CASE 20-M-0082 – In the Matter of Strategic Use of Energy Related Data

DEPARTMENT OF PUBLIC SERVICE STAFF WHITEPAPER REGARDING A DATA ACCESS FRAMEWORK

Dated May 29, 2020

Table of Contents

1. The Path Forward – Statewide Data Access Framework

Increasing the availability of, and appropriate access to, system and customer energy usage data, has long been a priority of the Public Service Commission (Commission). Useful access to useful energy-related data is key to implementing REV[1] and the Governor's clean energy policies. While the ability of market participants to deliver smart economically sound energy solutions to meet New York's clean energy goals depends on their ability to obtain access to useful data, it is critical to protect information technology (IT) and data systems against cyber and other risks, to ensure the protection of customers' privacy, especially as relates to sensitive data, and to preserve customer control over his or her energy usage data (as the owners of the data) including control over access to that data, based on consent. This whitepaper and this proceeding will lay out approaches that serve the principle of useful access to useful energy-related data while simultaneously ensuring that cybersecurity requirements are followed and customer privacy is protected.

Data-related topics have been addressed across numerous Commission proceedings in recent years. In its Accelerated EE Order,[2] for example, the Commission, announced that a new, comprehensive data proceeding would be instituted. The Commission established guiding principles to serve as foundational elements for developing policies that appropriately balance privacy concerns with the rapidly changing energy marketplace, including: (1) increasing customers' familiarity with, and consent to, appropriate data sharing; (2) a movement towards improved access by an Energy Service Entity (ESE) to customer energy-related data, consistent with consent;[3] (3) linking energy-related data with other sources of building data, energy use drivers, and energy systems data to enable enhanced identification of Energy Efficiency/ Distributed Energy Resource (DER) opportunities; and (4) ensuring that the mechanisms for appropriate access to energy-related data are implemented in a useful, timely, and quality-assured manner.

The Commission in its *Order Instituting Proceeding*, issued March 19, 2020 in this case, reinforced its view that existing requirements related to data access are inconsistently applied and lack clarity.[4] The Commission therefore directed the establishment of a "Data Access Framework" that clearly defines the process for access to customer energy-related data and standardizes the necessary privacy, cybersecurity, and quality requirements for data access to ensure uniform treatment across various

---

1 Case 14-M-0101, Proceeding on Motion of the Commission in Regard to Reforming the Energy Vision, (issued April 24, 2014) (REV).

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

3 Any entity (including, but not limited to, ESCOs, DERs, and CCA Administrators) seeking access to energy related data. In limited circumstances, the utility may also be an ESE.

4 Case 20-M-0082, Proceeding on Motion of the Commission Regarding Strategic Use of Energy Related Data, Order Instituting Proceeding (issued March 19, 2020).

energy-related data use cases. In addition, the Commission stated that the Data Access Framework shall include the development of metrics regarding quality and accuracy of energy-related data. It directed Staff of the Department of Public Service (Staff) to, within 60 days of the date of the Order, file a whitepaper consistent with the objectives stated above.

As proposed by Staff, the Data Access Framework would serve as a single source for data access policies and provides uniform and consistent guidance on what is needed for access to, and the availability of, energy-related data. In addition, the proposed Data Access Framework would provide a more workable approach that is designed to provide access to data, while preserving all the necessary protections, to fully enable the intentions of the Commission.

To accomplish these outcomes, the proposed Data Access Framework endorses the risk-based approach to managing the cybersecurity and privacy risks associated with allowing access to energy-related data. Adoption of a risk-based approach would provide a standardized process, along with specified requirements defined by the access and data type, while still ensuring the necessary protections are in place. The proposed Data Access Framework also recognizes the customer's right to access and share his or her data and enables useful access to useful energy-related data by ESEs. In order to fully optimize the benefits of useful access to data, customers must be made aware of their rights to control and share their energy-related data in the simplest and most seamless manner. Customers should be enabled to understand the true value of their data and how a simple act of informed consent correlates directly to meeting their own interests and those of the State. This whitepaper includes a proposal to develop a customer consent mechanism that facilitates a customer's ability to easily consent to share useful energy data in a manner that protects personal privacy.

