

# Robinson+Cole

JOEY LEE MIRANDA

280 Trumbull Street  
Hartford, CT 06103-3597  
Main (860) 275-8200  
Fax (860) 275-8299  
jmiranda@rc.com  
Direct (860) 275-8227

Also admitted in District of Columbia and  
Massachusetts

*Via Electronic Filing and First Class Mail*

August 28, 2018

Honorable Kathleen H. Burgess  
Secretary  
New York Public Service Commission  
Three Empire Plaza  
Albany, NY 12233-1350

**Re: Case 18-M-0376 - Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place**

**RESA Motion to Form a Cybersecurity Working Group**

Dear Secretary Burgess:

Please find attached the Retail Energy Supply Association's ("RESA") Motion to Form a Cybersecurity Working Group in connection with the above-referenced proceeding.

Please feel free to contact me if you have any questions or require additional information. Thank you.

Sincerely,

  
Joey Lee Miranda

Enclosure

Copy to: Party List

**STATE OF NEW YORK**  
**PUBLIC SERVICE COMMISSION**

---

Proceeding on Motion of the Commission  
Regarding Cyber Security Protocols and  
Protections in the Energy Market Place

---

Case 18-M-0376

**RETAIL ENERGY SUPPLY ASSOCIATION'S  
MOTION TO FORM A  
CYBERSECURITY WORKING GROUP**

Joey Lee Miranda  
Robinson & Cole LLP  
280 Trumbull Street  
Hartford, CT 06103  
[jmiranda@rc.com](mailto:jmiranda@rc.com)  
*Counsel for Retail Energy Supply  
Association*

Dated: August 28, 2018

The Retail Energy Supply Association (“RESA”)<sup>1</sup> hereby moves the Public Service Commission (“Commission”) to establish a Cybersecurity Working Group (“Motion”) modeled after the current EDI Collaborative.

## BACKGROUND

On June 14, 2018, the Commission, in response to concerns raised by stakeholders about protecting the utility and retail energy provider industry systems from cybersecurity breaches, issued an order opening this proceeding that directed “Department [of Public Service] Staff to review the issues being addressed in the current business-to-business process between the Joint Utilities and energy service entities, and ensure that any issues that cannot be properly resolved in that forum are addressed in this proceeding.”<sup>2</sup> RESA has been an active participant in this proceeding.<sup>3</sup>

On July 26 and 27, 2018, Department of Public Service Staff (“Staff”) convened a stakeholder meeting “to discuss cyber security issues raised in the above-referenced proceeding.”<sup>4</sup> In particular, the stakeholder meeting focused on the following topics: i) the Attestations ii) the comments received on the DSA; and iii) additional processes moving forward.<sup>5</sup>

During that meeting, the various stakeholders, including the Joint Utilities, agreed that it would be beneficial for technical representatives to meet periodically in the future to discuss

---

<sup>1</sup> The comments expressed in this filing represent the position of the Retail Energy Supply Association (RESA) as an organization but may not represent the views of any particular member of the Association. Founded in 1990, RESA is a broad and diverse group of twenty retail energy suppliers dedicated to promoting efficient, sustainable and customer-oriented competitive retail energy markets. RESA members operate throughout the United States delivering value-added electricity and natural gas service at retail to residential, commercial and industrial energy customers.

<sup>2</sup> Order Instituting Proceeding (Issued and Effective June 14, 2018).

<sup>3</sup> *See, e.g.*, RESA Request for an Extension and a Formal Collaborative Process (Jun. 21, 2018).

<sup>4</sup> Notice of Stakeholder Meeting (Issued and Effective July 17, 2018).

<sup>5</sup> *Id.*

appropriate items for future versions of the Attestation and future iterations of the DSA, and a commitment was made to considering the establishment of such a group using the current EDI Collaborative as a model. Consistent with those discussions, RESA now hereby submits this Motion to Form a Cybersecurity Working Group (“CWG”).

### **MOTION**

As technology evolves, cybersecurity will continue to be an imperative topic for the Commission, ESCOs, the Joint Utilities and EDI vendors alike. A CWG will provide all stakeholders with the organizational structure necessary to address the rapid technological changes in this area. This proposed construct is especially important to ensure that the appropriate personnel with the necessary skill sets are involved in the development of future cybersecurity protocols and to protect the interests of the various market participants. Accordingly, the Commission should form a CWG modeled after the current EDI Collaborative as soon as practicable.

