 2017) (CCA DSA Order).

the Joint Utilities propose to require it in the present version of the DSA to be applied to all entities that electronically exchange customer information with the distribution utilities. As discussed above, the DSA was modified based on comments and feedback from ESEs during the business-to-business process and is now before the Commission for approval.

Maintaining the security of customer data and the distribution utilities' IT systems is of paramount importance. The Commission is cognizant of potential benefit of data and information to underpin the provision of valuable offers and services to customers, and to enable smart deployment of distributed and clean resources that provide value to the energy system, and hence to customers. It thus gives weight to the concerns of third parties regarding potentially burdensome cyber hygiene requirements. Importantly, the Commission recognizes that the data is the customer's data and that customers have a right to direct or consent to the use of that data.

Therefore, 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.

The Business-to-Business Process

The business-to-business collaborative process provided interested stakeholders an opportunity to discuss and negotiate the terms of the DSA prior to it being brought before the Commission. Several parties express dissatisfaction with the collaborative process which led up to the filing of the present Petition.

1. Party Comments

Energy Technology Savings, Inc. DBA Logical Buildings (Logical Buildings) comments that the business-to-business process utilized to develop the DSA was necessary and productive, but that it should not be used as a substitute to a formal SAPA process with the Commission as the final decision maker. Some parties assert that the business-to-business process was "coercive" or that the utilities had more bargaining power. These parties, including UtiliSave Inc. (Utilisave), the Retail Energy Suppliers Association (RESA), Mission:data Coalition (Mission:data), and Agway Energy Services, LLC (Agway) claim that granting the Petition would inappropriately affirm this unreasonable process. These commenters argue that the process was unfair due to the inherently superior bargaining power of the Joint Utilities. The New York Retail Choice Coalition and supporting ESEs (collectively, the DSA Coalition) asserts that granting the Petition would result in Commission approval without any consideration of the issues identified by the DSA Coalition, and that instead a rulemaking is necessary. RESA comments that, while the utility compromised on several points, they did not modify and/or address all the aspects of the DSA which the ESCOs disagreed with.

Agway offers that the business-to-business process was too short and did not include enough industry participation to be considered a suitable process. Consumer Power Advocates (CPA) and

Luthin Associates, Inc. (Luthin) (collectively CPA) and New York Solar Energy Industries Association (NYSEIA) Comment that not all ESCOs, DERS, or other ESEs were participants to the business-to-business process and that the process was not a level playing field. CPA and Utilisave claim that the DSA was originally developed to apply to ESCOs and that the utilities are improperly attempting to expand its applicability to other third parties, including DERS.

Advanced Energy Economy Institute (AEE Institute) in conjunction with Advanced Energy Economy (AEE), the Alliance for Clean Energy New York (ACE NY), the Northeast Clean Energy Council (NECEC), Advanced Energy Management Alliance (AEMA), and their joint and respective member companies (collectively, the Advanced Energy Companies) comment that the business-to-business process was not appropriate for development of the terms under which the Joint Utilities must provide customer data to third parties due to potential anti-competitive and market-access concerns. Advanced Energy Companies propose that the GBC collaborative is the proper venue for addressing cybersecurity requirements.

Some parties assert that a more formal process should be used to develop the DSA going forward. RESA, the DSA Coalition, and the National Energy Marketers Association (NEM) avow that the development of a DSA or other cybersecurity requirements should be accomplished through a rulemaking process, not a collaborative. RESA asserts that the business-to-business process without Commission involvement has been an unsuitable process for development of the DSA. They ask that the utilities be required to ask for Commission approval in order to implement and enforce the DSA.

NEM asserts that the appropriate way to establish cybersecurity protections in the retail market is for the Commission to issue a notice of proposed rulemaking, gather

stakeholder feedback, and then adopt a policy based on the record. Only the Commission, NEM continues, can adopt rules and enforce them, and such authority cannot be delegated to the utilities. NEM proposes that a business-to-business process should occur after the Commission rulemaking to address implementation details.

NEM, Agway, and the DSA Coalition further argue that the business-to-business process did not comply with SAPA and that the Joint Utilities inappropriately sought to enforce the DSA and SA against ESCOs. These parties assert that the DSA was not issued for public comment via a notice of proposed rulemaking in the State Register, and that the business-to-business process did not satisfy the requirements of SAPA.

Moreover, several commenters, including Mission:data, the DSA Coalition, RESA, and NEM claim that in granting the Petition, the Commission would effectively be abdicating its responsibility to regulate the utilities and the markets, and instead be delegating that authority to the utilities. The DSA Coalition claims that the DSA allows the Joint Utilities to modify the DSA in their sole discretion at any time, for any reason, without recourse by ESEs.

Mission:data asserts that the Commission should not grant the Joint Utilities the authority to modify the DSA in the future without Commission intervention. NYPA comments that the Commission should develop a clear procedure for future amendments to the DSA in order to promote contractual and regulatory certainty.

In reply comments, the Joint Utilities assert that the business-to-business process was robust, that it included numerous meetings and discussions, and provided interested ESEs with multiple opportunities to submit written comments. In response to assertions that the Joint Utilities disregarded the comments and suggestions of ESEs, the Joint Utilities respond that the DSA is

replete with modifications that were made based on comments and input from ESEs during the collaborative process. The Joint Utilities further declare that they have the authority and the obligation to protect their IT systems and customer data, even without further action from the Commission.

Additionally, the Joint Utilities point out that through negotiation of the specific terms of the DSA, they have made numerous concessions and compromises in response to the comments and concerns of stakeholders. This included replacing the lengthy technical risk assessment to a two-page Self Attestation, reducing the amount of cybersecurity insurance from $10 million to $5 million, adding reciprocal language to the indemnification and other provisions, as well as numerous definition and language changes.

2. Discussion & Conclusion

The business-to-business process was initiated by Staff and endorsed by the Commission. This was not a utility driven process, but instead was a platform by which interested parties could engage in discussions to refine the DSA. Ultimately, it is the Commission's responsibility to decide what the appropriate level of cybersecurity and data privacy protections a third party obtaining customer data through electronic access to the utility IT systems should maintain. As discussed below, there is no need to affirm the business-to-business process utilized to arrive at the current draft of the DSA.

Several commenters contend that, such a collaborative process, while publicly noticed with multiple opportunities to comment, does not satisfy the requirements of SAPA. However, the Commission satisfied the requirements of SAPA through the publication of a Notice of Proposed Rulemaking in the State Register on February 27, 2019 and by considering the comments that were received thereto. Regardless of whether stakeholders

participated in, or agreed with, the results of the business-to-business process, the Commission now acts in response to the Joint Utility Petition in compliance with the due process afforded under SAPA. The collaborative process that led up to this rulemaking served as a valuable tool which allowed stakeholders to discuss and develop these issues in real time prior to being proposed to the Commission for approval. The collaborative process that led to the current Petition before the Commission is not determinative of the Commission's decision in this Order. Any party that believes it was not able to participate effectively in the collaborative process was able to submit comments in response to the SAPA notice.

With respect to comments that granting the Petition cannot be done until the Commission considers the DSA through a rulemaking process, there appears to be a misunderstanding regarding SAPA and the Commission's consideration of petitions. In filing the Petition, the Joint Utilities put the DSA before the Commission for consideration; and in filing a Notice of Proposed Rulemaking in the State Register, a rulemaking was commenced.

Contrary to the assertions of some commenters, the DSA does not allow the utilities to determine the appropriate protections and enforce those requirements with unlimited discretion. The Commission, by this Order, is determining the appropriate cybersecurity and privacy protections, in response to the Petition and stakeholder comments. Regarding the comments asserting that the business-to-business process did not comply with SAPA and thus any results of the collaborative should be disregarded, the Commission notes that a notice of proposed rulemaking is not required to convene a collaborative. Thus, the assertion that the Petition is seeking to cure process deficiencies from the business-to-business process is misplaced and represents a misunderstanding of SAPA. Prior to this Order,

no rule was adopted by the Commission, and the Joint Utilities did not seek formal discontinuance against any entity.

As a result, the Joint Utilities request that the Commission confirm the appropriateness of the business-to-business process is unnecessary. The appropriateness of the preceding collaborative is irrelevant to the actions taken pursuant to this Order.

Applicability of Cyber Requirements to DERS - Mission:data Declaratory Ruling Petition & the JU Request for Clarification

The June 2018 Order which initiated this proceeding directed parties to address cybersecurity issues with respect to DERS as well as retail market participants.[25] In the Mission Data Declaratory Ruling Petition, Mission:data asserts, inter alia, that the DER Oversight Order expressly prohibits a distribution utility from requiring cybersecurity requirements of DERS accessing customer data through GBC. Mission:data focuses on Section 2C.A. of the UBP-DERS which states, in part, that "[t]his Section establishes practices for release and protection of customer information by distribution utilities or DSPs to DER suppliers using EDI," and that "[t]his section does not impose any obligations on DER suppliers that do not request or receive data using EDI." Mission:data thus argues that the distribution utilities are prohibited from requiring DERS not using EDI from complying with the data protection requirements of the UBP-DERS or any other data security requirements.

In the JU Request for Clarification, the Joint Utilities ask the Commission to clarify that the DER Oversight Order did not limit the application of data protection requirements to DERS using EDI. The Joint Utilities assert that UBP-DERS provisions

[25] June 2018 Order, p. 3.

regarding the provision and protection of customer data should apply to DERS using any utility platforms for data access, not just EDI.

In response to the present Petition, several parties comment on the applicability of the DSA and the definition of ESEs. The Petition proposes that some level of cybersecurity should be required of all entities seeking access to utility customer data or distribution utility IT systems. This proposal includes DERS.

1. Party Comments

Mission:data asserts that the DER Oversight Order and the UBP-DERS do not require any data protection requirements for DERS who receive customer data from the distribution utility by means other than EDI. Thus, Mission:data claims that the requirement that a DER provider using GBC execute a DSA conflicts with the DER Oversight Order.

Moreover, Mission:data offers that the relief requested by the Joint Utilities in the Petition conflicts with the Commission's Order Adopting Accelerated Energy Efficiency Targets, which directed Staff and the utilities to convene a collaborative to develop terms and conditions for GBC use.[26] Mission:data asserts that applying the DSA to DERS using GBC would render the directive in the EE Order and the resulting GBC Working Group moot. Mission:data suggests allowing the GBC Working Group effort to run its course before the Commission adopts any cybersecurity requirements for GBC users. Finally, Mission:data asserts that the DSA would not satisfy the standard for data access via GBC established in the EE Order that "[t]he terms and conditions

[26] Case 18-M-0084, In the Matter of a Comprehensive Energy Efficiency Initiative, Order Adopting Accelerated Energy Efficiency Targets (issued December 13, 2018) (EE Order).

should make it no more difficult for a DER provider, for whom a customer has provided consent, to access data than it is for the individual customer to access data."[27]

Home Energy Analytics, Advanced Energy Management Alliance, EnergyHub, Arcadia Power, and MACH Energy provided comments in response to the Mission:data Declaratory Ruling Petition on or before December 21, 2018. These comments parallel one another, asserting that the DER Oversight Order specifically exempts DERS that use GBC from cybersecurity requirements and that in order to impose any such requirement on these entities, the Commission must first modify the DER Oversight Order.

Logical Buildings support Mission:data's interpretation of the DER Oversight Order. The Advanced Energy Companies provided comments in support of the Mission:data Declaratory Ruling Petition stating that the application of cybersecurity requirements to DERS that don't use EDI will stifle development of the DER marketplace. The DSA Coalition Comments that the Joint Utilities' request that all ESEs, including DERS, execute a DSA directly contradicts the plain language of the DER Oversight Order. Further, the DSA Coalition asserts that GBC does not pose a risk to utility IT systems or of release of customer information. UtiliSave supports Mission:data's position on the DER Oversight Order and believes that the Joint Utilities' position regarding the DSA conflicts with that Order.

AES Distributed Energy, Inc. (AES) comments that all DERS should be exempt from compliance with cybersecurity requirements because the DER market is mainly comprised of large commercial and/or municipal customers who are more business savvy and aware of data security issues and thus pose less of a threat. Moreover, AES asserts that DERS get a majority of their data

[27] EE Order, p. 44.

directly from the customer, not through direct access to utility systems and thus pose little, to no, risk of security breaches.

Logical Buildings comments that the DSA imposes strict regulations on DERS that would likely stifle the growth of the DER market. Logical Buildings asserts that the proposed restrictions on the use of customer data are an unnecessary burden and that the utility should not control a DER provider's use of customer data.

The Joint Utilities commented in response to the Mission:data Declaratory Ruling Petition that they have a responsibility to protect utility IT systems and customer data regardless of the type of entity receiving data or the platform used to communicate that data. The Joint Utilities assert that requiring the execution of a DSA prior to obtaining customer data is consistent with Commission policy, including the DER Oversight Order. In specifically applying the UBP-DERS to DERS that use EDI, the Joint Utilities continue, the Commission recognized that other data transfer platforms exist, and that requirements for those platforms would be addressed elsewhere.

2. Discussion & Conclusion

In the June 2018 Order, the Commission directed that issues regarding the cybersecurity protections that would be sufficient to protect utility IT systems and customer information should be developed to address DERS as well as retail market participants. The Commission is cognizant of the concerns surrounding applying cybersecurity requirements to DERS and the potential stifling effect that could have on DER markets. However, simply because a market is in a nascent stage, cybersecurity requirements cannot be completely disregarded. All entities, including DERS, need to observe adequate cyber hygiene in order to ensure that utility IT systems and customer data are not compromised. Developing these requirements now while the market is developing is the appropriate approach. Doing so will

help to instill customer confidence in new markets that might otherwise suffer reputational damage in the wake of cybersecurity events. Additionally, failure on behalf of DERS to maintain adequate cyber protections increases the risk of a cybersecurity incident and shifts the costs of those risks to the distribution utilities and its rate payers. By this Order, the Commission strikes the appropriate balance between protecting utility IT systems and customer information and facilitating the transfer of customer consented data.