To ensure that ESEs seeking access to energy-related data have instituted the necessary cybersecurity and privacy protections, the proposal includes implementation of an ESE risk management program that would provide certification of an ESE's readiness to access data. The proposed Data Ready Certification process: (i) includes verification that the ESE is authorized by the Department of Public Service (DPS or Department); (ii) requires the ESE to detail access consideration information - purpose, transmittal mechanism, and data sets; and (iii) validates that the appropriate cybersecurity and privacy requirements are in place by relying on a charting of the existing cybersecurity and privacy requirements and how they apply to the various combinations of purpose, access mechanism, and data. Creation of such a cybersecurity and privacy requirement matrix requires a detailed examination of all existing requirements, accounting for duplicative and inconsistent requirements, and evaluation of correct risk assignment. Once an ESE is certified as "Data Ready," the ESE can request access to data from any data custodian, without having to access each data custodian's process. Certification as Data Ready enables the data custodian to efficiently determine the data an ESE has been certified to access, and by what means. The Data Ready certification has the potential to speed up the ESE verification process, enable access to data in a manner that assures the ESE has the necessary protections in place, and provide a consistent understanding and implementation of the Data Access Framework.

In Summary, this whitepaper details a proposed Data Access Framework that:

- Provides standard definitions of key data-related terms.

- Provides a consistent path to harmonizing existing approaches that have arisen in multiple contexts and Commission proceedings, while also improving achievement of the goals of useful and protective access to useful energy data.

- Identifies the rules, roles, and responsibilities for parties seeking access to energy-related data and ensures uniform treatment of energy data access requests, regardless of where the data are being housed, which provides certainty to customers, utilities, and ESEs.

- Is foundational in that an ESE must be deemed suitable before it can be granted access to energy-related data. To be deemed suitable, an entity would need to satisfy the necessary DPS requirements to become an authorized ESE that is able to request access energy usage data.

- Requires that requests for access to energy data must be proper with regard to purpose, transmittal, and data sets. In this regard, the whitepaper differentiates between categories of data as follows:
    - Highly confidential personal information, as defined in this whitepaper, and similarly sensitive data, should never be shared.
    - Other data, which is enumerated in this whitepaper, is appropriate to share – upon consent or Commission Order, State, Federal, and Local Laws or regulation.
    - Anonymized data presents far fewer privacy concerns and thus fewer requirements for consent.

- Supports the findings in the Commission's Cybersecurity Order,[5] including that the necessary cybersecurity and privacy protections must be commensurate to the risk associated with the data being shared and the way it is being accessed. In this respect, the whitepaper proposes:
    - Consolidation of existing cybersecurity and privacy protections into a matrix that determines the appropriate requirements based upon the risk presented.
    - A proposed Data Ready Certification program to confirm the ESE has implemented the appropriate requirements.

- Gives practical meaning to customer control of energy-related data and recognizes that customers need simple, practical, yet still protective approaches to granting informed consent.

- Recognizes that access to data is moot without assurance of quality, integrity, and timeliness of the data when provided by a utility or other data custodian.

[5] Case 18-M-0376, Proceeding on Motion of the Commission Regarding Cybersecurity Protocols and Protections in the Energy Market Place, Order Establishing Minimum Cybersecurity and Privacy Protections and Making Other Findings (Issued October 17, 2019) (Cybersecurity Order).

- Creates an easy to understand *Data Access Framework Application Guide* that outlines the necessary steps to obtain access to energy-related data in a uniform and consistent manner.

2. Useful Access to Useful Energy Data – Actions and Outcomes

The Commission has taken many actions to enable access to energy-related data. Based on Staff's review, however, the ESE's ability to gain access to customer and system data remains inhibited predominantly due to unclear access requirements, data quality and integrity, and cybersecurity and privacy concerns. Some of these programs were adopted prior to advancements in computer-based technologies, while others were adopted with the sole focus on the risks inherent in the simple transfer of information via IT systems. The process by which the Commission has adopted the policies, however, has resulted in a piecemeal approach to the addressing these data access issues. The proposed Data Access Framework in this whitepaper would incorporate existing Commission-established data access policies and requirements to create a universal statewide data access process that enables useful access to useful data while still preserving protection of IT systems and the data they house.