#### **I. A CWG WILL HELP ENSURE UNIFORM STATEWIDE STANDARDS AND PROMOTE FUNDAMENTAL FAIRNESS**

The EDI Collaborative was organized in October 1998 for the purpose of evaluating retail access data exchange practices and developing statewide data exchange standards.<sup>6</sup> In establishing the EDI Collaborative, the Commission recognized the importance and value of developing uniform statewide standards to guide the business processes of the stakeholders in the retail energy markets<sup>7</sup> and in avoiding individualized utility standards.<sup>8</sup> In doing so, the Commission recognized:

---

<sup>6</sup> Case 98-M-0667, *In the Matter of Electronic Data Interchange*, Opinion No. 00-05 (Issued and Effective April 12, 2000) (“Opinion 00-05”), at 1-2.

<sup>7</sup> Case 98-M-0667, *In the Matter of Electronic Data Interchange*, Opinion No. 01-03 (Issued and Effective July 23, 2001) (“Opinion 01-03”), at 13 (“In our view, the Collaborative should strive for statewide uniformity in crafting New York’s EDI data standards”).

If ESCOs/Marketers are confronted with a variety of information exchange systems, the complexity of doing business increases, and they will be less able to offer competitive options to smaller customers. In addition, different systems increase the likelihood of errors and processing delays, and variations in processing procedures across utilities would result in redundant programming costs for ESCOs/Marketers/Direct Customers.<sup>9</sup>

For similar reasons, cybersecurity standards should also be uniform across all utility service territories. For instance, while RESA recognizes that the Joint Utilities proposed a standardized DSA, it is possible that, in the future, each utility could require a different DSA or establish different cybersecurity protocols to which ESCOs must agree to abide. Depending on these requirements, ESCOs could be required to make significant modifications to their systems or protocols at substantial expense in order to do business in one utility service territory and have to make entirely different system and protocol modifications to do business in another utility service territory. Such a paradigm is untenable. Furthermore, without uniform DSAs, “ESCO/Marketers could be forced to accept utility unilateral offers and/or expend resources to negotiate separate agreements with each utility.”<sup>10</sup> Accordingly, to ensure uniform statewide standards, the Commission should establish a CWG modeled after the EDI Collaborative.

## **II. A CWG WILL HELP ENSURE A MORE COMPREHENSIVE AND WELL INFORMED SET OF STANDARDS AND PROMOTE FUNDAMENTAL FAIRNESS**

The EDI Collaborative is a consortium of individuals representing utilities, ESCOs, software and hardware vendors, and members of various standard setting bodies.<sup>11</sup> Notably, the EDI Collaborative consists of both business and technical representatives in order to

---

<sup>8</sup> Opinion 01-03, at 14 (“To insure uniformity and efficiency, initiatives such as those proposed by NYSEG and Rochester must be undertaken by the Collaborative, rather than by an individual utility...”).

<sup>9</sup> Case 98-M-1343, *In the Matter of Retail Access Business Rules*, Opinion No. 99-3 (Issued and Effective February 16, 1999), at 9.

<sup>10</sup> Opinion 01-03, at 29 (summarizing a stakeholder’s comments).

<sup>11</sup> *Id.* at 2, n.3.

comprehensively address the evolution of EDI processes.<sup>12</sup> Just like with EDI, “an understanding of the interrelationships between business rules, operating practices and information technology is critical to the development of a policy framework for the implementation of” cybersecurity.<sup>13</sup> Accordingly, the CWG should include a cross disciplinary mix that ensures that the impact of any proposed changes can be understood from a technical, business and regulatory perspective.

In addition, the integration of cybersecurity protocols into existing processes is a complex commercial and technical exercise. From a practical perspective, all parties would benefit from the opportunity to receive input from other stakeholders in a centralized setting instead of through communications with individual parties, which inherently leads to a lack of consistency. As evidenced by the discussions during the stakeholder meeting, no one stakeholder or group of stakeholders has a complete understanding of the current business rules and transaction sets or can adequately represent the impact of proposed cybersecurity standards on all other stakeholders. A CWG modeled after the current EDI Collaborative would provide a process for stakeholder discussion in a manner that ensures the people with the necessary expertise are involved and that allows for a free exchange of ideas and more informed discussion than one-on-one negotiations or a more formal regulatory proceeding can provide. Cybersecurity protocols that are structurally comprehensive and well-informed will also benefit consumers by ensuring that customer information is adequately protected.