With respect to the Mission:data Declaratory Ruling Petition, Mission:data is correct that the data security provisions UBP-DERS currently only applies to DERS who utilize EDI to receive customer data. However, in establishing protections regarding EDI, which is the existing mechanism utilized by ESCOs and some DERS today, the Commission did not prohibit the development of cyber protections regarding other data transfer protocols, including GBC.

As the Commission noted in the DER Oversight Order, "EDI on its own may not be sufficient to meet the data needs of DER suppliers as the market develops," and that "[a]dditional methods of sharing data are already being implemented through technologies such as AMI and in other venues including through Green Button Connect and NYSERDA's Utility Energy Registry. Requirements and policies associated with receiving data through these IT systems will be developed in those venues."[28] The Commission, in the DER Oversight Order, signaled that application of data protection requirements, including cybersecurity, would be developed and applied to other DERS who receive customer data from the distribution utility in the future. While those discussions were occurring in various proceedings at the time, the present

[28] DER Oversight Order, p. 28 (citations omitted).

proceeding has consolidated many of the issues surrounding cybersecurity related to Commission initiatives.

The comments of Mission:data and others that the Commission cannot now develop cybersecurity protections applicable to DERS in this proceeding are mistaken. The Commission is free to modify and/or supplement existing rules as policies develop and circumstances change. Given that the DER Oversight Order specifically indicated that data protection requirements for DERS that do not use EDI would be developed subsequently, it can come as no surprise that the Commission is establishing those requirements now.

The Mission:data Declaratory Ruling Petition is denied. While the DER Oversight Order did not impose specific cybersecurity requirements on DERS not using EDI, such DERS will be required to comply with the cybersecurity requirements directed in this Order. Additionally, while the Commission establishes appropriate protections surrounding the sharing of customer data between the utility and DERS, the Commission may consider incorporating the requirements into the UBP-DERS in the future.

With respect to the assertion that the Commission should wait until the GBC Working Group process concludes before adopting cybersecurity requirements for GBC users, the Commission notes that discussions in that proceeding appear to have been hindered by the ongoing disputes surrounding the DSA.[29] Cybersecurity requirements are expected to be an aspect of GBC terms and conditions. Establishing the minimum cybersecurity protections to be applied to all entities seeking access to customer data or connection to the utility IT systems will allow the development of

[29] Case 18-M-0084, supra, Request for an Extension (filed April 26, 2019).

GBC terms and conditions to continue and settle a potentially contentious issue encumbering the working group process.

Turning to the JU Request for Clarification, that request is also denied consistent with the discussion above. As the DER Oversight Order explained, the requirements of UBP-DERS section 2C currently applies only to DERS that utilize EDI to obtain customer data. Nevertheless, cybersecurity and privacy requirements for all DERS are being addressed in this proceeding.

Finally, the Commission is cognizant of the fact that not all DER providers are currently subject to the UBP-DERS. This Order does not expand upon the types of DER providers currently register with the Department of Publish Service (Department) pursuant to the UBP-DERS. However, this issue shall be addressed in the working group process to establish terms and conditions for GBC access.

Applicability of Cyber Requirements to Third Party Representatives

As stated above, the Petition proposes that some level of cybersecurity should be required of all entities seeking access to utility customer data or the utility IT systems. The Petition also proposes to require execution of the DSA by third party representatives or contractors with whom an ESE may contract and who may receive customer data.

1. Party Comments

CPA Comments that the DSA inappropriately extends to third parties with whom an ESE may contract with that in one way or another will have access to customer information. CPA objects to any requirement that ESEs be responsible for the behavior of their third party contractors and that those third parties be required to sign the DSA.

Several commenters assert that it would be inappropriate to require third party representatives or contractors of ESEs to

execute the DSA, and by extension, the requirements of the UBP or UBP-DERS. The DSA Coalition proposes that alternatively, each ESE should be responsible for its contractors/vendors and should be free to choose the terms of any DSA between them and their contractors instead of being required to extend the current DSA to those entities.

Hansen Solutions LLC (Hansen) comments that it should be the responsibility of each ESE to ensure that the appropriate cybersecurity standards have been implemented by their third party representatives and that these third parties should not be required to sign the DSA. Instead, Hansen proposes that the DSA should simply require that ESEs have several specific requirements in their data agreements with their third party representatives, including compliance with appropriate standards, requirements to maintain confidentiality, and ensuring an appropriate process is in place to respond to data security incidents. Hansen further comments that EDI providers should not be considered ESEs and instead should be third party representatives exempt for executing the DSA.

Logical Buildings assert that the DSA should not be applied to third party representatives of DERS, or any entity that does not interact with the utilities' IT systems. Logical Buildings comments that release of customer information by DERS to third parties is normally done with customer consent and with a non-disclosure agreement (NDA) between the parties. NEM offers similar comments regarding the application to third party representatives, stating that the term as used in the DSA is too broad and imposes obligations on entities that do not present a risk to the utilities' IT systems where an NDA would be sufficient.

In reply comments, the Joint Utilities assert that "[w]hen a third party gains access to a customer's utility account

data, even without direct interaction with the utility's IT systems, the third party can expose the utility to claims and damages, including reputational harm, from loss of utility account data,"[30] and as such, are requiring any entity seeking access to utility customer data or utility IT systems to execute a DSA. Such entities include, among others, ESCOs, ESEs, Demand Response Providers, EDI providers, GBC participants, State Agencies, and Direct Customers. The Joint Utilities assert that the requirement for a DSA is not based "on the type of entity asking for data but on whether the ESE is connecting to a utility system and/or obtaining confidential customer information."[31] In response to party comments, the Joint Utilities offered a concession on the issue of third party representatives who do not have electronic communication with the utility other than by email. The Joint Utilities propose to eliminate that requirement, leaving it up to the ESE to negotiate the terms of a DSA or something similar with their third party representatives. Nevertheless, the Joint Utilities still propose that the ESE remain liable for the actions of its third party representatives.

2. Discussion & Conclusion

Execution of a DSA by ESEs who electronically exchange data directly with the distribution utility, including EDI providers, is appropriate and necessary. However, also requiring third party representatives of ESEs, who have no direct link to the utility, to execute a DSA would create a burdensome and unnecessary process. This could also lead to a situation whereby numerous "downstream" entities are required to abide by the terms of a DSA that does not adequately address the relationship between the entity and the utility, nor their use of customer data.

[30] Joint Utilities' Reply Comments, p. 18.

[31] Joint Utilities' Reply Comments, p. 19.

It is important to note that, in most instances, the utility may only share customer data with ESEs who have received the customer's consent. ESEs who intend to, in turn, share that customer data with third party representatives need to obtain the proper customer consent to do so. Absent express consent from the customer to share their data with additional third parties, ESEs may only share customer data with a third party when it is necessary for the ESE to provide the service the customer signed up for.

Third party representatives, as the term is defined in the DSA, shall not be required to execute the DSA or Exhibit B thereto. Instead, it is up to the ESE and the third party representative to determine the type of data security that is appropriate for their business relationship. However, any ESE utilizing a third party representative and/or contractor to provide service to customers will be responsible for the actions of their third party representatives. The ESE is responsible for ensuring that the third parties with whom it shares customer data properly safeguard that data.

Applicability to Direct Customers and New York State Entities

The Joint Utilities' Petition asks that cybersecurity protections be required of all entities who connect with utility IT systems in order to obtain customer data, including Direct Customers and New York State Entities (State Entities). The UBP defines a Direct Customer as:

> An entity that purchases and schedules delivery of electricity or natural gas for its own consumption and not for resale. A customer with an aggregated minimum peak connected load of 1 MW to a designated zonal service point qualifies for direct purchase and scheduling of electricity provided the customer complies with NYISO requirements. A customer with annual usage of a minimum of 3,500 dekatherms of natural gas at a single service

> point qualifies for direct purchase and scheduling of natural gas.[32]

State Entities include, inter alia, agencies and authorities such as the New York Power Authority (NYPA) and the Office of General Services (OGS).

1. Party Comments

With respect to Direct Customers, Fluent Energy (Fluent) comments that Direct Customers differ from many of the other entities classified as ESEs because they are end-users. Direct Customers, Fluent avows, do not present a risk of unauthorized disclosure of another market participant's data because they only manage their own data and account number(s). Fluent further proposes that Direct Customer be divided into two groups: those that electronically interact, in whole or in part, with Utility IT systems, including EDI systems and secure web portals, referred to as Interacting Direct Customers (IDCs); and those who do not interact with such IT systems, referred to as Non-Interacting Direct Customers (NIDCs).

Fluent asserts that NIDCs do not pose the same risks as IDCs and other ESEs and thus should be addressed in an alternative manner. Fluent proposes that these NIDCs, who utilize third party contractors to perform all required electronic interactions with utility systems, do not present any risk to utility IT systems and should not be required to execute the DSA.

The Advanced Energy Companies comment that Direct Customers are utility customers and have a right to access their data. Requiring Direct Customers, Advanced Energy Companies continue, to obtain cybersecurity insurance and indemnify utilities against damages creates too high a burden to access your own data.

[32] UBP Section 1.

Turning to State Entities, the New York Power Authority (NYPA) comments that the DSA does not account for the unique statutory and regulatory obligations and responsibilities of State Entities, which limits their ability to comply with certain DSA provisions. To address this issue, NYPA proposes that the Joint Utilities be allowed to enter into modified DSAs with State Entities. Alternatively, NYPA proposes modifications to the DSA, such as removal of any references to the UBP and UBP-DERS, which NYPA is not subject to, and modifications allowing for the retention of data after termination of the DSA so as to meet the requirements of Federal, State, and local laws, tariffs, rules, and regulations.

In reply comments, the Joint Utilities offer that "as long as [State Agencies and Direct Customers] have an electronic connection with the Joint Utilities' IT systems and maintain customer data shared by the Joint Utilities, the entities must meet the DSA requirements."[33] In response to party comments, the Joint Utilities agreed to add language to the DSA clarifying that, "where an ESE exclusively uses a Third Party Representative(s) to communicate electronically with a utility other than by email and the ESE's Third Party Representative executes a DSA with the utility, a DSA is not required of the ESE."[34] The Joint Utilities comment that if a Direct Customer engages only in one-way data transfers without any connection to a utility system, they should not be required to sign the DSA. With respect to State Entities, the Joint Utilities agree to amend the DSA for governmental entities accordingly, including reflecting that such entities utilize the cybersecurity protections required by the New York State Office of Information Technology

[33] Joint Utility Reply Comments, p. 19.

[34] Id.

2. Discussion & Conclusion

Direct Customers and State Entities present unique circumstances with respect to the DSA. Due to the fact that Direct Customers are accessing their own data, they do not present the same data security concerns of other ESEs who maintain other customer's confidential data. However, in most instances, they do present similar security risks to distribution utility IT systems. The Commission adopts the modification presented by the Joint Utilities in their reply comments which forgoes the need to sign a DSA in the event a Direct Customer does not communicate electronically with utility IT systems, but instead uses a third party who has executed a DSA for such communication.

Alternatively, a Direct Customer who directly exchanges data electronically with the utility, through EDI for example, presents a similar IT system security risk as an ESCO and should be required to execute a DSA. Although these entities are end use customers, they interface with the utility differently than a typical customer, and thus present a different risk to the Joint Utilities' IT systems.

With respect to State Entities, as NYPA points out, some of the DSA provisions may conflict with Federal, State, and local laws, tariffs, rules, and regulations. The unique circumstances presented by State Entitles foreclose making a generic determination as to the applicability of cybersecurity protections. The Joint Utilities are directed to work with each applicable State Entity to develop a customized DSA to address each State Entities' unique situation.

Similar to the process recently adopted for the New York State Energy Research and Development Authority (NYSERDA) in the Commission's Order Regarding New York State Energy Research and Development Authority Data Access and Legacy Reporting, the Joint Utilities and each State Entity shall jointly file a revised DSA

within 60 days of the effective date of this Order.[35] Alternatively, if the Joint Utilities and any State Entity are unable to agree on the terms of a DSA, each shall file a proposed DSA under cover indicating the areas of disagreement for Commission consideration. Finally, to the extent practicable, the State Entity DSA should be consistent among the various State Entities for which a DSA is necessary.

Risk-Based Approach

1. Party Comments

Several commenters suggest that, instead of developing a DSA that should be applied to all entities that seek access to customer data or utility IT systems, cybersecurity measures should be tailored to each individual ESE based on the risk they pose. The DSA Coalition comments that variations in the size of an ESE, the type of data it handles, as well as other factors necessitate custom solutions tailored to the needs of the ESE. The DSA Coalition asserts that the DSA improperly allows the utilities to interject themselves into ESE business decisions and prevents ESE from developing tailored, risk-based security programs. DSA Coalition also comments that all ESEs be treated the same and be held to the same cybersecurity standards.

The Advanced Energy Companies comment that the DSA inappropriately uses broad strokes to address various differing types of data transactions, all of which have different risk levels. The Advanced Energy Companies propose that the Commission consider the varying levels of risk associated with different types of data and different types of data exchange in determining

[35] Case 14-M-0094, Proceeding on Motion of the Commission to Consider a Clean Energy Fund, Order Regarding New York State Energy Research and Development Authority Data Access and Legacy Reporting (issued January 17, 2019).

the level of cybersecurity requirements for certain entities. For example, the Advanced Energy Companies assert that one-way transfers of non-operational data, such as the utility providing customer historical usage data through GBC, poses very little risk to the utility compared to other data transfers that might include two-way data exchanges of operational data or personally identifiable information (PII). Thus, the Advanced Energy Companies state that the requirements of the DSA impose unreasonable and artificial costs on third parties who may pose little, to no, risk to the utilities.

The Advanced Energy Companies further assert that many third parties who receive customer data from the utility have no business relationship with that utility and that the DSA is attempting to treat those third parties as though they are vendors with such a business relationship. NEM likewise asserts that it is inappropriate to equate ESEs to vendors because a vendor is rendering a product or service to the utility and has the option to reject the DSA, but ESEs must rely on the utilities' distribution system or IT systems in order to serve their customers. Mission:data also opposes similar treatment of ESE and vendors.