2.1. Enabling Access to Data

REV Track 1 and Track 2 Orders

Approximately five years ago, the Commission recognized in its REV Track 1 Order that effective DER markets required a framework that enables customers and third parties to become active participants in the planning, management and operation of the electric system.[6] The Commission understood that, to incentivize effective DER markets, utilities would need to revolutionize their communication and data management capabilities. Accordingly, the REV Track 1 Order required each utility, as the Distributed System Platform (DSP), to file a Distribution System Implementation Plan (DSIP).

The Commission reiterated in its REV Track 2 Order that ready access to information regarding customer energy usage is vital to the success of the DER market.[7] The Commission specified that a utility's satisfactory performance of its DSP function would rely in part on its success in facilitating customer engagement regarding access to data and connecting customers with ESEs.

[6] Case 14-M-0101, supra, Order Adopting Regulatory Policy Data access policy and Implementation Plan (issued February 26,2015) (REV Track 1 Order).

[7] Case 14-M-0101, supra, Order Adopting a Ratemaking and Utility Revenues Model Policy Data access policy (issued May 19, 2016) (REV Track 2 Order).

Distributed System Implementation Plans

In April 2016, the Commission adopted the DSIP Guidance Order, which provided greater detail with respect to the DSIP filing process and the contents of the DSIP filings pertaining to both customer and system data.[8] The utilities' subsequent biennial DSIP filings describe their current status and future plans for timely and efficient sharing of useful data.

With respect to customer data access, the DSIP Guidance Order required each utility with Advanced Metering Infrastructure (AMI) deployment plans to submit a proposed implementation plan, budget, and timeline for implementing Green Button Connect (GBC) or an alternate standard that offers similar functionality.[9] The Commission directed the utilities without AMI deployment plans to identify other tools that could be used to enable customer and authorized third-party access to customer data, as well as implementation plans, budgets, and timelines. The Commission also encouraged utilities to include GBC implementation plans for rolling out AMI.

Staff provided the utilities with more detailed DSIP guidance in a May 2018 whitepaper,[10] further emphasizing the importance of customer and distribution system data, stating that, "maintaining a full and timely exchange of DSIP information between the utilities and market participants is critical to achieving the most beneficial deployment and use of DERs. Key areas of emphasis should include: the purposeful development of market participant tools and information sources useful to DER providers in fostering productive DER development; collecting, managing, and sharing system and customer data; and, advances toward an integrated planning environment."

Green Button Connect Implementation

The Commission again addressed GBC within the Accelerated EE Order,[11] in which it recognized that irrespective of the fact that the rollout of AMI is not expected to be completed for several more years, utilities should try to include GBC implementation plans in their DSIPs, as well as AMI rollout plans. The Accelerated EE Order noted that monthly customer usage, available with current metering, is useful to

[8] Case 16-M-0411, In the Matter of Distributed System Implementation Plans, Order Adopting Distributed System Implementation Plan Guidance (issued April 20, 2016) (DSIP Guidance Order).

[9] Green Button Connect (GBC) is a widely recognized and well-accepted method of providing customers access to their energy usage data and enabling customers to consent to the provision of their energy consumption data to one or more third parties.

[10] Case 16-M-0411, supra, DPS Staff Whitepaper, Guidance for 2018 DSIP Updates (filed May 24,2018) (2018 DSIP Guidance).

[11] Case 18-M-0084, supra, Order Adopting Accelerated Energy Efficiency Targets (Issued December 13, 2018) (Accelerated EE Order).

potential ESEs, and directed utilities to expedite their implementation of GBC to enable ESEs to gain access to customers' monthly data.

Despite the Commission's direction to expedite the implementation of GBC, to date only Consolidated Edison Company of New York, Inc. (Con Edison) and Orange & Rockland Utilities, Inc. (O&R) have fully implemented GBC. As reported within the Joint Utilities' October 16, 2019 Status Report on Green Button Connect My Data,[12] even within these two utilities, only three ESEs have been able to successfully complete the necessary steps of the onboarding process allowing them to receive customer data and be identified as an available ESE with whom customers can consent to share their data. Additionally, one of the three ESEs that completed the process asserted that they were unable to utilize GBC because the utility implementation of GBC was not developed consistent with the GBC Standard. For its part, Con Edison reported that, from the time period between April to October 2019, only 362 of its customers had shared data via GBC.[13] The small number of onboarded ESEs and customers who have utilized GBC to date demonstrates that Con Edison's and O&R's GBC implementation have not produced the anticipated benefits.