Moreover, requiring the CWG to file a report with its recommendations with the Commission for review and approval, like is currently done by the EDI Collaborative, will

---

<sup>12</sup> See, generally, Case 12-M-0476, *Proceeding on Motion of the Commission to Assess Certain Aspects of the Residential and Small Non-residential Retail Energy Markets in New York State* (established October 19, 2012).

<sup>13</sup> See Opinion 00-05, at 1-2.

promote fundamental fairness. The DSAs and Attestations as proposed have terms and requirements embedded within them that will have the effect of setting precedent on many important issues, including standards for information security programs and insurance requirements, to name a couple. Cybersecurity standards of general applicability should be subject to Commission review and approval.<sup>14</sup>

Furthermore, it is RESA's understanding that the Joint Utilities believe they have the authority, pursuant to section 2(F)(a) of the Uniform Business Practices ("UBP"), to discontinue an ESCO's participation in their retail access programs if that ESCO refuses to complete the Attestation and/or sign the DSA. If that is the case (which RESA disputes), the utilities should not simply be permitted to require the ESCOs to abide by whatever requirements they propose. Under this paradigm, the utilities could unilaterally require that ESCOs enter into DSAs that they have drafted and then deny ESCOs continued participation in their retail access program if they refuse to do so. However, before ESCOs are potentially deprived of their continued ability to serve customers in any particular utility service territory, fundamental fairness dictates that the requirements that the utilities impose should be subject to review and approval by the Commission to ensure that, at a minimum, they are not arbitrary and capricious.<sup>15</sup> Accordingly, RESA requests that the Commission establish a CWG modeled after the EDI Collaborative that provides stakeholders an opportunity to evaluate and recommend standards subject to

---

<sup>14</sup> Cf. State Administrative Procedure Act, Article 2 (requiring certain procedural protections before the adoption of "the whole or part of each agency statement, regulation or code of general applicability . . .").

<sup>15</sup> Cf. *Mobarak v. Xyz Two Way Radio Service Inc.*, 2006 NYLJ LEXIS 3099 (Supreme Court, Kings County 2006), \*8 ("This rule comports with the notion that . . . an individual is to be free from arbitrary and capricious rules . . . Accordingly, the lack of fundamental fairness in a disciplinary proceeding . . . may result in a finding . . . that the resulting decision was arbitrary and capricious."); *Lindemann v. American Horse Shows Ass'n*, 164 Misc. 2d 937, 949 (Supreme Court, New York County 1994) ("The arbitrary action of a private association is not immune from judicial scrutiny . . . where there is a showing of 'economic necessity' for membership and 'monopoly power' over the profession") (quoting *Jacobson v. New York Racing Ass'n*, 33 N.Y.2d 144, 150 (1973)).

Commission review and approval and avoids giving one set of stakeholders the unilateral and unfettered power to both establish and enforce standards to which their competitors will be subject. In this way, the Commission can promote a free exchange of ideas while ensuring fundamental fairness to all stakeholders.

### III. THE EDI COLLABORATIVE ESTABLISHED A MODEL FOR A CWG

In Opinion 01-03, the Commission directed the utilities and ESCOs to implement EDI systems to ensure uniformity in their business communications.<sup>16</sup> Since 2002, numerous transaction set standards have been effectively and efficiently developed, adopted and implemented.<sup>17</sup> Once a data standard is adopted by the Commission, the standard remains “in place until there is a request to modify the standard to support a new initiative or resolve processing concerns raised by market participants.”<sup>18</sup> Over time, the Commission has approved modifications in EDI transaction set standards and related test plans as necessary, *inter alia*, “to accommodate changes in retail access market structure or at the request of specific parties.”<sup>19</sup> Given the speed of technological advancement, RESA anticipates that fairly regular modifications to the cybersecurity standards established in the DSAs will be required. The EDI Collaborative model provides an organized and productive forum for the sharing of commercial and technical ideas and is instrumental in consensus building amongst stakeholders before modification recommendations are submitted to the Commission for review and approval. Thus, RESA recommends that the Commission model a CWG on the EDI Collaborative.

---

<sup>16</sup> See, generally, Opinion 01-03.