Mission:data comments that cybersecurity risks should be broken out into two distinct categories; system risk and data misuse risk. Mission:data offers that utilities should be solely responsible for system risk, that the risk posed by having ESEs access their IT systems. Mission:data asserts that a breach of a utilities' IT systems, such as a GBC platform, is the sole responsibility of the utility and that if a successful cyber attach occurs, it must be that the utility did not adequately protect its system. According to Mission:data, ESEs should have no responsibility when it comes to protecting utility IT systems from a cybersecurity incident. Conversely, Mission:data proposes

that the Commission expressly waive the utilities' responsibilities regarding data misuse risk, which is the risk that an ESE will abuse a customer's privacy rights using information received from the utility. Finally, Mission:data asserts that GBC does not pose the same system risk as EDI because GBC requires utility-processed consent prior to providing customer data to the ESE.

In reply comments, the Joint Utilities assert separately developing a DSA for each entity based on their specific risk is unworkable and unnecessary. Such a process, the Joint Utilities continue, would create a significant burden on ESE and the Joint Utilities because ESEs would need to constantly update their information as, for example, customer counts change and potentially require repeated reassessments of risk. Additionally, the Joint Utilities claim that such a process would be ripe for discrimination claims.

2. Discussion & Conclusion

Addressing first the comments asserting that ESE should not be treated the same as utility vendors, the Commission agrees. However, the Petition is clear that though the Joint Utilities would like the ESEs to have more protections, they are not being treated like distribution utility vendors. Vendor requirements are established via contractual terms and agreements that are based upon the vendor having a high level of access directly into the utility IT systems, possibly behind firewalls. ESEs will not have this higher level of access and have a direct relationship with the customer, not implementing a program or service for the utility. The necessary cybersecurity and privacy requirements for ESEs will not be established based upon the risk associated with vendor access but on the risk associated with the ESEs restricted access to utility IT systems and/or data.

Turning next to the suggestions that a fully risk-based approach be implemented, the Commission concurs that there is a difference in the risk of compromise to the utility IT systems and the risk associated with a breach once the customer consented data is in the possession of the third party, and that the requirements should reflect that. As such, discussions regarding appropriate controls that address the risk to IT systems will be classified as cybersecurity protections and risk of release of customer data will be classified as privacy protections.

Globally implemented frameworks and cybersecurity experts recognize the difference in risk to IT systems and risk to data and use controls from a cybersecurity framework to address risk to IT systems and from a privacy framework to address risk to data.[36] A control implemented to address IT system security will not necessarily protect customer privacy in the event of a breach and vice versa. 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. In organizing the risks into these two categories, the Commission, in this Order, establishes the necessary requirements for any entity seeking access to customer data through the utility IT systems so as to mitigate both the system risk and the data misuse risk. In order to implement a more detailed risk analysis approach for further consideration, with the potential of performing a fully risk-based assessment for each

[36] National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Center for Internet Security (CIS), Department of Energy (DOE), and many more.

ESE, applicable frameworks for cybersecurity and data privacy need to be identified and analyzed.[37]

Thus, a fully risk-based approach will not be adopted at this time. However, the Commission clarifies that only entities that electronically receive or exchange customer information from a direct connection with the utilities' IT systems, except by email, will need to adopt the cybersecurity requirements established in this Order. ESEs that have access to customer information but do not have a direct connection into the utility IT systems will need to implement the appropriate privacy protections to ensure customer data is protected from improper disclosure or misuse. Not requiring cybersecurity protections for ESEs who have access to customer data does not mean that the ESEs should not have adequate cybersecurity protections, only that the attestation of those protections will not be a requirement to do so. The Commission strongly urges all ESEs to implement and maintain adequate cybersecurity protections regardless of whether the ESE is connecting to the utility IT systems.

For these reasons, the Commission, at this time, will also not be individually developing the cybersecurity protections and/or a DSA for each ESE operating in the State. Instead, the approach taken here to develop the minimum level of protections for any entity electronically exchanging customer data with a distribution utility is more appropriate at this time.

---

[37] In its November 1, 2016, Supplementary Distribution System Implementation Plan (SDSIP) filing, the Joint Utilities reported development, and individual utility level adoption, of a Cyber Security and Privacy Framework that focuses on people, processes, and technology to maintain data security. The Framework was reported to consist of six main parts: Information Security Management, Risk Methodology, Security Design Principles, Cybersecurity Capabilities to Manage Risk, Privacy Management, and Vendor Awareness.

Discontinuance of ESEs Who Do Not Execute a DSA and the JU Declaratory Ruling Petition

The Petition asks the Commission to affirm the Joint Utilities' authority to require ESEs to execute a DSA and to prohibit or disconnect ESEs from accessing utility IT systems and/or customer data if they have not executed a DSA. The JU Declaratory Ruling Petition makes a similar request specifically with respect to the authority of a distribution utility to discontinue an ESCO's participation in the utility's retail access program pursuant to Section 2.F. of the UBP if the ESCO fails to meet minimum cybersecurity standards, including execution of a DSA.

1. Party Comments

Agway asserts that UBP Section 2.F.2. does not provide the utilities with the authority to unilaterally discontinue an ESCO's access to utility IT systems without intervention by the Commission. According to Agway, the discontinuance provisions of the UBP require that the Commission make a case specific finding that there is good cause to discontinue an ESCO's access.

Moreover, Agway avows that an ESCO's failure to execute the DSA does not constitute an "act that is likely to cause, or has caused, a significant risk or condition that compromises the safety, system security, or operational reliability of the distribution utility's system" under UBP Section 2.F.1.a. An ESCO may choose not to sign the DSA, Agway continues, but may nevertheless have robust cybersecurity protections such that the ESCO does not present a risk to system security.

The DSA Coalition comments that a distribution utility must demonstrate an actual risk before seeking Commission permission to terminate an ESCO's connection to utility IT systems. The DSA Coalition asserts that the utilities should not be allowed to unilaterally determine that an ESCO is out of

compliance with the requirements of the DSA and seek to discontinue the ESE from access to utility IT systems and customer data. Instead, the DSA Coalition comments that the discontinuance process requires involvement by the Commission and requires the utility to demonstrate that an ESCO's failure to execute the DSA represents an actual risk to the utilities' IT systems before the ESCO's access to those IT systems can be terminated. Finally, the DSA Coalition comments that the Joint Utilities have failed to demonstrate that failure to execute a DSA presents a risk to utility IT systems.

Mission:data comments that there is no analogous discontinuance provision found in the UBP-DERS and that the Joint Utilities cannot avail themselves of the discontinuance provisions in the UBP in order to terminate a DERS access to distribution utility IT systems. Moreover, Mission:data asserts that it would be inappropriate for the utility to be the entity who decides when a violation of the DSA has occurred because doing so would give the utility the right of unilateral termination. Mission:data proposes that more due process is needed in order to terminate a DER provider.

NEM comments that the Joint Utilities incorrectly interpret the discontinuance provisions of the UBP by assuming that an "ESCO's decision not to execute the DSA would constitute incontrovertible evidence of a 'significant risk' to the utility system without any inquiry into whether the ESCO's operations or conduct in fact posed such a risk."[38] NEM asserts that the Joint Utilities do not have the authority to exert unrestricted discretion regarding whether an ESCO should be discontinued, and that the discontinuance process requires Commission intervention.

[38] NEM Comments, pp. 18–19 (citation omitted).

NEM further Comments that UBP Section 8 establishes the dispute resolution process available to resolve disputes between utilities and ESCOs. NEM asserts that this process is necessary to provide an objective assessment of an ESCO's decision not to sign the DSA and the risk to utility IT systems that failing to do so may cause.

RESA comments that the Joint Utilities seek delegation of authority that should remain with the Commission. RESA notes that neither the UBP nor the Joint Utilities' tariffs afford the Joint Utilities with the ability to discontinue and ESCO without Commission intervention. UBP Sections 2.F.4. and 2.F.5., RESA continues, specifically provide for Commission involvement in the discontinuance process. Additionally, RESA asserts that UBP Section 2.F.1. requires a case-specific finding under that there is cause to discontinue an ESCO. RESA contends that it would be inappropriate to provide the Joint Utilities unchecked authority to interpret and enforce Commission rules and policies due to the fact that ESEs and utilities are competitors. Doing so, RESA offers, would constitute an amendment to the UBP without complying with SAPA.

Similar to the arguments of the DSA Coalition and NEM, RESA asserts that the failure to execute a DSA does not by itself create a risk to utility IT systems. RESA comments that "[t]he DSA itself does not increase or decrease any perceived risk to a utility's system, nor does executing the agreement mitigate any such perceived risk."[39]

In reply comments, the Joint Utilities contest comments which assert that the Joint Utilities will terminate access to utility IT systems and customer data without cause or justification are incorrect. The Joint Utilities comment that the

[39] RESA Comments, p. 10.

discontinuance process under the UBP requires involvement by Staff, and that the Joint Utilities are committed to meeting the requirements of the UBP, including the due process afforded prior to discontinuance. However, the Joint Utilities identify that, in an "emergent situation . . . a utility appropriately has the right to cease providing a system connection or providing customer data to any entity that may be under attack or under the threat of an attack."[40] Such an action, the Joint Utilities continue, would be temporary until the situation is addressed.

2. Discussion & Conclusion

The JU Declaratory Ruling Petition focuses on the interpretation of Section 2.F. of the UBP, which deals with the discontinuance of the ESCO's or Direct Customer's participation in the distribution utilities' retail access program. Pursuant to UBP Section 2.F.1.a., a distribution utility may discontinue an ESCO or Direct Customer for "[f]ailure to act that is likely to cause, or has caused, a significant risk or condition that compromises the safety, system security, or operational reliability of the distribution utility's system, and the ESCO or Direct Customer failed to eliminate immediately the risk or condition upon verified receipt of a non-EDI notice."

UBP Section 2.F. further details the process by which a distribution utility initiates a discontinuance, including sending a discontinuance notice to the ESCO or Direct Customer and the "Department."[41] Commenters who assert that the discontinuance process requires participation by the Commission confuse the distinction between the Department and the Commission. The UBP refers to the Commission in numerous places separate and distinct

[40] Joint Utilities Reply Comments, p. 15.

[41] The UBP uses the term "Department" to refer to the Department of Public Service; see UBP Section 2.A.

from the Department, which refers to Staff.[42] An example of this distinction can be found in Section 2.B. of the UBP which deals with the application requirements for an ESCO seeking eligibility to sell natural gas and/or electricity in New York State. An ESCO seeking eligibility is not required to petition the Commission, but instead files an application package with Staff. Similarly, the discontinuance provisions of the UBP require participation by Staff, but not necessarily the Commission.

Nevertheless, and as NEM correctly points out, the UBP also provides for dispute resolution processes, which after an initial decision from Staff, provides parties to the dispute an opportunity to appeal the decision to the Commission.[43] Nothing in this Order shall be construed as to deny any entity the due process afforded under the UBP. Furthermore, this Order does not modify the provisions discontinuance nor the dispute resolution provisions of the UBP.

Returning to the discontinuance process, commenters are correct that the distribution utility, in relying on UBP Section 2.F.1.a., would need to demonstrate that an ESCOs action or inaction "is likely to cause, or has caused, a significant risk or condition that compromises the safety, system security, or operational reliability of the distribution utility's system. . ." The process would require Staff to evaluate the reason for discontinuance, review the sample discontinuance notice to be sent to customers, and generally oversee the process and associated timelines.

Regarding comments which assert that the failure to execute a DSA does not necessarily constitute a significant risk

---

[42] See, UBP Section 2.D.6 which refers to "the Commission or Department," emphasizing that the two are not synonymous.

[43] UBP Section 8.B.1.

that compromises system security, the Commission supports such an assertion. Failure to execute a DSA by itself does not establish that an ESCO "is likely to cause, or has caused, a significant risk or condition that compromises the safety, system security, or operational reliability of the distribution utility's system. . ."[44] As Commenters point out, there may be numerous reasons why an ESCO might not sign a DSA, but still have robust cybersecurity protections. A distribution utility seeking to discontinue an ESCO or Direct Customer would need to assert that, in addition to not executing a DSA, the ESCO or Direct Customer's action or inaction presents a specified risk to the utility's IT systems.

Additionally, with respect to DERS, Mission:data is correct that, while the UBP provides for discontinuance of an ESCO or Direct Customer, there is no analogous discontinuance provision found in the UBP-DERS. The Joint Utilities cannot rely on the discontinuance process in the UBP to discontinue a DER provider. Nevertheless, by this Order, the Commission establishes the minimum level of cybersecurity and privacy protections that all ESEs must maintain. Thus, utilization of a discontinuance process is unnecessary in this instance. ESEs that fail to maintain these minimum levels of protections shall not have access to customer data, and/or the Utility IT systems. Disputes regarding whether an entity has complied with these requirements should be brought to Department Staff.

Customer Access vs. ESE Access to Data

1. Party Comments

The Advanced Energy Companies assert that the risk associated with a one-way data transfer of customer data to an ESE is no different than a transfer of the same data from the utility

[44] UBP Section 2.F.1.a.

to the customer. Customers have a right to access their own data without execution of a DSA, the Advanced Energy Companies continue, and also have a right to contract with third parties for energy services. The Advanced Energy Companies assert that the DSA would create significant differences in cost and method between how a customer accesses their own data and how an ESE accesses that customer's data. Thus, the Advanced Energy Companies propose that ESE be required to do no more to access customer data then the customer would themselves to access their own data. Mission:data asserts that the DSA would inappropriately make it more difficult for a DERS to access a customer's data than it would be for the customer themselves to access their data.