In sum, inconsistent GBC implementation by the utilities, ESE onboarding problems, and the lack of ease for a customer to find and use GBC have resulted in GBC being utilized at rates far below what the Commission envisioned in the DSIP Guidance and Accelerated EE Orders.

Community Choice Aggregation

CCA programs allow municipalities to procure energy supply services and DER products for eligible energy customers in their communities. By pooling demand, communities aggregate the load necessary to negotiate a supply contract with private suppliers. To commence a CCA, a CCA Administrator must receive three different types of data from the utility - aggregated data, customer contact information,

[12] The Joint Utilities' October 16, 2019, Updated Joint Utility Green Button Connect Report provides the following status of each utilities GBC Implementation. Con Edison and O&R launched GBC on December 19, 2017, and the first ESE was successfully onboarded on December 12, 1018. Their customers can currently share their energy data with three ESEs, with ten additional ESEs in various stages of the onboarding process. Central Hudson Gas & Electric Corporation (Central Hudson) does not offer GBC but offers Green Button Download My Data. Niagara Mohawk Power Corporation d/b/a National Grid (National Grid) is currently planning to implement GBC for its electric and gas customers by March 31, 2021. New York State Electric & Gas Corporation (NYSEG) allowed customers to use GBC using a third-party vendor as part of its Energy Smart Community (ESC) Energy Manager pilot. Customers in the ESC were temporarily able to use GBC to share energy usage data with six approved ESEs. NYSEG and Rochester Gas and Electric Corporation's (RG&E) full implementation of GBC as part of their Energy Manager Web Portal is subject to the Commission's approval of the Companies' AMI proposal in their ongoing rate proceeding in Cases 19-E-0378 et al.

[13] Case 16-E-0060 et al., AMI Metrics Report (filed October 31, 2019).

and detailed customer usage data. These datasets must be transferred to a CCA from the utility before a CCA can begin to supply energy to its members. Utilities are responsible to transfer the aggregated customer and usage data within twenty days of a request from the municipality or the CCA Administrator. At this time, the 15/15 privacy screen is applied to the CCA aggregated data.[14] After each municipality has entered into a CCA contract with an Energy Service Company (ESCO), the utility transfers the customer-specific data to the municipality or CCA Administrator within five days of a request to support the mailing of opt-out notices. After the opt-out period has ended, the municipality or the ESCO may submit a request to the utility for detailed customer data, including energy usage data, for customers consistent with existing Electronic Data Interchange (EDI) protocols.

CCA Administrators continue to notify Staff of data access problems they encounter with utilities, including the failure to provide data within the Commission adopted timeframes, the inaccuracy and inconsistency of the data, and problems with the privacy screens. Understanding that the Commission adopted the CCA program only a few years ago and that some utilities are unaccustomed to this type of data compilation, Staff has been working with both CCA Administrators and utilities to resolve these data issues.

Utility Energy Registry

On April 20, 2018, the Commission issued an Order approving the development and implementation of the Utility Energy Registry (UER).[15] The UER is an online public platform developed and maintained by the New York State Energy Research and Development Authority (NYSERDA), with the support of the investor-owned gas and electric distribution utilities, to provide streamlined public access to aggregated community-scale utility energy data.[16] The UER, as authorized in the UER Order, was a starting point to require continuing Commission oversight and refinement and was understood as a platform that would evolve over time.

Semiannually, utilities report monthly aggregated data that populates maps of municipalities and counties statewide, and zip codes in the New York City metropolitan area. Following additional privacy standards adopted by the Commission in the UER Order, utilities withhold data in locations with limited

[14] By the DSIP Order, the Commission adopted a 15/15 standard for aggregated data set use cases which established that an aggregated data set may be shared only if it contains at least 15 customers, with no single customer representing more than 15 percent of the total load for the group and adopted a whole building energy data aggregation standard of 4/50 that established an aggregated data set may be shared only if it contains at least 4 customers, with no single customer representing more than 50 percent of the total load for the group.

[15] Case 17-M-0315, In the Matter of the Utility Energy Registry, Order Adopting Utility Energy Registry (issued April 20, 2018) (UER Order).