<sup>17</sup> See Electronic Data Interchange (EDI) - Standards & Working Group (available at: <http://www3.dps.ny.gov/W/PSCWeb.nsf/ArticlesByTitle/6806CF784702477285257EC4005698D8?OpenDocument>) (“EDI Website”).

<sup>18</sup> Opinion 01-03, at 43.

<sup>19</sup> Case 98-M-0667, *In the Matter of Electronic Data Interchange*, Order Modifying Electronic Data Interchange (EDI) Standards and Test Plans for Utility Bill Ready Billing (Issued and Effective August 26, 2009) (“Aug. 2009 Order”), at 1.



First, the CWG should be established by a Commission order that sets forth the scope of its authority and the steps that must be undertaken to propose a change to cybersecurity protocols and practices, the DSA or Attestation.<sup>20</sup> By setting forth these requirements in an order, the Commission can ensure that a uniform process is employed for all such changes and that all stakeholders, including new market entrants, are aware of the CWG and its role.

Second, the CWG should be structured and run similar to the EDI Collaborative. As with the collaborative, Staff should participate in the CWG meetings. Staff's attendance at such meetings provides for the opportunity to receive detailed feedback on proposals before a report and recommendations are submitted to the Commission.<sup>21</sup> The CWG should also meet on a regular basis; in the beginning, at least monthly to ensure that any incremental concerns or issues that arise as the DSAs are finalized and implemented are addressed in a relatively expedient fashion. Each meeting of the CWG should include a detailed agenda, meeting minutes and copies of all meeting materials.<sup>22</sup> The CWG should also have a dedicated webpage similar to that of the EDI Collaborative that provides market participants with access to key documents and meeting materials.<sup>23</sup>

Lastly, for the reasons discussed more fully above,<sup>24</sup> as with the EDI Collaborative, the CWG should be required to submit a report and recommendations, including any necessary

---

<sup>20</sup> See Opinion 01-03, at 43 (noting that Change Control process established “to ensure that EDI data standards are kept current.”).

<sup>21</sup> See, e.g., EDI Collaborative, Final Meeting Minutes (Apr. 11, 2014), at 1 (“Staff said that it will send feedback...to the Business Working Group on the open issues when it becomes available.”).

<sup>22</sup> See EDI Website.

<sup>23</sup> See, generally, *id.*

<sup>24</sup> See Section II *supra*.

implementing documents,<sup>25</sup> to the Commission for review and approval. To ensure that all stakeholders are given adequate opportunity to provide input, the recommendations should then be subject to public comment.<sup>26</sup> Once the comment period has concluded, the Commission should issue an order memorializing the changes so that all stakeholders, including new market entrants, are aware of the standards.<sup>27</sup>

By establishing a CWG that is modeled on the EDI Collaborative, the Commission can easily and quickly establish a forum for an open exchange of ideas and consensus building that will provide an effective and efficient process for addressing the rapidly changing cyber landscape and its impact on “business rules, operating practices and information technology.”<sup>28</sup>

## CONCLUSION

For all the foregoing reasons, RESA respectfully requests that the Commission issue an order forming a CWG modeled on the EDI Collaborative as soon as practicable.

---

<sup>25</sup> Aug. 2009 Order, at 1, n.2 (noting that an EDI “transaction set standard is normally comprised of an implementation guide (technical rules associated with a transaction), a data dictionary (clarifying the unique use of data segments or elements by specific parties) and a business process document.”).

<sup>26</sup> *Cf. id.* at 2-3 (noting that an opportunity for comment on the proposed EDI changes was provided).

<sup>27</sup> *See* EDI Website (providing copies of EDI orders issued by the Commission).

<sup>28</sup> *Cf. Opinion 00-05*, at 1-2; *see also id.*, Attachment B, § 7.3 (discussing an EDI Collaborative Change Control subgroup to provide “a process to modify, test and implement necessary changes in data standards in an efficient, effective, timely, and well-coordinated manner.”).

Respectfully submitted,  
RETAIL ENERGY SUPPLY ASSOCIATION

By:   
Joey Lee Miranda  
Robinson & Cole LLP  
280 Trumbull Street  
Hartford, CT 06103  
Phone: (860)-275-8227  
Fax: (860)-275-8299  
E-mail: [jmiranda@rc.com](mailto:jmiranda@rc.com)

Dated: August 28, 2018