In Reply Comments, the Joint Utilities offer that the customer-facing IT systems and ESE-facing IT systems are not analogous and were developed and designed differently. The joint Utilities comments that the customer-facing IT systems require multi-factor authentication and are designed for single customer interactions with the system where the customer can only access their individual information. The cybersecurity design for the customer-facing IT systems, the Joint Utilities continue, takes these limitations into account.

The Joint Utilities distinguish their ESE-facing IT systems, stating that they are designed for a greater number of transactions for a greater number of customers and that data is provided in bulk. The Joint Utilities comment that, while these IT systems were designed to reduce risk, they also rely on the reasonable assumption that the recipient of the data also maintains adequate cyber security protections. Moreover, the joint Utilities assert that interactions with ESEs are inherently a two-way interaction whereby ESEs identifies the customers for whom data is sought, followed by transfer of that data by the utility.

2. Discussion & Conclusion

There is an inherent difference between a single customer viewing their own data through a distribution utility's customer-facing system, and an ESE obtaining utility housed customer data from a direct connection to the distribution utility's IT systems. While recognizing that there may be a different level of risk associated with the way the transaction is being initiated, authorized, and transmitted, lowering ESE requirements to the same level of a consumer does not fully assess the risk or provide the appropriate cybersecurity and privacy protections.

The Joint Utilities comments do not differentiate the risk associated with different data connection mechanisms (API, EDI, etc.), data sets being shared, recognize that the ESE has obtained customer consent, is acting as the customer representative/agent, nor the no more onerous requirement established in the EE Order for ESEs using GBC. Additionally, the Joint Utilities designing IT systems and implementing protections around the assumption of adequate cyber protections by the data recipient does not correctly assign risk. The Joint Utilities must continually evaluate cyber exposure, protections, and associated risks and implement the appropriate controls to address that risk.

The Commission's EE Order directed development of terms and conditions for use of GBC that "must, among other things, include reasonable requirements for third parties to ensure the privacy and integrity of customers' data in relation to the risk associated with any breech of customer data."[45] Thus, the Commission found that the third party should be able to access the

[45] EE Order, p. 44

data just as easily as the customer itself when they have obtained the consent to do so.

Pertaining to GBC, the technical standards of the platform, connection process, and necessary protections are still being identified and assessed. As such, the cybersecurity and privacy protections will continue to be developed and will be included in the terms and conditions for GBC participation. When properly implemented, GBC provides for an authenticated request for customer data, with the customer's consent, through a platform outside the distribution utility's IT systems. Issues of quantity aside, this will more closely resemble a customer's request for data. While all ESEs are currently required to sign the DSA in order to access customer data and/or the utility IT systems, refinement of these requirements will be ongoing and will change as technology and policy considerations change.

DSA Term Definition

1. Confidential Utility Information

The DSA proposed in the Petition defines "Confidential Utility Information" as:

> information that Utility is: (A) required by the UBP at Section 4: Customer information(C)(2), (3) or UBP DERS at Section 2C: Customer Data, to provide to ESCO, Direct Customer or DERS or (B) any other information provided to ESE by Utility and marked confidential by the Utility at the time of disclosure, but excludes (i) information which is or becomes generally available to the public other than as a result of a disclosure by Receiving Party or its Representatives; (ii) information which was already known to Receiving Party on a non-confidential basis prior to being furnished to Receiving Party by Disclosing Party; (iii) information which becomes available to Receiving Party on a non-confidential basis from a source other than Disclosing Party or a representative of Disclosing Party if such source was not subject to any prohibition against transmitting the information to Receiving Party and was not bound by a

> confidentiality agreement with Disclosing Party; (iv) information which was independently developed by the Receiving Party or its Representatives without reference to, or consideration of, the Confidential Information; or (v) information provided by the customer with customer consent where the customer expressly agrees that the information is public.[46]

a. Party Comments

The DSA Coalition asserts that the definition of Confidential Utility Information does not account for the varied types of data and does not address that different data carries different levels of sensitivity and risk of harm. NEM comments that the DSA places inappropriate restrictions on what is customer, not utility data. NEM asserts that the Joint Utilities have market power in data and that the DSA should be constructed to mitigate that market power in favor of customer choice.

RESA comments that the definition of Confidential Utility Information would inappropriately categorize all data provided by the utility as confidential without regard as to whether or not the data is actually confidential. RESA proposes that a risk-based classification scheme of data be implemented.

CPA opposes the language "any other information provided to ESE by Utility and marked confidential by the Utility at the time of disclosure," commenting that this creates too broad a category of information for which protection is required. CPA comments the protection should be limited to only what is necessary, and this language expands the data protection requirement to information that is potentially not related to confidential customer data and does not relate to the UBP or UBP-DERS.

[46] Petition Attachment 1, p. 2.

b. Discussion & Conclusion

The proposed definition of Confidential Utility Information appropriately extends protection to all customer data transferred by the distribution utility to an ESE. The Joint Utilities are charged with maintaining customer data and based upon the sensitivity of the specific data points, keeping it confidential. ESEs who, in turn, receive customer data from the utility must only use the data for the purposes the customer consented to. The comments of NEM, RESA, and the DSA Coalition do not recognize this requirement.

Regarding CPA's comment about protecting data labeled as confidential by the distribution utility, CPA has not identified any basis to modify this requirement. There is a possibility that an ESE may seek confidential customer information that is not specifically required by the UBP and UBP-DERS but that the ESE has received customer consent for. In this instance, the distribution utility should mark that information as confidential when it is transmitted so as to fall under the data protection requirements of the DSA.

Finally, while the Commission agrees with the scope of this definition, the term "Confidential Utility Information" does not adequately represent the data itself. This term advances the idea that this is utility information when that is not the case. Instead, this is customer information that is held by the utility. For these reasons, the term "Confidential Utility Information" shall be replaced with the term "Confidential Customer Utility Information." This will better reflect that this is the customer's utility data, not data "owned" by the utility.

2. Data Protection Requirements

The DSA proposed in the Petition defines "Data Protection Requirements" as:

> (A) all national, state, and local laws, regulations, or other government standards relating to the protection of information that identifies or can be used to identify an individual that apply with respect to ESE or its Representative's Processing of Confidential Utility Information; (B) industry best practices or frameworks to secure information, computer systems, network, and devices using a defense-in-depth approach, such as and including, but not limited to, NIST SP 800-53, ISO 27001 / 27002, COBIT, CIS Security Benchmarks, Top 20 Critical Controls as best industry practices and frameworks may evolve over time; and (C) the Commission rules, regulations, and guidelines relating to confidential data, including the Commission-approved UBP and UBP DERS.[47]

a. Party Comments

Blueprint Power Technologies, Inc (Blueprint) comments that referring to such a broad range of requirements creates a likelihood that there will be inconsistencies across the grid. It would be difficult, Blueprint continues, to meet all the cited requirements and provide evidence of the same. Blueprint suggests that there should be clear, well-defined criteria for meeting minimum data security standards. Blueprint suggests establishing NIST SP 800-171 as the proper standard.

CPA comments that the cybersecurity requirements must be knowable, and the definition of Data Protection Requirements is too vague to impose an obligation on ESEs with consequences for failing to meet that obligation. The DSA Coalition asserts that the Data Protection Requirements are ambiguous and that failure to comply with any of these vague standards improperly creates an automatic breach of the DSA. RESA comments this definition lacks specificity as to what the actual requirements are and that ESCOs should not be asked to comply with unknown and undefined requirements.

[47] Petition Attachment 1, p. 2.

In reply comments, the Joint Utilities offer that this DSA by its design is intended to provide ESEs with the flexibility to implement the cybersecurity protections that are appropriate for them. In order to clarify any uncertainties regarding the definition of Data Protection Requirements, the Joint Utilities propose to add the following language to the end of that definition: "The means of data protection chosen by each ESE will be determined by the ESE, which is limited only by the requirement that it remain in compliance with the [Self Attestation]."[48]

b. Discussion & Conclusion

The Commission declines to adopt a specific framework or standard for determination of appropriate controls for data access at this time. 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 ESEs to observe the cybersecurity standards that are most appropriate for their businesses. The bare minimum standards that must be followed are found in the Self Attestation discussed below. Otherwise, ESEs should adopt data protection requirements that go beyond those in the Self Attestation as appropriate. The Commission may consider adoption of a more prescriptive standard at a future date. Finally, the Joint Utilities proposed addition is a helpful clarification and shall be incorporated into the DSA.

[48] Joint Utility Reply Comments, p. 21.

Protection of IT Systems – Cybersecurity Requirements

1. The Self Attestation Form

Prior to the business-to-business process, the Joint Utilities were utilizing their individual VRA forms to evaluate the security risks posed by ESEs. During the business-to-business process however, stakeholders and Staff urged the Joint Utilities to create uniformity between the various VRAs so that an ESE that undergoes an assessment in one distribution utility territory, would satisfy the assessment requirement in other territories and would not be subject to multiple lengthy VRAs. In working toward uniformity, the Joint Utilities further simplified the process by replacing the various VRAs with a Self Attestation form that would be the same for every distribution utility.

The Self Attestation presents a 16-point checklist of minimum cybersecurity protections that each ESE would be required to observe and would have to attest that the protections are in place. Among those 16 cybersecurity protections are implementation of an Information Security Policy, implementation of an Incident Response Procedure, multi-factor authentication, antivirus software, encryption of confidential data in transit and at rest, security awareness training, and employee background screening.

a. Party Comments

CPA comments that the requirements of the Self Attestation are reasonable and the many entities, including CPA, should already meet these standards. NYPA comments that it already implements cyber protections set forth in the Self Attestation. Hansen recommends that the Commission adopt the requirements in the Self Attestation as the appropriate cybersecurity protections that should be observed by all market participants.

The DSA Coalition opposes the protections included in the Self Attestation because they assert that these protections are robust and detailed and have not been established to be appropriate. More Specifically, the DSA Coalition opposes the requirement to encrypt confidential information in transit, asserting that such a requirement is challenging, costly, and impedes business communication. The DSA Coalition also opposes the requirement in the DSA and Self Attestation that limits the location of stored data to the United States and Canada.

Logical Buildings similarly oppose the requirement to encrypt data in transit as overly burdensome and disruptive to normal business practices. NEM opposes the "extensive data security regime"[49] set forth in the Self Attestation.

b. Discussion & Conclusion

The Self Attestation, which is Exhibit A to the DSA, provides a list of foundational cyber hygiene practices and protections. All entities that interface with utility IT systems and maintain customer data should observe these basic principles. The Commission rejects the comments of NEM, Logical Buildings, and the DSA Coalition which state that the Self Attestation creates extensive, burdensome, or robust requirements. The Commission adopts the protections required in the Self Attestation with the exception of one modification.

With respect to the requirement to store data within the United States or Canada, the Commission finds this to be a reasonable requirement. Even if an entity is using a cloud-based service there is the ability to choose the location for data storage. Currently, there is no certification or authorizing board that could provide validation of adequate cybersecurity and privacy protections for alternative locations.

[49] NEM Comments, p. 17.

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.[50] 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.

2. Audit Requirements

In the Petition, the Joint Utilities seek authority to audit ESE's compliance with the DSA, including all applicable data protection requirements. The audit requirement would be avoided if the ESE provides an independent third-party audit of ESE's compliance.

a. Party Comments

Blueprint comments that focus should be placed on risk management and not on an audit by the utility. NEM expresses concern with allowing the utility, who they characterize as a business partner and a direct competitor to access the confidential and proprietary IT systems of ESCOs. Moreover, NEM

[50] Joint Utilities Petition, p. 12.

comments that the process to be utilized in the audit remains uncertain.

RESA objects to any utility audit requirement as inappropriately granting the utility direct oversight responsibility over ESCOs. RESA asserts that, through the broad way audits are described in the DSA, utilities will be able to gain an unfair advantage through insight into the confidential internal procedures of ESCOs. RESA comments that the need for audits should be replaced with robust requirements that ESCOs certify or attest to compliance with cybersecurity protections. If audits are required, RESA proposes that they be conducted by an independent third-party auditor.

b. Discussion & Conclusion

An audit provision should be included to ensure ESEs have implemented the appropriate cybersecurity and privacy protections. However, the audit should be done by an agreed upon third party and paid for by the utility. It is not the utilities business model to audit ESE cybersecurity and privacy programs or to determine compliance. Moreover, it would be inappropriate to require ESEs to submit to audits by the utility for several reasons. First, doing so would essentially amount to utility oversight over ESEs. Second, in some cases, the utility may be a business partner or competitor of an ESE and would be able to access confidential and/or proprietary information regarding the ESE's business and IT systems. Finally, it is possible that an independent third party auditor who specializes in this type of work would be able to conduct these audits more efficiently than the various distribution utilities. For these reasons, the distribution utilities should not be the entities conducting these audits, which are intended to ensure that ESEs are complying with the necessary cybersecurity and data privacy requirements.

A third party auditor shall be selected by the utility through a competitive solicitation. The auditor will audit ESE's compliance with the terms of the DSA and SA and provide those results to the ESE and the utility. The report provided to the utility should not disclose confidential information of the ESE but should instead simply provide an assessment as to the ESE's compliance with the terms of the DSA and SA. Any disputes arising out of a "failed" audit should utilize the dispute resolution processes in the UBP or be brought to Department of Public Service's Office of Consumer Services Staff through the filing of a complaint, as appropriate. Additionally, the alternatives provided for in the DSA for independent audits obtained by the ESE shall remain an option for ESEs.

Protection of Data – Privacy Protections

1. Indemnification

The Petition proposes to require all ESEs to indemnify the Joint Utilities for all damages caused by an ESE's violation of the terms of the DSA. The indemnification provision in the present DSA substantially mirrors the same provision in the CCA DSA approved by the Commission for use in CCA programs.[51]

a. Party Comments

CPA comments that the damage caused by a major cyber breach could result in tens or hundreds of millions of dollars in costs, which no ESE could possibly pay. Further, CPA contends that there are numerous ways that non-compliance with the DSA could occur exposing ESEs to immense levels of liability. This, CPA asserts, would cause many ESE to do business elsewhere. RESA

[51] See CCA DSA Order, and Case 14-M-0224, supra, Revised Data Security Agreement (filed November 20, 2017).

comments that there should be a cause and effect relationship to any indemnification clause.