[16] Available at: https://utilityregistry.org.

numbers of customers to protect consumer privacy.[17] The UER now contains four years (2016-2019) of monthly electricity and natural gas data for 1,300+ municipalities. The public can visualize data and download it in Comma Separated Values (CSV) format. All data are associated with a Census code so communities can look at energy performance against demographic drivers.

On December 30, 2019, NYSERDA filed a UER Status Report (Report) prepared by Climate Action Associates, LLC to report on the progress of the UER's implementation and operation, including the demand for, and uses and benefits of UER data, as well as the need for refinements.[18] Some of the proposed modifications within the Report include restructuring the existing data fields and increasing access to data by recommending modification to the privacy screen to rely solely on a customer count. The Commission is expected to act on the recommendations contained within the Report in a future order.

Building Benchmarking

The Accelerated EE Order recognized benchmarking of building energy performance as an important market enabling mechanism to provide energy users information about how their consumption compares with peer buildings. New York City began requiring benchmarking and disclosure of energy and water usage in 2009 through Local Law 84, and cities in other states have also implemented this requirement.[19] Local Law 84 requires utilities serving New York City to establish systems and processes to electronically provide aggregated metered consumption data for all electric and gas accounts by building to support automated upload to the Energy Star Portfolio Manager.

Given the experience of the downstate utilities, the Commission recognized that the upstate utilities should assess their readiness to support eventual statewide benchmarking. Specifically, the Accelerated EE Order requires the utilities to, upon building owner request, provide aggregated whole building electric and/or gas meter data for any given building or tax lot to an owner, subject to the 4/50 privacy screen established by the Commission, for use in benchmarking through the Energy Star Portfolio Manager. The Accelerated EE Order also requires the utilities to develop the capability to automate the uploading of aggregated data and, in consultation with NYSERDA, a programmatic offering that utilizes benchmarking data to be marketed to decision-makers of suitable building types.

As of 2019, Con Edison, National Grid, KeySpan Gas East Corp. d/b/a National Grid (KEDLI), and Brooklyn Union Gas Company d/b/a National Grid (KEDNY) are the only utilities to have automated upload

[17] Utilities withhold sector data to protect consumer privacy if it fails a count/magnitude screen. The residential sector screen is 15/15. If there are less than 15 accounts, or if one account is more than 15% of the total, the entire sector is withheld. The screen for non-residential sectors is 6/40.

[18] Case 17-M-0315, supra, NYSERDA UER Status Report, (filed December 30,2019).

[19] New York City Local Law 84 of 2009.

capabilities of monthly aggregated whole building data. NYSEG, RG&E, and Central Hudson have each initiated the system integration to be able to provide automated upload capabilities, a process they believe will be completed within the next two years. O&R and National Fuel Gas Distribution Corporation (NFG) have not yet initiated the implementation process to develop the IT capabilities to provide automated upload functionality but are expected to do so in the near term. Regarding programmatic offerings, NYSERDA, along with select utilities, continue to meet with Staff to discuss what would be needed within a successful programmatic offering and are taking steps to identify specific program components.

Utility System Data

Since 2016, each regulated electric utility in New York State has separately implemented, enhanced, expanded, and maintained one or more online portals for sharing useful electric system information with ESEs and other industry market participants. The types and attributes of shared information, and the methods for sharing the information, have been both prescribed directly by the Commission and determined through a Commission-directed market participant engagement process that is led by the Joint Utilities of New York (JU).

The categories of system information currently available online for each utility are as follows:

- Distributed System Implementation Plans (via the DPS Document Matter Management System (DMM)).
- Capital Investment Plans (via the JU web site or the DPS DMM).
- Planned Resiliency/Reliability Projects (via the JU web site or the DPS DMM).
- System Reliability Statistics (via the utility's web sites or the DPS DMM).
- Hosting Capacity (via the individual utility web sites).
- Beneficial Locations for DERs (partially available via the individual utility web sites, the JU web site, or the DPS DMM).
- System Load Forecasts (partially available via the individual utility web sites).
- Historical System Load Data (partially available via the individual utility web sites).
- Opportunities for Non-Wires Alternatives (partially available via the individual utility web sites).
- Distributed Generation Queued for Interconnection (via the DPS web site).
- Installed Distributed Generation (via the DPS web site).
- System Interconnection Request (SIR) Pre-Application Info (via the individual utility web sites).

