



April 22, 2019

Hon. Kathleen H. Burgess  
New York Public Service Commission  
Three Empire State Plaza  
Albany, New York 12223-1350

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

CASE 18-M-0084, In the Matter of a Comprehensive Energy Efficiency Initiative.

CASE 16-M-0411, In the Matter of Distributed System Implementation Plans.

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

Dear Secretary Burgess:

Blueprint Power Technologies, Inc (Blueprint) submits the following comments on the Data Security Agreements and Self-Attestation Forms proposed by the Joint Utilities of New York to apply to DER Suppliers under the Distributed Energy Resource Suppliers Uniform Business Practices.

We appreciate your consideration of these comments. Please do not hesitate to contact us should you have any questions or require additional information regarding this filing.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "R. Beavers", written in a cursive style.

Robyn Beavers,  
CEO  
Blueprint Power Technologies, Inc.



BEFORE THE  
STATE OF NEW YORK  
PUBLIC SERVICE COMMISSION

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

18-M-0376

COMMENTS OF BLUEPRINT POWER TECHNOLOGIES ON  
NOTICE SOLICITING COMMENTS  
(Issued February 20, 2019)

Blueprint Power is focused on selling surplus power from buildings to new electricity customers. A key aspect of Blueprint's operations has been to go beyond the underlying technology challenge and concentrate on ingraining military and intelligence security practices into the ethos of the company. As such, we recognize the key role of a document such as the DSA is to drive consistent control and frameworks across all Energy Service Entities (ESEs) in order to ensure enhanced security practices are put into place. Therefore, Blueprint would like to respectfully submit comments, as solicited, to improve clarity and rigor to the overall development of data security standards for our industry.

Per the referenced solicitation of comments, issued February 20, 2019, the Joint Utilities have filed a petition to the Commission on affirming their authority to require and enforce the execution of the Data Security Agreement (DSA) by entities seeking access to the utility customer data or utility systems. Although it has been proposed, and justifiably so, that cybersecurity standards be applied, a specific set of standards have yet to be identified. By making reference to numerous standards, the DSA leaves open the very real possibility of inconsistencies across the grid thereby resulting in security risks and interoperability issues. Evidence of this contention follows.

The DSA defines "Data Protection Requirements" as follows:

*"Data Protection Requirements" means, collectively, (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.*

It is not comprehensible that the DSA refers to such a wide range of "requirements" as suggested by the definition above. Although there are some overlap and traceability, it would still be arduous and untenable to meet all the cited requirements and provide evidence that they have indeed been met. If, however, it is intended that the identified standards are

examples (“such as”), then inconsistencies and varying levels of security could result. Three examples of inconsistencies across “example” requirements follow:

(1) Audit log content

NIST SP 800-53	ISO 27001
The system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring

(2) Timestamps

NIST SP 800-53	Top 20 Critical Control
Record time stamps for audit records that can be mapped to Coordinated Universal Time or Greenwich Mean Time	Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

(3) Default Passwords

Top 20 Critical Control	ISO 27001
Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.	<i>Silent on default passwords.</i>

Although Blueprint Power is encouraged by the appropriate request by the Joint Utilities that the Commission adopt a framework for further development of the DSA, which is expected to evolve as technology and cybersecurity standards evolve, an initial evolution of the DSA should take place in the near-term to establish a strong framework capable of adequately addressing

future technology and threats. As such, it is our opinion that further evolution should take place prior to the Commission's affirmation of the DSA in its current form.

Additionally, Blueprint Power 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's programs that may occur as a consequence of an audit. Confirmation by the Commission to allow this discontinuance should only occur subsequent to the establishment of a clearly characterized, risk-based system approach to achieving system security across the energy marketplace.

The "Audit" definition section of the DSA, which reads as cited below, refers to "all applicable Data Protection Requirements" so is thus fraught with inconsistency, unintelligibility, and unpredictability that is requisite to managing auditor expectations. The focus should be placed on risk management, not the audit.

*Audit. Upon thirty (30) days notice to ESE, ESE shall, and shall require its Third Party Representatives to permit Utility, its auditors, designated representatives, to audit and inspect, at Utility's sole expense (except as otherwise provided in this Agreement), and provided that the audit may occur no more often than once per twelve (12) month period (unless otherwise required by Utility's regulators). The audit may include (A) the facilities of ESE and ESE's Third-Party Representatives where Confidential Utility Information is Processed by or on behalf of ESE; (B) any computerized or paper systems used to Process Confidential Utility Information; and (C) ESE's security practices and procedures, facilities, resources, plans, procedures, and books and records relating to the privacy and security of Confidential Utility Information. Such audit rights shall be limited to verifying ESE's compliance with this Agreement, including all applicable Data Protection Requirements. If the ESE provides a SOC II report or its equivalent to the Utility, or commits to complete an independent third-party audit of ESE's compliance with this Agreement acceptable to the Utility at ESE's sole expense, within one hundred eighty (180) days, no Utility audit is necessary absent a Data Security Incident. AnAny audit must be subject to confidentiality and non-disclosure requirements set forth in Section 6 of this Agreement. Utility shall provide ESE with a report of its findings as a result of any audit carried out by or on behalf of Utility. ESE shall, within thirty (30) days, or within a reasonable time period agreed upon in writing between the ESE and Utility, correct any deficiencies identified by Utility, and provide the SOC II audit report or its equivalent or the report produced by the independent auditor to the Utility and provide a report regarding the timing and correction of identified deficiencies to the Utility.*

Lastly, consideration should be given to establishing NIST SP 800-171 as the cybersecurity standard since it traces well to the other standards cited in the DSA and is specifically intended for non-federal systems. NIST SP 800-53, which is used today, also has viability. Both standards have well-defined guidance for meeting and verifying the requirements (aka Controls) such that the audit process can proceed most expediently. The key is to select a single standard that is understandable, implementable and provides the requisite level of security. Paramount to the above discussion is the determination of what specific criteria must be established to:

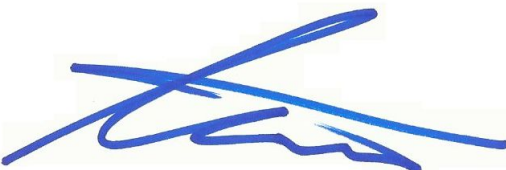
1. Ensure the necessary security across the grid
2. Guarantee a reasonable, cost-effective audit process

Respectfully submitted,

Nicholas Schmidt

Chief Technology Officer & Director of Security

Email: [nschmidt@blueprintpower.com](mailto:nschmidt@blueprintpower.com)

A handwritten signature in blue ink, consisting of several overlapping, fluid strokes that form a stylized representation of the name Nicholas Schmidt.

Dated: April 22, 2019  
New York, NY