NYPA comments that the unlimited indemnification clause in the DSA would discourage participation in the State's DER markets. Instead, NYPA proposes a focused indemnification clause which is limited to damages resulting directly from a cybersecurity incident caused by a failure to maintain the data protection requirements established in the DSA and is capped at an amount equal to that of the ESE's cybersecurity insurance coverage.

In reply comments, the Joint Utilities assert that the ESEs should be liable for their own actions that may cause a cyber incident or the loss of customer data. The Joint Utilities assert that if an ESE breaches or fails to comply with the DSA and the affected utility suffers harm as a result of that breach or non-compliance, the ESE should be liable for the harm, except in situations where the harm is caused by the negligence, gross negligence, or willful misconduct of the utility.

b. Discussion & Conclusion

The Commission finds the indemnification clause contained in the DSA to be reasonable. With respect to the comments of RESA that there should be a causal relationship between the breach and the harm, the indemnification clause is already drafted in such a way. ESEs are only required to indemnify the distribution utility where they have breached or failed to comply with the DSA, and that breach or failure causes damage.

This language also matches the proposal offered by NYPA to limit damages to those resulting directly from a cybersecurity incident caused by a failure to maintain the data protection requirements established in the DSA. Given that the Commission is declining to adopt a cybersecurity insurance requirement, NYPA's

proposal to limit the damages to an amount equal to that of the ESE's cybersecurity insurance coverage is declined.

Aside from general complaints regarding uncertainty surrounding the level of costs, no party offered any persuasive arguments as to why they should not be responsible for harm cause by their breach of or failure to comply with the terms of the DSA. Failure to hold ESEs responsible for their actions will lead to costs shifts to the distribution utilities and ratepayers, who may or may not participate in one or more of these markets.

2. Cybersecurity Insurance

The Petition proposes that the DSA include a provision requiring all entities who electronically receive or exchange customer data with the utility to procure a $5 million cybersecurity insurance policy. This policy would help to cover the damages arising out of a cybersecurity incident. The June 2018 Order specifically requested stakeholders to evaluate "whether insurance is an efficient and effective vehicle for mitigating any potential financial risks."[52]

a. Party Comments

The DSA Coalition opposes a cybersecurity insurance requirement as without any reasonable basis. Alternatively, the DSA Coalition comments that the amount of insurance should be determined on a case-by-case basis and that a self-insurance option should be recognized. AES requests that maintaining cybersecurity insurance at the parent or corporate level be allowed to satisfy the insurance requirement.

CPA and NYSEIA assert that any level of cybersecurity insurance is unlikely to significantly offset the potential costs associated with a major cyber breach. CPA and NYSEIA propose that this requirement simply acts as a barrier to entry and should be

[52] June 2018 Order, p. 3.

eliminated for DERs, contractors, and third parties. Alternatively, both CPA and NYSEIA comment that if cybersecurity insurance is required, the amount should be scaled to the level of risk associated with each entity, taking into consideration their revenues.

NEM comments that the cybersecurity insurance requirement has not been justified by the Joint Utilities and the cost of such insurance will likely force some ESEs out of the market or prevent market entry in the first place. NEM asserts that the level of cybersecurity insurance should be commensurate with the type of data to be protected, the level of interaction with utility IT systems, the risk associated with those interactions, and cybersecurity protections already in place at the entity. NEM further proposes that there should be flexibility in satisfying this requirement, including allowing for self-insurance and allowing use of letters of credit or other similar security instruments.

Additionally, NEM recommends that, as an alternative to requiring ESEs to obtain cybersecurity insurance, the Joint Utilities should instead become certified by the Department of Homeland Security under the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act[53] The SEFETY Act, NEM continues, can serve as an "important component of cybersecurity risk management in the utility industry that is safeguarding its delivery infrastructure and IT systems from cyber attacks."[54] NEM asserts that the liability protections under the SEFETY Act extend beyond the certified entity itself to downstream entities, limiting the liability of both the utilities and ESEs that interact with the utilities' IT systems.

[53] 6 U.S.C. §§ 441-444; See also www.safetyact.gov.

[54] NEM Comments, 14.

In reply comments, the Joint Utilities assert that cybersecurity insurance is an "unavoidable cost of doing business."[55] In addition to addressing the financial costs of a cyber incident, the Joint Utilities comment that cybersecurity insurance can help prevent such an incident because the ESE may need to implement increased protections in response to an insurance provider's review. Finally, the Joint Utilities support the comments proposing that a parent company be able to provide cybersecurity insurance for their affiliates provided that the affiliate is a named insured on the policy and the policy still provides $5 million of insurance benefit to the affiliate per incident.

b. Discussion & Conclusion

The Joint Utilities have not established that cybersecurity insurance would be an efficient and effective means of mitigating cybersecurity risks and financial costs associated with security breaches. Several commenters oppose this requirement as not connected to any reasonable benchmark for the actual risk posed by the entity, or the actual costs of cyber incidents. Moreover, the insurance requirement would serve to act as little more than a market barrier to entry. The Commission recognizes the need to protect utility IT systems and customer data, but does not see a cybersecurity insurance requirement, which is mainly intended to address damages after an incident occurs, as the appropriate means of doing so. Thus, at this time, the Commission declines to adopt a generic cybersecurity insurance provision but may revisit this issue at a future date.

3. Derivative Data

The Petition proposes to limit an ESEs ability to create derivative data from customer data provided by the distribution

[55] Joint Utilities Reply Comments, p. 13.

utility except as provided for under the DSA or authorized by the UBP or UBP-DERS.

a. Party Comments

CPA comments that this restriction is unreasonable, and that ESEs should be able to develop derivative data from customer information regardless of the fact that it came from the utility. Logical Buildings asserts that the Joint Utilities should not determine what ESEs can do with customer data. Logical Buildings comments that these activities are undertaken with the customer's consent. The DSA Coalition proposes that language is needed to clarify that ESEs are entitled to use this information for all lawful purposes allowed pursuant to the UBP and/or UBP-DERS.

Mission:data comments that this language is inappropriate as it would prohibit any processing function of customer-authorized software programs. Mission:data asserts the ESEs should be able to create derivative energy data when authorized by the customer.

NEM comments that the derivative data language would hinder DER product and service development. NEM asserts that the DSA exceeds the requirements of the UBP with respect to ESCO's use of customer data.

NYSEIA comments that the derivative data prohibition in the DSA is unreasonable because the term derivations is too broadly defined and doesn't account for data uses undertaken with the consent of the customer, regardless of such uses being allowed under the DSA or authorized by the UBP.

In reply comments, the Joint Utilities assert that restricting use of customer data to those instances specifically permitted by the DSA, UBP, or UBP-DERS is appropriate. The Joint Utilities agree that when a customer gives express consent for data uses, the data may be used for that authorized purpose, except as restricted by law or regulation.

b. Discussion & Conclusion

As a general matter, ESEs receive consent to obtain customer data in order to provide products or services. Any use of the customer's data, including creation of derivative data, requires the ESE to notify the customer of the purpose and obtain consent to do so. Notification, choice, and consent are privacy principles essential for the appropriate management and protection of the customers data. It is not up to the utility to decide what the customers data should be used for nor police these actions. The use of the customer data once it's out of the utility system should instead be decided between the ESE and the customer.

Parties which comment ESEs should be able to use data consistent with the consent provided by the customer are correct. To avoid any confusion, language should be added to DSA section 14.a. to read: "ESE shall not create or maintain data which are derivative of Confidential Customer Utility Information except for the purpose of performing its obligations under this Agreement, ~~or~~ as authorized by the UBP or UBP DERS, or as expressly authorized by the customer, unless that use violates Federal, State, and local laws, tariffs, rules, and regulations."

4. Termination of the DSA & Return/Destruction of Information

The provisions in the DSA dealing with termination of the agreement and return/destruction of information require that ESEs return or destroy Confidential Customer Utility Information either upon a distribution utility's written demand, or upon termination of the agreement by the distribution utility. These provisions provide for retention information required to be maintained pursuant to applicable federal, state and local laws, rules, regulations, and orders, or for legitimate business or legal needs.

a. Party Comments

The DSA Coalition comments that decisions regarding access to Confidential Customer Utility Information should be subject to the requirements of the UBP or UBP-DERS, as applicable. RESA comments that the termination language should require the utility to specifically identify and describe the alleged breach of the DSA. Additionally, RESA asserts that there should be some form of recourse to challenge a utility's determination that a material breach of the DSA had occurred.

Logical Buildings comments that, because entities received customer data from the utility with the customer's consent, they should be allowed to retain that data until the customer withdraws that consent or the authorization expires. Logical Buildings asserts that the utility should not dictate what they can do with customer information.

b. Discussion & Conclusion

The provisions dealing with the return/destruction of information requires ESEs to destroy or return Confidential Customer Utility Information upon written demand of the utility or upon revocation of customer consent. This provision further qualifies when a distribution utility may make a written demand to destroy or return Confidential Customer Utility Information; which may be done when the ESE has been decertified under the UBP or UBP-DERS, in the event of a data security incident where the utility has a reasonable belief of potential ongoing harm, or when Confidential Customer Utility Information has been held for a period in excess of its retention period. The Commission finds this qualification reasonable. Moreover, ESEs are appropriately permitted to retain information as required by federal, state and local laws, rules, regulations and orders, or for legitimate business or legal needs. This provision also includes reciprocal

language providing that an ESE may make a written demand to the utility to destroy or return Confidential ESE Information.

Finally, the Joint Utilities are directed to clearly lay out in the written demand to destroy/return information the reason(s) for such a demand. Any ESE who disputes a demand to destroy or return Confidential Customer Utility Information can utilize the dispute resolution processes in the UBP or file a complaint with the Department of Public Service's Office of Consumer Services Staff, as appropriate.

Turning to the provision regarding termination of the DSA, the Commission supports RESA's comment proposing to require the distribution utility claiming a material breach of the DSA has occurred to specifically identify and describe the alleged breach of the DSA. Likewise, ESEs that wish to dispute a determination that a material breach of the DSA has occurred remain entitled to utilize the dispute resolution processes in the UBP or file a complaint with the Department of Public Service's Office of Consumer Services Staff, as appropriate.

5. Data Security Incidents

a. Party Comments

The DSA Coalition comments that the Data Security Incident provision affords the utilities undue control over and ESE's response to an incident. The DSA Coalition asserts that the requirements regarding customer notification and offering of credit monitoring go beyond what is required under New York State and U.S. Federal law. The DSA Coalition proposes that this provision should provide for a case specific response approach, with disputes being brought to Staff or the Commission. NEM comments that New York Law already prescribes the process to be followed in the event of a cybersecurity breach and that the DSA gives the Joint Utilities too much discretion. Additionally, NEM and RESA assert that the DSA should include reciprocal language

requiring that the distribution utility notify ESCOs of a data security incident at the utility.

b. Discussion & Conclusion

While the Data Security Incident provision provides the Joint Utilities with some discretion as to how cyber events will be handled, no party has provided a basis as to why such discretion would be inappropriate in light of the serious consequences that could arise out of a major cybersecurity breach. Moreover, actions taken pursuant to this provision are subject to the dispute resolution, appeal, or complaint processes before the Department of Public Service or the Commission, as applicable.

Regarding the assertions that the Data Security Incident provision goes beyond what is currently required under New York Law, such deviations are acceptable in this instance. The Commission is hereby establishing the appropriate protocols to be followed in the specific instance when Confidential Customer Utility Information is inappropriately released. This requirement is more specific than the general requirements found in New York Law.[56]

Other Modifications

In addition to the modifications to the DSA and SA discussed above, the Joint Utilities should also make two additions to the DSA. First, a "Date" line should be added to the signature page for both the ESE and distribution utility signatures. Second, the Joint Utilities should execute and return a copy of the final DSA to the ESE within five business days of receiving an executed DSA/SA from the ESE. The Joint Utilities should ensure that modifications and/or exceptions have been

[56] See NY GBL §899-aa.

incorporated into the DSA and SA that take into consideration the differences for GBC, such as requirements for consent.

CONCLUSION

Maintaining the security of customer utility data and the distribution utilities' IT systems is essential to ensure that markets operate efficiently and that customers are not harmed by the unauthorized release of their data. The DSA presented by the Joint Utilities in the Petition, with the modifications discussed above, establishes the minimum cybersecurity and data protection requirements necessary to access customer data through utility IT systems. Cybersecurity is an ever-changing issue, and one the Commission expects to address in future proceedings, including the examination of a more risk-based approach to supplement the foundational protections provided for in this Order.

Additionally, notably absent from the DSA are the obligations of the utility for service levels and processes when they are providing data to ESEs. The UBP does include some utility responsibility provision but these have not been developed for use by all ESEs. The identification of applicable utility side obligations, including timely and meaningful access to accurate data, should continue to be discussed and developed, including development and inclusion in the terms and conditions for GBC participation. The Commission supports the provision of useful access to useful data for entities offering potentially valuable products and services to customers, with customer consent.

The Commission orders:

1. Consolidated Edison Company of New York, Inc., Orange and Rockland Utilities, Inc., Central Hudson Gas & Electric Corporation, National Fuel Gas Distribution

Corporation, The Brooklyn Union Gas Company d/b/a National Grid NY, KeySpan Gas East Corporation d/b/a National Grid, and Niagara Mohawk Power Corporation d/b/a National Grid, New York State Electric & Gas Corporation, and Rochester Gas and Electric Corporation are directed to, within 60 days from the date of this Order, file a revised Data Security Agreement and Self Attestation consistent with the discussion in the body of this Order.

2. Energy Service Entities seeking access to customer data through utility IT systems shall be required to execute a Data Security Agreement and Self Attestation as revised in conformance with Ordering Clause No. 1 as a prerequisite of accessing such customer data.