The system data needed to support innovation and efficiency is not available in the way it was intended. Web links to all the utilities' online system information sources are publicly accessible via the System

Data page of the JU web site.[20] However, the structure, attributes, semantics, availability, and accessibility of the information from many of these sources vary significantly across the utilities. In addition, these sources provide very little of the information related to electric vehicle loads and energy storage as advised in Staff's 2018 DSIP Guidance. Finally, and very importantly, only the few sources pertaining to DER interconnections provide any sort of association between a utility customer and the system infrastructure that serves that customer.

Date Access Fees

The REV Track 2 Order set forth the conditions under which utilities may charge for data that is more granular and/or is requested on a more frequent basis than basic individual customer usage data. The Commission agreed that certain basic levels of information will be free of charge to customers and vendors authorized by the customer, while utilities could charge a fee for provision of more refined data or analysis, such as aggregated data. The Commission understood that the development of providing aggregated data would impose costs on utilities until fully automated systems were developed.

In the CCA Framework Order, the Commissioner permitted utilities to charge a fee for access to aggregated community load data, as well as the customer information needed to facilitate opt-out mailings.[21] In December 2017, the Commission established a uniform fee, for all utilities, of $.80 per account.[22] The fee was apportioned 20% to requests to utilities for aggregated data and 80% to request to utilities for customer lists. CCA Administrators have been paying the data access fees, and complying with all other requirements for data access. However, as previously mentioned, there are significant lag times for receiving the data and questionable quality and accuracy of the data.

In summary, the Commission's actions meant to empower customers' right to share their data and enable market offerings, such as GBC adoption and the data-sharing achievements and plans reported in the DSIPs to-date, have not been successful to this point and have fallen well short of Commission expectations. Avenues for access to system data remain limited and inconsistent between what is available and the paths available for access to that data.

[20] Available at: https://jointutilitiesofny.org/system-data/.

[21] Case 14-M-0224, Proceeding on Motion of the Commission to Enable Community Choice Aggregation Programs, Order Authorizing Framework for Community Choice Aggregation Opt-Out Program (issued April 21, 2016) (CCA Framework Order).

[22] Case 17-M-0315, et al., Order Establishing Community Choice Data Access Fees (issued December 14, 2017).

2.2. The Evolution of Data Access Requirements

The Commission has developed a series of requirement to enable access to energy related date, including those related to cybersecurity and privacy protections, as well as registration requirements. Those requirements and related policies are summarized below.

Uniform Business Practices (UBP)

ESCO UPB

In February 1999, the Commission adopted the Uniform Business Practices (UBP), to provide for consistent business procedures for both ESCOs and electric and natural gas utilities across the state.[23] As the competitive retail energy market has evolved in New York, the UBP has been revisited and modified to reflect changes in the market while continuing to provide consumer protections, streamlined business transactions, and communications protocols between ESCOs and utilities. The ESCO UBP is a comprehensive document that details the requirements and obligations of ESCOs providing service in New York State. It includes information that can be categorized into two main topics: ESCO operation requirements; and ESCO customer requirements. The customer requirements include, among other things, marketing standards and customer data protections.[24]

DER UBP

As part of the REV initiative, the Commission initiated a proceeding to consider the regulation and oversight of DER providers and products.[25] The Commission's experience in regulating ESCOs in the gas and electric supply market demonstrated that DER oversight is required to ensure that customers participating in DER markets and programs understand the costs and benefits of their investments and are protected from confusion, fraud, and abusive marketing practices. The Commission realized that clear, consistent rules and uniform marketing and contracting practices are needed to, among other things, prevent exploitive pricing and deceptive marketing practices to residential and small business customers, ensure that customers and DER suppliers know their rights and responsibilities, and provide oversight tools needed to monitor the growing markets and resolve potential conflicts.

The ESCO UBP and DER UBP (UBPs) have been a necessary, and integral, part of the regulation and oversight of ESCOs and DERs participating in NY markets. Since their inception, the UBPs have been modified to keep pace with market changes. Up to this point, attempts to modify the ESCO UBP have taken an extended amount of time. In particular, changes to the customer requirements have often been delayed due to market participant challenges to the proposed changes of operation requirements.