3. In the Secretary's sole discretion, the deadline set forth in this order may be extended. Any request for an extension must be in writing, must include a justification for the extension, and must be filed at least one day prior to the affected deadline.

4. These proceedings are continued.

By the Commission,

(SIGNED) KATHLEEN H. BURGESS
Secretary

APPENDIX A

LIST OF COMMENTERS

Advanced Energy Economy Institute[1]	Advanced Energy Companies
AES Distributed Energy, Inc.	AES
Agway Energy Services	Agway
Blueprint Power Technologies, Inc.	Blueprint
Consumer Power Advocates	CPA
Energy Technology Savings, Inc. dba Logical Buildings	Logical Buildings
Fluent Energy	Fluent
Hansen Solutions LLC	Hanson
Joint Utilities	Joint Utilities
Mission:data Coalition, Inc	Mission:data
National Energy Marketers Association	NEM
New York Power Authority	NYPA
New York Retail Choice Coalition	DSA Coalition
New York Solar Energy Industries Association	NYSEIA
Retail Energy Supply Association	RESA
UtiliSave, Inc	UtiliSave

[1] On behalf of Advanced Energy Economy (AEE), the Alliance for Clean Energy New York (ACE NY), the Northeast Clean Energy Council (NECEC), and the Advanced Energy Management Alliance (AEMA).

COMMENT SUMMARY

Blueprint Power Technologies, Inc.

Blueprint Power Technologies, Inc. (Blueprint) referenced it's concerns with certain definitions within the DSA. By making references to numerous standards, Blueprint continues, the DSA leaves open the very real possibility of inconsistencies across the grid thereby resulting in security risks and interoperability issues. Blueprint states that it is not comprehensible that the DSA refers to such a wide range of "requirements" covered by the DSA definition of Data Protection Requirements. These cited requirements, Blueprint claims, are arduous and untenable to meet and provide evidence. Blueprint specifically referenced the inconsistencies and varying levels of security definitions of Audit Log Content, Timestamps, and Default Passwords. Blueprint seeks clear, well-defined criteria for meeting minimum data security standards to ensure that there is no ambiguity as to the level of security that must be attained to preclude the discontinuance of an ESE's participation in utility programs that may occur as a consequence of an audit. Blueprint's concerns with the Audit definition section of the DSA, refers to "all applicable Data Protection Requirements" which is fraught with inconsistency, unintelligibility, and unpredictability that is requisite to managing auditor expectations and the focus should be placed on risk management.

Blueprint recommends that consideration be given to NIST SP 800-171 as the cybersecurity standard, which is specifically intended for non-federal systems. Blueprint indicates that the NIST SP 800-53 framework also has viability. The key according to Blueprint is to select a single standard that is understandable, implementable and provides the requisite level of security. Blueprint notes that a specific criterion must be established to

ensure necessary security across the grid and guarantee a reasonable, cost-effective audit process.

Hansen Solutions LLC

Hansen Solutions LLC (Hansen) agrees that there is a need for appropriate cyber security standards and fully supports the application of reasonable requirements. Hanson submitted five recommendations within their comments. Hansen recommends adopting information security requirements in the “Self-Attestation of Information Security Controls” as the appropriate cyber security standards to be applied by all market participants.

Hansen requests that the DSA be updated accordingly, by removing all references to EDI providers being ESEs. The wording of “contractors of such entities” in the definition of “ESE” in the DSA “and contractors of such entities with which utility electronically exchanges data other than by email or by publicly available portal” should be removed, according to Hansen.

Hansen further recommends updating the definition of “Third-Party Representatives” by (a) inserting EDI providers into the definition; and (b) inserting reciprocal language with respect to processing of Confidential Information by a Utility's third-party contractors and subcontractors. Hansen also recommends updating the terms of the DSA (a) to ensure the DSA is consistent with the reciprocal nature of the updated 'Third-Party Representatives' definition, (b) that it is the responsibility of each Party to ensure that the Appropriate Cyber Security Standards have been implemented by their Third-Party Representatives, and that each Party is solely responsible to the other Party for the performance of their respective Third-Party Representatives with respect to the Appropriate Cyber Security Standards, (c) to set out other specific data security obligations that a Party needs to include in their agreements with its Third-Party Representatives,

and (d) remove ambiguous language. Finally, Hansen recommends an affirmation that third-party providers to either Party (such as EDI providers) do not have to sign the DSA.

Energy Technology Savings, Inc. dba Logical Buildings

Energy Technology Savings, Inc. dba Logical Buildings (Logical Buildings) comments that as the DSA stands today, many of the provisions will cause DERS to hesitate to enter the market and may also force existing DERS to exit the market due to the complexities and costs in the DSA requirements. Logical Buildings agrees with Mission:data, that the UBP-DERS specifically excludes DERS from having to sign the DSA if they do not utilize EDI to obtain customer data. Logical Buildings further states that signing the DSA will stifle the development of the growing DER market and may cause competitive limitations in the marketplace.

Logical Buildings notes that strict regulations, such as those resented in the DSA regarding use of customer data are an unnecessary burden. A reasonable requirement of signing a Non-Disclosure Agreement (NDA), Logical Buildings asserts, would provide adequate protections without the DERS being subject to the strict requirements of the DSA.

Logical Buildings notes the definition of Third-Party Representative lacks clarity as to who is required to comply. It claims that these requirements will make it more difficult for DERs to communicate and work with third parties. Logical Buildings notes that the release of customer information to third parties is normally done with customer consent, and NDAs between the parties. Logical Buildings suggests that Con Edison pre-approve certain third-party services commonly used by DER businesses such as Amazon Web Services, Google Cloud Platform, Microsoft Azure, etc.

Logical Buildings states that the DSA requirements should not apply to any party that does not interact with utility systems and certain sections within the DSA need clarification regarding that point. It further states that there should be no requirement of cyber insurance for any party not directly interacting with utility systems and that the email encryption requirement is overly burdensome and would disrupt normal business processes due to regular communications with customers via email.

National Energy Marketers Association

The National Energy Marketers Association (NEM) supports the development and implementation of reasonably cybersecurity standards for the retail energy marketplace. NEM respectfully recommends the Commission to reject the Joint Utilities' Petition for a Declaratory Ruling regarding their "right" to discontinue ESCO service if an ESCO has not executed a DSA and SA. NEM asserts that the JU Petition and relief requested should be denied by the Commission.

NEM states that the business-to-business process did not result in a balanced agreement. NEM argues that the utilities heavy-handed business-to-business process to develop the DSA and SA was not appropriate and resulted in major substantive disagreement. According to NEM, Staff's conclusion that a "balanced DSA" was developed during the business-to-business process fails to recognize the utilities position of superior bargaining power vis a vis the ESCOs. NEM argues that an ESCO decision not to acquiesce to a utility's demand to sign the DSA and SA should not be grounds for discontinuance, particularly not without Commission intervention in the process.

NEM projects that the Commission has the authority to promulgate and adopt rule, not the utilities it regulates. The Public Service Law, NEM continues, vests the Commission with the

authority to promulgate and adopt rules and to approve tariffs, not the utilities that the Commission regulates through the business-to-business process. However, NEM claims that neither of the documents' terms and conditions have been reviewed and approved by the Commission. NEM states this should be a SAPA compliant rulemaking process and a business-to-business process would be better utilized after the Commission has adopted a policy. Certain provisions and terms within the DSA and SA are policy and precedent setting according to NEM. The specific terms that NEM is referring to are customer data, cyber insurance, third-party representatives, locations for storing data, and audit rights. NEM states that the business-to-business process did not satisfy SAPA requirements. The DSA and SA, NEM continues, effectively establish cybersecurity policy for the retail energy marketplace through amendments pertaining to customer information via EDI and by requiring a regime for data access, use, storage and destruction.

Additionally, NEM claims that an ESCO's decision not to sign the unapproved agreements does not constitute non-compliance with a Commission rule and that the utilities do not have the right to discontinue ESCO service because an ESCO has not signed the DSA or SA. NEM asserts that an ESCO's decision not to sign the DSA or the SA does not mean that the ESCO has not implemented robust cybersecurity measures to protect customer data that are appropriate to the size and scope of its individual business. In the absence of such Commission guidance, NEM continues, the Joint Utilities should not be permitted to exert unchecked discretion in deciding that an ESCO should be discontinued under the UBP.

NEM proposes that the Joint Utilities' request to discontinue ESCO service without Commission intervention should be denied. In discussing DER provider's obligations, NEM notes that UBP Section 2.F.1.a has no corollary provision in the UBP-DERS.

Interpreting Section 2.F.1.a. to allow the Joint Utilities to discontinue an ESCO that has not executed the agreements, NEM asserts, is an extremely harmful and dangerous precedent to set.

Agway Energy Services

Agway Energy Services (Agway) supports the need for DSA between the JUs and ESCOs. However, Agway argues that, the current DSA, and business-to-business process used to create the DSA, have significant shortcomings that require rejection, both the process and resulting DSA. According to Agway, the business-to-business process did not provide enough opportunity for adequate industry participation. Agway asserts that the participating ESCOs had no control over the duration of the process and had very little input into the frequency of the meetings.

Agway further argues that the business-to-business process was grossly unfair. Agway claims that the Joint Utilities are direct competitors of the ESCOs and have an interest in limiting the ESCOs access to customers. Agway states there is an imbalance in bargaining power for provisions such as the right to audit ESCO operation, restrict ESCO derivative data uses, restrict the locations where ESCOs are permitted to process and store data, impose unlimited liability and indemnification on the ESCOs, and require a $5 million cyber insurance policy. Agway urges the Commission to reject the Joint Utilities' request to affirm the collaborative business-to-business process as it was neither collaborative nor did it offer opportunity for genuine negotiation.

Agway notes that adopting the DSA standards would violate SAPA and the SAPA compliant rulemaking process. It claims that the business-to-business process was invalid and therefore the resulting DSA is also invalid. With the current DSA and SA,

Agway continues, the Commission did not submit a notice of proposed rulemaking to the secretary of state, and no publication of the DSA occurred in the state register. Agway asserts that the Commission should reject the JUs request that the Commission adopt specific standards for cybersecurity included in the DSA and SA as the constitute a rule making in violation of SAPA.

Additionally, Agway argues that the Commission should not affirm that the JUs has the authority to end access to disconnect ESCOs who have not signed the DSA and can do so without Commission intervention. Not signing the DSA does not necessarily compromise JUs system security, according to Agway, and intervention from the Commission would be required to determine if an ESCOs refusal to sign the DSA constituted a threat to the Joint Utilities.

New York Power Authority

The New York Power Authority (NYPA) supports a statewide initiative to adopt data security requirements which provide protections for physical systems and consumer information. NYPA argues that implementing these protections though a single, uniform Data Security Agreement does not account for how the unique statutory and regulatory obligations and responsibilities of New York State Agencies and Authorities, limiting their ability to comply. NYPA claims that it cannot comply with certain provisions of the proposed DSA, which cannot be implemented in the manner or timeframe proposed by the Joint Utilities, while also ensuring that State Agencies are contributing to the achievement of the State's energy goals by processing and analyzing historical energy consumption data. NYPA argues that modified DSAs for NYPA and other State Entities that both maintain the data protection standards desired by the Commission and the Joint Utilities and account for the unique nature of NYPA and other State Entities are

necessary. NYPA states these modified agreements will foster development of terms that protect utility systems and customer data while accounting for the unique statutory and regulatory obligations.

NYPA recommends that if modified agreements are not allowed, then the proposed DSA must be amended to be flexible enough to ensure that State Entities can comply and be modified to provide signatories with commercially reasonable terms. NYPA notes that any references to the UBP and UBP-DERS must be removed as NYPA is not subject to either. NYPA also suggests allowing for retention of data after termination of DSA to meet applicable Federal, State, and local requirements. NYPA further notes that the indemnification provision must also be modified to be commercially balanced. Lastly, NYPA suggest the inclusion of a defined contractual term and a clear process for modifications, in addition, any future amendments to the DSA should be made through clearly defined procedures.

Consumer Power Advocates

While Consumer Power Advocates (CPA) and Luthin Associates, Inc. (Luthin) (collectively CPA) find the SA to appear reasonable, they do not believe the DSA is reasonable claiming the DSA to be a lopsided agreement crafted without the benefit of input from most of those to whom utilities intend that it should apply. CPA claims that the proposal insulates the utilities, imposes unreasonable requirements on entities, and discourages new entities from participating in the market.

CPA voices concern about the applicability and awareness of the requirements outlined in the proposed DSA and SA. The proposals, CPA continues, are intended to apply to ESCOs, DERs, and ESEs yet many of the entities that the JU refers to as ESEs, such as consults and contractors, only became aware that their

access to customer data was at risk late in the process. CPA asserts that it is not clear that all, or even most, consultants and other third parties are aware that potentially onerous and expensive cybersecurity rules are being developed for them.

CPA believes that there needs to be a reasonable balance between the burden of cyber security protections and their efficacy. After reviewing the proposed Self-Attestation Form, CPA does not believe that any of the requirements are unreasonable.

CPA stated the definition of "ESE" is too broad and they object to a requirement that holds companies responsible for the behavior of others that they have no control of. CPA further states the need for more clarity in the definition of what data needs to be protected and is too broad as written. CPA acknowledges that the proposed DSA takes a very expansive view as to what information is deemed to be confidential and must be protects. However, it believes that the following clause is problematic: "any other information provided to ESE by Utility and marked confidential by the Utility at the time of disclosure." According to CPA, the data that should be subject to that protection should be limited to only what is needed and not every piece of data merit the exact same degree of protection.

CPA recommends that cyber insurance requirement be eliminated for DERs, contractors, and third parties. It claims that focus should instead be on assuring that all entities have robust policies and practices, such as those described in the Self-Attestation Form, in place. To the extent that cyber insurance is required, CPA recommends that the Commission should consider scaling the requirement according to the level of risk imposed and the revenues of the firm. Referencing the indemnification provision, CPA states that companies facing this liability may choose to do business elsewhere.

CPA further argues that DSA Section 1.d(B) should be

deleted in its entirety. It states that no entity without staff dedicated to following cyber threats and cybersecurity issues on a full-time basis could understand the data protection requirements. CPA expresses concerns with maintaining compliance as well, with the inclusion of the phrase "may evolve over time." CPA would further like to call attention that Luthin, and perhaps others, are facing an immediate issue with respect to access to customers' gas usage information from Con Edison's Transportation Customer Information System.

Fluent Energy

Fluent Energy (Fluent) indicates that they are generally supportive of the Joints Utilities' need to require enhanced cybersecurity but are also concerned that the new proposed requirements as applied to a particular class of Direct Customers would be inappropriate as a consequence of both how these Direct Customers participate in the market, and what the underlying rationale for the application of the requirement is. Fluent argues that non-interacting direct customers (NIDCs) do not represent the same risk to utilities as interacting parties and must be addressed in an alternative manner.

Additionally, Fluent asserts that Direct Customers do not present the same risk to utilities as entities that manage the data of external parties. It claims that there is no risk of unauthorized disclosure or breach of other market participants' confidential data because Direct Customers do not manage the data and account numbers.

The application of security requirements to NIDCs presents difficulties according to Fluent. Fluent argues that NIDCs are ratepayers and should not be considered ESEs and should not be exposed to duplicative costs related to security requirements. Fluent believes it is unfair to impose the same

security requirements and associated financial burdens on NIDCs which have already been required of its agent(s) and paid for. Fluent believes that NIDCs should not be considered ESEs and are genuinely unaware of factors that would preclude eliminating the requirements, if they are met by the third party. Fluent suggests that a "Proxy Agent" based approach would allow NIDCs agent, such as Fluent, to serve as a proxy in meeting new security requirements, which might not require revision or amendment of the DSA with respect to Direct Customers going forward.

Fluent requests the Commission to affirm that NIDCs are not subject to the requirements to execute DSAs, provide SAs, or be required to indemnify or otherwise insure other entities or utilities unless specific credible risks to the utility has been established.

New York Retail Choice Coalition

New York Retail Choice Coalition (DSA Coalition) states the Joint Utilities are encroaching on authority reserved for the Commission and the proposed requirements cannot be considered without a proper rulemaking procedure. The DSA Coalition contends the request by the Joint Utilities for Declaratory Order is premature and the business-to-business process was not the appropriate vehicle for developing new industry-wide cybersecurity standards. The DSA Coalition contends that the cybersecurity requirements imposed on an ESE should be promulgated by the Commission. The business-to-business process, the DSA Coalition continues, occurred outside of the scope of SAPA where the Joint Utilities' were delegated authority that should have been held by the Commission. According to the DSA Coalition, the DSA and SA alter key provisions of and ESCO rights arising under the UBP. The DSA Coalition notes that the Joint Utilities do not have authority to promulgate rules under SAPA and to date, the

Commission has not provided notice of any proposed rule regarding cybersecurity standard for ESCOs. The DSA Coalition recommends that the cybersecurity standards should encompass an individualized, risk-based approach rather than a unilateral template. The DSA Coalition recommends that the Commission should reconsider the DSA's overly broad framework and instead adopt standards that embody risk-based principles like the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The DSA Coalition proposes an establishment of a cybersecurity working group to develop industry standards.

Additionally, the DSA Coalition believes that provisions of the DSA and SA has made substantial progress but require further revision. According to the DSA Coalition, the Commission cannot make its determination while issues from the Department Staff report remain unaddressed, such as vulnerabilities in the Joint Utilities' systems that threaten the security of confidential and sensitive customer information, an independent analysis of whether the practices under the DSA and SA would protect utility systems, and an analysis on whether insurance is the best way to mitigate financial risks.

The DSA coalition outlined several disagreement areas. It noted specific issues with the definitions for "Confidential Utility Information" and "Data Protection Requirements." The DSA coalition claims the definition for "Confidential Utility Information" fails to account for varied classifications of data and does not support a risk-based program for protecting information according to its sensitivity and risk of harm. The DSA coalition believes revisions are needed to clarify that ESEs can use Confidential Utility Information for all lawful purposes allowed under the UBP or UBP DERS, as applicable. The DSA coalition also states that, as written, the definition of "Data Protection Requirements" contains numerous cybersecurity

standards, and failure to comply with any of them creates an automatic "Data Security Incident" regardless of whether there is actual harm to the Joint Utilities' systems, or if the ESE is following other equally or more stringent standards. This is inconsistent, according to the DSA Coalition, with the DSA provision that states an ESE will comply if it returns a SA that meets with the Joint Utilities' requirements.

The provision of information section, the DSA Coalition continues, discusses extensively a utility's rights to limit provision of information if the utility determines that an ESE does not comply with one or more aspects of the DSA. The DSA Coalition believes it is important to include language that decisions regarding access are subject to the UPB or UBP DERS process.

Speaking further about "Data Security Incidents," The DSA coalition contends that the requirements of notifying customers and offers of credit monitoring are beyond what is required under current applicable State and Federal laws. The DSA coalition notes that they have argued for this provision to be modified to provide for a good-faith agreement between the utility and an ESE on a case-by-case basis. It proposes that if agreement could not be reached, any deficiencies could be addressed by appeal to Department Staff or the Commission itself.

The DSA coalition asserts that mandatory cybersecurity insurance requirements set in the DSA is without foundation and is not authorized under Commission regulations or pursuant to any UBP process. It recommends the provision be revised to allow for a determination of the amount required on a case-by-case basis. The DSA coalition also believes that a self-insurance option should be recognized.

The DSA coalition states they have previously recommended a list of countries that should be automatically

approved for data storage, due to their data privacy regimes that are as protective, if not more protective, than the US and Canada, and believes this list should be accepted in its entirety.

The Third-Party Representatives section, the DSA Coalition continues, imposes excessive requirements on those who may have access to Confidential Utility Information, including extending UBP requirements onto third parties. The DSA Coalition argues that the DSA must be revised to account for actual risk profiles of third parties when determining which security requirements, if any, be imposed. Finally, The DSA coalition notes the use of the Self-Attestation form to require compliance is inappropriate while negotiations on the scope of the DSA are pending.

Retail Energy Supply Association

Retail Energy Supply Association (RESA) urges that cybersecurity protections should not be achieved at the expense of tailored solutions that address the unique aspects of each stakeholder's role in the marketplace, and that the Commission should reject the instant Petition. RESA argues that providing this level of authority to the utilities introduces a dangerous precedent for future matters and that the petition should be rejected because the utilities seek an improper delegation of authority. RESA notes that Commission intervention is required pursuant to the UBP, and the business-to-business process is inequitable. RESA contends that neither the UBP nor the utilities' tariffs provide the utilities with the authority to discontinue ESCO interactions without Commission intervention. They provide that Section 2 of the UBP states that Commission oversight is to be present when initiating a discontinuance, and Section 2.F.1 states there must be a case-specific finding that there is reason to discontinue an ESCO. RESA argues that failure

to execute a DSA does not trigger the discontinuance process in the UBP and that the utilities have failed to provided evidence of risk associated with ESCOs operating pursuant to the status quo absent a DSA. The DSA, RESA continues, is nothing more than a contractual agreement governing liability and does not actually ensure that the utility network is not compromised by EDI transactions.

RESA points out the petition should be rejected because the requested business-to-business approach is inequitable. According to RESA, the proposed approach eliminates the need for Commission oversight over the contents of the DSA and provides utilities with unfettered discretion to unilaterally impose cybersecurity requirements on ESEs. RESA does not oppose the use of a collaborative process between the utilities, stakeholders, and security experts to better understand whether, and to what extent, revisions to the DSA are needed.

RESA notes that the Joint Utilities' request should be rejected because some concerns from stakeholders have yet to be addressed, such as determining what constitutes "Confidential Utility Information," establishing a cause/effect and limitation of liability with respect to an indemnification provision, and revising the DSA to include mutual data protections for the Utilities and ESCOs.

AES Distributed Energy, Inc.

AES Distributed Energy, Inc. (AES) argues that further revisions must be made to strictly tailor the DSA and SA to account for the unique circumstances of and limited risk posed by the DER market. AES argues that DER suppliers should be exempt from compliance with the DSA, SA, or any similar policies as the potential implications and consequences are less significant in the DER market. AES contends that the DER market is mainly

comprised of large commercial and/or municipal customers who are more business savvy and aware of data security issues compared to residential customers.

AES recommends DER suppliers be exempt from purchasing cyber liability insurance as DER suppliers have very little, if any, direct access to the Joint Utilities' systems and therefore pose little, to no, risk of security breaches. If the Commission determines that the cyber security protocols are applicable to DER supplier, AES respectfully requests that maintaining cyber security liability insurance at the parent corporate level be allowed to satisfy requirements.

Advanced Energy Economy Institute

Advanced Energy Economy Institute (AEE Institute) submitted comments on behalf of Advanced Energy Economy (AEE), the Alliance for Clean Energy New York (ACE NY), the Northeast Clean Energy Council (NECEC), and the Advanced Energy Management Alliance (AEMA) (collectively, the Advanced Energy Companies). Advanced Energy Companies support efforts across the energy sector to strengthen cybersecurity. Advanced Energy Companies contends that the DSA is too broad when addressing diverse types of data transactions. Throughout the DSA, Advanced Energy Companies continue, there is no distinction between varying levels of threats, treating them all the same. Furthermore, Advanced Energy Companies claim that the DSA covers multiple types of entities, however, the rationale applied to the requirements in the DSA is based on a vendor-utility relationship and does not adequately account for a third party's relationship with its customer. According to Advanced Energy Companies, the DSA should recognize the different types of relationships between customers, vendors, third parties, and utilities.

Advanced Energy Companies argue that the business-to-business process, that the JU seek to affirm, is not appropriate given that third parties have anti-competitive and market-access concerns. Advanced Energy Companies argue that the Green Button Connect (GBC) collaborative is the appropriate venue for addressing GBC data security requirements. Advanced Energy Companies recommend that Staff should lead a separate stakeholder process to revise the DSA under certain guidelines to address non-GBC data exchanges and then adopt a final DSA following stakeholder comment.

Advanced Energy Companies argue that the petition does not adequately account for the rights of the customer. According to Advanced Energy Companies, the Commission should be cognizant that a direct transfer of data from the customer remains an alternative if the conditions of the DSA prove to be overly restrictive or too costly. There is aligned risk, Advanced Energy Companies continue, that the hassle may outweigh the benefits the customers experience and lead to customer attrition. Advanced Energy Companies encourage the Commission to find the appropriate balance, as cybersecurity requirements that are not appropriately focused will impair the productive use of energy data, limit the potential for vibrant markets for energy services, and ultimately impede private consumer investment that will help meet the state's important greenhouse gas reduction goals.

New York Solar Energy Industries Association

New York Solar Energy Industries Association (NYSEIA) claim that the current DSA and business-to-business process have significant shortcomings and that the business-to-business process that resulted in the creation of the DSA and SA was fundamentally flawed. NYSEIA claims that the ESEs were not afforded meaningful participation before the utilities declared the DSA and SA as

final, invalidating the business-to-business process used.

According to NYSEIA, a cybersecurity insurance requirement of $5 million is cost-prohibitive and would not significantly offset costs to a utility in the event of a major breach. Any cybersecurity insurance policy, NYSEIA continues, that would cover costs to a utility of a large breach would be completely unaffordable for all but the largest market participants, therefore erecting a barrier to entry by smaller firms. To the extent that cybersecurity insurance is required, NYSEIA recommends that the Commission consider scaling the requirement according to the nature of the data to be protected and the level of risk imposed and the revenues of the firm.

NYSEIA claims the Derivative Data Prohibition is unreasonable and irrational because it appears to prohibit the creation or maintenance of data which are derivative, which is broadly defined to encompass the most basic mathematical manipulations, of Confidential Utility Information. According to NYSEIA, where a customer has consented to the use of its data for a particular purpose, regardless of whether it is for the purposes of the DSA or authorized under the UBP, the fact that the data was obtained from the utility should be immaterial. NYSEIA asserts that it is not reasonable to bar such consultants from engaging in any analytical work simply because the utility wants to assert proprietary rights over data, that is the customers not the utilities.

UtiliSave, Inc.

UtiliSave, Inc. (UtiliSave) believes the Joint Utility Petition should be denied. UtiliSave notes that compliance with the DSA is complex and claims the additional requirements are onerous and unnecessary. UtiliSave details utilities policies of limiting the amount of “hardcopy” documents in the interest of

saving money but also while increasing the availability of electronic information. Utilisave asserts that the Joint Utilities have limited what they can be relied upon to produce, and are now they are making an attempt to curtail access to the electronic information specifically to entities like UtiliSave, who serves as a consumer watchdog.

UtiliSave further argues that the process by which the DSA was created was coercive and unfair. U tiliSave strongly objects to the process by which the DSA was negotiated and believes the Commission should be determining a fair agreement between parties rather than deferring the Joint Utilities' unfair process. UtiliSave supports the Mission:data Petition because they believe the Joint Utilities' position conflicts with the Commission's Order Establishing Oversight Framework and UBP for DER Suppliers.

Mission:data Coalition, Inc.

Mission:data Coalition, Inc. (Mission:data) strongly urges the Commission to dismiss the Joint Utilities' Petition. Mission:data states that the Joint Utilities' Petition seeks authorities that are inconsistent or incompatible with Commission Orders. Mission:data argues that the Joint Utilities' petition would violate language in the DER Oversight Order that states Section 2(c) of the UBP DERS does not impose any obligations to DER suppliers not using EDI. According to Mission:data, the Joint Utilities are proposing to terminate companies that are in breach of the DSA without Commission intervention, which Mission:data argues is too much control in the hands of the utilities. Furthermore, Mission:data notes that the UBP-DERS does not include the same termination provisions as the UBP for ESCOS (Section 2.F.1.a) and that section would not apply to DERS.