---

[23] Case 98-M-1343, Retail Access Business Rules, Opinion NO. 99-3, Opinion and Order Concerning Uniform Business Practices (issued February 16, 1999).

[24] UBP ESCO, Section 4.

[25] Case 15-M-0180, In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products.

This delay, in turn, has hampered the Commission's ability to ensure the appropriate customer protections are in place in the context of fast-paced changes in the ESCO and DER markets.

CCA Data Security Agreement

Per the CCA Framework Order,[26] a Data Security Agreement (DSA) is required to be signed by the CCA Administrator, and possibly other parties, before any data can be requested or received for establishing a CCA program. The CCA DSA was a starting point for the development of the ESS DSA that was implemented and required by the utilities for ESEs seeking access to customer-related data.

Cybersecurity and Privacy Protections

The Cybersecurity Order adopted a minimum level of cybersecurity and data privacy requirements for companies that electronically receive and exchange utility housed customer data with the utilities' IT systems, and ensured privacy requirements were in place for those who received customer energy-related data through any means. These protections included requirements from the previously developed DSA and Self-Attestation. The Self-Attestation consists of a 16-point inventory of cybersecurity controls based upon the National Institute of Standards and Technology (NIST) Cybersecurity Framework listing of risk mitigation controls.[27] The contents of the Self-Attestation and DSA were developed by the JU, Staff, and the ESEs in a collaborative, business-to-business process.

These cybersecurity and data privacy requirements provided a universal foundation of protections and ensured the privacy of customer data and protection of the utility IT systems, all while enabling and encouraging data access. The Cybersecurity Order also recognized that there may be certain entities that would be unable to agree to these requirements but would still need access to energy-related data (e.g., New York Power Authority (NYPA) and the State University of New York (SUNY)). The Cybersecurity Order thus allowed for these entities to work with the utilities in modifying the agreement in a way that still ensured the necessary protections were maintained. The baseline cybersecurity and privacy requirements were adopted from the DSAs that were in use by the utilities, which had been based upon the JU-developed Cybersecurity and Data Privacy Risk Strategy.[28]

The Cybersecurity Order recognized that the data belongs to the customer and that customers have a right to direct or consent to the use of that data. The Cybersecurity Order also recognized that it is not

---

[26] Case 14-M-0224, Proceeding on Motion of the Commission to Enable Community Choice Aggregation Programs, Order Authorizing Framework for Community Choice Aggregation Opt-Out Program (issued April 21, 2016).

[27] The utilities identified these requirements as being necessary under NIST Special Publication 800-53.

[28] Case 16-M-0411, supra, Joint Utility Supplemental Distributed System Implementation Plan, (filed November 1,2016) (Supplemental DSIP).

the utilities' business model to audit ESE cybersecurity and privacy programs or to determine compliance. A balance was thus 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, receiving and/or collecting customer data with the utilities and facilitating the dissemination of customer information with customer consent to companies. Ultimately, a market where all parties observe cybersecurity and privacy protections would reduce the risks associated with electronic exchanges of customer data between distribution utilities and companies, instilling customer confidence and promoting market development.

NYSERDA Data Order

In its Order Regarding New York State Energy Research and Development Authority Data Access and Legacy Reporting, the Commission authorized utilities to transfer non-anonymized, non-participant customer data to NYSERDA and established a process for facilitating the data requests while ensuring appropriate protection of the datasets.[29] NYSERDA sought the data transfer to carry out its statutory duties relating to assessment of program and policy goals and the effectiveness of clean energy programs and policies, including potential, baseline, and market-characterization studies, as well as other Evaluation, Measurement, and Verification (EM&V) activities. To effectuate the flow of customer data between the utilities and NYSERDA, the Commission required NYSERDA and the Joint Utilities to develop and file a Memorandum of Understanding (MOU) for the request and transfer of customer data sets for the specifically approved purposes, including non-participant data.[30]

Joint Utility Cybersecurity and Data Privacy Risk Strategy – DSIP Appendix E

The DSIP Guidance Order required the utilities to jointly develop an evolving cybersecurity program that incorporated new technology and updated information regarding threats and countermeasures. Accompanying the JU Supplemental DSIP filing, was Appendix E: Cybersecurity & Privacy Strategy Framework (DSIP Appendix E). This document was reported to be a risk-based approach to

[29] Case 14-M-0094, et al., Order Regarding New York State Energy Research and Development Authority Data Access and Legacy Reporting (issued January 17, 2019).