Mission:data notes that the original definition of ESE in the Commission's Order initiating this proceeding does not include DERs. Mission:data claims that, twice the Commission has limited the application of data security provisions to entities that use EDI, and yet the Joint Utilities Petition ignores this important distinction.

Mission:data claims that the Joint Utilities' request to modify DSA in the future causes concern over what provisions they might add or remove and how that may affect DERs, such as billing information or audit requirements. According to Mission:data, the Joint Utilities are seeking to eliminate the due process of DERs while utilities and DERs are co-equal market participants providing energy related services and should have an equal right to participate in rulemaking concerning Commission oversight of DERs that use GBC.

Commenting on the process, Mission:data states that the business-to-business process has not been the appropriate method for development of this issue. This process, Mission:data argues is an abdication of the Commission's legal responsibilities and is a breach of SAPA. Mission:data claims that DERs were not given enough opportunity to speak at stakeholder meetings and were not well received by Joint Utilities when they did.

Mission:data argues that Derivative Data Prohibition is too broadly defined and could encompass practically every processing function of customer-authorized software program. Mission:data contends that creating derivatives should be encouraged by the Commission, not prohibited, since engaging customers with new data analysis techniques that help save energy is one of the primary goals of REV.

Concerning customer consent, Mission:data points out that the UBP-DERS require suppliers to retain verifiable proof of authorization for each customer for a minimum of two years. DERs

would be subject to holding the customer's authorization for inspection by the Commission for a minimum of two years, but it is the utility, not the DER, that receives the customer's authorization. Thus, according to Mission:data, without that verifiable proof, the DER could immediately by in breach of the DSA.

Mission:data asserts that the Joint Utilities responded to Mission:data's Petition for Declaratory Ruling in related proceeding (DER Oversight Order) as "moot" since the Joint Utilities will be working with Staff and stakeholders, including presumably Mission:data, to develop appropriate GBC cyber security and customer data protections. Mission:data responded with stating if the Commission's consideration of GBC terms and conditions in an ongoing proceeding is reason to deny Mission:data's petition concerning the DER Oversight Order's cybersecurity requirements, then the Commission must also deny the Joint Utilities' request to enforce the DSA against GBC users because of ongoing proceedings discussing cybersecurity requirements. Both Mission:data and the Joint Utilities seek guidance from the Commission on the applicability of the DER Oversight Order; it would be illogical for the Commission to apply different standards to the respective petitions of Mission:data and the Joint Utilities.

Mission:data argues that the Joint Utilities are incorrect in stating other jurisdictions require similar terms to the DSA. It asserts that the Joint Utilities cited NDAs in a utility in Illinois which are unenforceable to the extent they conflict with the Illinois's Commission-approved tariff or decision that governs GBC. According to Mission:data, the tariff requirements in this case are much simpler than the DSA, in that they must meet certain confidentiality requirements, complete interoperability testing with the utility, and submit a

registration with contact information. Mission:data claims that none of the following points are present in those tariffs or required agreements: adherence to specific, named cybersecurity standards including NIST SP 800-53 and ISO 27001 / 27002; a SOC II audit, or any other on-site audit rights for the utility to inspect the third party's facilities; notification to the utility of a data security incident; prohibitions on creating or maintaining "derivations" of energy data; prohibitions on sharing energy data with "third-party representatives" unless consistent with the customer-authorized purpose; return or destruction of customer energy data following termination; and cybersecurity breach insurance.

Although Mission:data strongly urges the Commission to reject the Joint Utilities Petition, Mission:data understands that merely rejecting the petition does not solve all the challenges faced by the Commission Mission:data ends with three recommendations. First, Mission:data argues that the relationship between the customers, DERs, and utilities must be clearly understood. Mission:data asserts that the Joint Utilities are correct when they say that the DSA is "routine" and typical of the utility industry, and that the Joint Utilities fail to understand why DERs that seek to use GBC are not the utility's vendors. In telecommunications, Mission:data continues, there is the concept of the "demarcation point" which separates the monopoly utility from the competitive market, and a demarcation point needs to be defined for utilities in New York for REV to succeed. Mission:data argues that customer's consent to share data with third parties should mark that demarcation point.

Second, Mission:data recommends that the Commission should require utilities to own their system risk but disown any downstream data misuse risk (risk that a customer-authorized third party will abuse the customer's privacy rights using information

collected from the utility). Regarding system risks, Mission:data believes the utilities should be solely responsible for their IT systems. Mission:data believes that the Commission should not conflate the system security risks of GBC with EDI. Mission:data asserts that the Joint Utilities have falsely claimed that all interactions with utility IT systems pose identical risks and that shifting cybersecurity responsibility to GBC users is inappropriate. If the GBC platform is successfully attacked, Mission:data avows, that can only be because the utility has not adequately prepared and managed its systems. Mission:data claims that, while it is reasonable and necessary for utilities to "police" the data management practices of their vendors, the same is not true of GBC users.

Mission:data's third recommendation is to look to California for enforcement procedures. Mission:data claims that to be eligible, third parties must: provide utilities their contact information, including federal tax identification number, so as to uniquely identify third parties across the three investor-owned electric utilities; demonstrate technical capability to interact with the GBC platform; acknowledge receipt of the commission's privacy rules; and not be present on the commission's list of "banned" third parties. California's Commission, Mission:data continues, established a process by which utilities can report to the commission a "reasonable suspicion" of a third party's violation of privacy rules, and the commission will investigate and if the third party is found to have violated the rules, the commission can place the offending third party on the "banned" list. Mission:data notes that the utility does not have the ability to unilaterally revoke a third party's access; it is only by reporting a suspected violation that the utility passes off responsibility for investigation and enforcement to the commission.

Joint Utilities

The Joint Utilities note that the objecting parties incorrectly argue that the Joint Utilities' have not demonstrated that ESEs should be required to sign the DSA and SA. According to the Joint Utilities, the comments demonstrate many parties' preference that there be no requirements associated with their connections to utility systems to receive customer data. The Joint Utilities interject that the ESEs that oppose the DSA prefer to maintain the status quo leaving the Joint Utilities and their customers to absorb the risks and costs associated with cybersecurity and data protection. The Joint Utilities urge the Commission take swift action to make clear that ESEs must promptly comply with the minimum data security requirements in the DSA to continue access to utility systems. This transaction, the Joint Utilities continue, would hold the ESEs responsible and accountable for their actions and protect cyber environments and customer data received. The Joint Utilities assert that a significant number of ESEs have already signed a DSA throughout this process, including ESCOs representing a majority of the customers that use an ESCO for supply.

The Joint Utilities propose that the Commission should reject the parties' positions calling for elimination of the DSA and associated cybersecurity standards, and as requested: confirm the Joint Utilities' authority to require the DSA, and future amendments using the business-to-business process, and require the DSA to include, at a minimum, standard requirements affirm the JU's authority to require ESEs to satisfactorily complete a DSA and prohibit ESEs from electronic access to utility systems as well as customer data without a DSA; confirm that the ongoing Commission-supported business-to-business process that resulted in the negotiation and development of a DSA to receive customer data through the interconnection to utility systems, was appropriate.

The Joint Utilities contend that the process was open, transparent, and comprehensive and produced a fair and balanced modified DSA and has been the subject of significant public discussions and process, which included substantial compromise on behalf of the Joint Utilities. The Joint Utilities assert that the DSA was substantially based on the Commission-approved CCA DSA and that before requiring ESEs to complete this DSA, the Joint Utilities included: (1) a cyber insurance requirement (2) a vendor questionnaire concerning the state of the entity's cyber security program, and for some utilities; (3) a data security rider detailing cyber security requirements.

The Joint Utilities note that the cyber risks associated with connection to Joint Utilities systems and maintain customer data must be addressed. The Commission has already concluded, the Joint Utilities continue, that the Joint Utilities face cyber-related risks and must take steps to protect customer data from such risks. The Joint Utilities further asserts that most of the terms in the DSA are standard contractual terms, such as indemnification, which are customary in business contracts. They explain that the DSA has flexible elements, including the option of choosing among several cyber security standards, including NIST or ISO, for compliance. Additionally, the Joint Utilities assert that, contrary to the claim that the risk of ESEs accessing data is the same as a customer accessing its own data, customer-facing systems and ESE-facing systems are not fungible and were developed and designed differently.

The Joint Utilities also claim that, contrary to their assertions, parties had ample opportunity to discuss their concerns with the Joint Utilities' cyber personnel. The Joint Utilities argue that the ESEs' claim that a risk assessment and associated DSA should be separately developed for each entity is unworkable, unnecessary, and a poorly disguised attempt to delay

addressing responsibility for cybersecurity. They argue that ESEs would need to update their information every time certain changes were made and developing a risk analysis type process is ripe for discrimination claims. The Joint Utilities further note that, although costs associated with credit monitoring may be less for an entity with one customer, that entity could cause the same level or greater damage to utility IT systems than an entity with many customers.

The Joint Utilities assert that the Commission has provided ample and appropriate public process to resolve this issue. The Joint Utilities believe the assertions that the business-to-business process is flawed should be dismissed because the Joint Utilities have the inherent authority to take steps when necessary to protect their systems and customer data. They claim the process has been robust and provided the ESEs with multiple opportunities to raise concerns. This process, the Joint Utilities continue, resulted in modifications to the DSA and SA, such as reducing the SA to a two-page checklist containing minimum standards and reducing the necessary cyber insurance requirement by half, from $10 million to $5 million. Finally, the Joint Utilities believe that any claims by commenters that the DSA should not be required until there is a formal SAPA process are moot since the Joint Utilities' Petition was noticed in the New York State Register with the full SAPA process.

The Joint Utilities defend that the DSA provisions are reasonable. In discussing cyber security insurance, the Joint Utilities asserts that this type of insurance is an unavoidable cost of doing business and is necessary to mitigate the risk associated with cyber security incidents; both whether an incident will happen and the financial cost of a cybersecurity incident. The Joint Utilities also assert that the indemnification provisions are reasonable and that the indemnification provision

is standard and clear; if an ESE breaches or fails to comply with the DSA and the affected utility suffers harm as a result of the breach or non-compliance, the ESE is liable except to the extent of the negligence, gross negligence, or willful misconduct of the utility. The Joint Utilities argue that the termination provisions require a utility to notify Staff prior to termination, except in an emergent situation. The Joint Utilities refute the claim from ESEs that they will be able to terminate access to their systems without justification, asserting that these statements are incorrect and not consistent with the DSA and the UBPs. The Joint Utilities clarify that they would follow the UBP-required process of termination, unless there is an emergency. The Joint Utilities claims that in an emergent situation, a utility has the right to terminate a system connection or cease providing customer data to any entity that may be under attack or under the threat of an attack. They explain that this would be temporary and last only until the situation is addressed to the utility's satisfaction.

Additionally, the Joint Utilities assert that the data usage terms are appropriate and that the DSA does not add additional restrictions to the use of customer data beyond the UBP and the UBP-DERS. They acknowledge and agree with the point made by some commenters that where the customer gives consent for data used for a particular purpose, the data may be used for the authorized purpose.

The Joint Utilities state that the DSA requirements place appropriate requirements on the market participants and refute the claim that the DSA will drive up the cost of entry for market participants or that it conflicts with the REV policy. They state the requirements are the same across the market, and the market should develop with the appropriate cybersecurity measures for all participants. According to the Joint Utilities,

these requirements should be established at the outset of market development and market participants should consider and invest in cyber protections from inception and existing market participants should invest in these protections immediately.

The Joint Utilities state that the DSA should be applicable to all ESEs that maintain customer data and interconnect with the Joint Utilities' IT systems. As for third-party requirements, the Joint Utilities argue that entities that have an electronic connection with the Joint Utilities' systems and maintain customer data shared by the Joint Utilities must sign the DSA. The Joint Utilities note that while they continue to work with parties and Staff on terms and conditions for GBC, the current onboarding process for GBC requires a DSA. The Joint Utilities further refute the claim that direct customer, EDI providers, and State Agencies should be exempt from the DSA. However, the Joint Utilities agree to add the following language as a footnote to DSA Section 2, Scope of the Agreement stating: Where an ESE exclusively uses a Third-Party Representative(s) to communicate electronically with a utility other than by email and the ESE's Third-Party Representative executes a DSA with the utility, a DSA is not required of the ESE. The Joint Utilities also notes that it will amend the DSA for governmental authorities accordingly.

Additionally, the Joint Utilities agree to make four changes to the DSA based off this most recent round of comments. First, they will amend the DSA to eliminate the requirement that Third-Party Representatives that do not have electronic communication other than by email with the utility sign the DSA. However, they note that the ESE should remain liable for its Third-Party Representatives and the Third-Party Representative may be named in a law suit. Second, they will Edit "Data Protection Requirements" to address inconsistencies noted by BluePrint Power

Technologies. The Joint Utilities are willing to clarify this language by inserting the following sentence at the end of DSA Section 1(d) Data Protection Requirements: The means of data protection chosen by each ESE will be determined by the ESE, which is limited only by the requirement that it remain in compliance with the SA. Third, the Joint Utilities agree that it is reasonable for a parent corporation to provide cybersecurity insurance for its affiliates, conditioned on the affiliate being a named insured on the policy and that the policy is sufficient to provide $5,000,000 per incident of insurance benefit to the affiliate. Fourth, the Joint Utilities will amend the DSA to reflect the governmental language for NYPA and other state agencies to reflect that these entities utilize use the cybersecurity protections required by the New York State Office of Information Technology.

The Joint Utilities assert that they are not going beyond what is needed to protect their systems and customer data. According to the Joint Utilities, the realities of today's cybersecurity and data privacy climate are rapidly evolving, and protections are more important now than ever before. They claim that there can be no question that the ESEs add cyber risk to customer data and to the Joint Utilities' systems and that the ESEs need to protect customer data and appropriately design and protect their systems to meet the requirements under the SA for system to system interaction. Accountability and responsibility are paramount to keeping customer data secure according to the Joint Utilities.