[30] The Commission affirmed that NYSERDA's data governance protocols and non-disclosure agreements must ensure protection of non-participant datasets received from the utilities held by NYSERDA or its contractors and must ensure that the data requested not be used for the financial gain of any third party and should include appropriate remedies for any data breach. The process prescribed by Commission by which NYSERDA is to request data from a utility requires NYSERDA to: identify the need for data; identify specific data fields, as well as time period, and frequency of refreshing such data set; the planned retention and use of such data; and provide a justification for the need for data. The requested utility must respond with the data or identify why the utility believes the request is not consistent with the permissions provided in the NYSERDA Data Order, detailing the utility's objection to the data set request. Should a utility object to a requested data set, Staff shall review the NYSERDA request and the utility objection and make a determination in response to the objection, which may include approving the request, rejecting it, or approving it with modification.

cybersecurity and privacy that incorporated numerous industry standards,[31] while allowing the flexibility for individual utility implementation. This strategy was used as the utility starting point for adoption of a formal risk management program and the determination of the necessary cybersecurity and privacy requirements for entities seeking access to energy related data and, subsequently, the creation of the DSA.

The development of the individual utility cybersecurity risk management programs, and the determination of requirements, has led to varying implementation strategies. With the differences in utility IT systems the implementation strategies are, understandably, not wholly consistent. The Joint Utilities intended DSIP Appendix E to be flexible enough to account for IT system differences across utilities and allow for individual utility implementation strategies. However, DSIP Appendix E turned out to be overly broad and generic. For example, it lacks concrete guidelines for implementation processes and fails to provide definitions of key terms, which has resulted in significant differences in how utilities define data sets, group data, and assign risk-based requirements. Indeed, most of the ESE complaints focused on this lack of uniformity and ultimately led to the Joint Utilities, Staff, and the ESEs engaging in a collaborative, business-to-business process.

Before issuance of the Cybersecurity Order, the Joint Utilities developed cybersecurity and privacy requirements from the JU risk management program, which became part of the necessary requirements for ESE access to data. While the DSIP Appendix E is a risk-based model and the cybersecurity and privacy controls implemented from it are valid for risk mitigation, Staff believes that the requirements, as applied, do not adequately address the actual risk associated with various types of data access or the customer's choice regarding data sharing.

With the continued disagreement between ESEs and utilities over the reasonableness of cybersecurity and privacy requirements and who they apply to, the Commission adopted in the Cybersecurity Order a minimum level of cybersecurity and privacy protections which were subsequently implemented by the utilities. Since that time, some ESEs have informed Staff of inconsistencies regarding the applicability of these minimum protections across utilities. For example, upon its own review, Staff determined that there are disparities regarding how each utility interprets the Cybersecurity Order with respect to which ESEs are required to have cybersecurity and/or privacy requirements.

In summary, while the various data access rules and requirements are meant to provide the means to safely allow access to energy-related data, the ability of an ESE to gain access to data, and customers'

[31] NIST, NIST Interagency/Internal Reports (NISTIR), Fair Information Practice Principles, Electric Sector Cybersecurity Capability Maturity Model, Department of Energy DataGuard Energy Data Privacy Program, American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standards, and Information Security Forum General Information Security Practices.

ability to share their data, continues to be limited. Based upon its analysis, Staff believes there are several reasons for the limited sharing of energy data, including a lack of standardized requirements and utility implementation strategies, as well as variability between utilities of the requirements for both customers and ESEs to get access to that data.

The ability to obtain useful access to useful data has been largely hampered by:

- Requirements developed in multiple proceedings, some of which are specific to market participants and others that are specific to the data access method, such as GBC. This has led to confusion regarding what requirements apply to whom.
- Difficulties with modifying existing requirements as data access standards evolve resulting in outdated and inconsistent requirements throughout different proceedings.
- Inconsistent interpretation of data access requirements which increases ESE confusion and extends the time necessary to be approved for data access.
- Inconsistent implementation of data access applications or tools across all utilities.
- Inaccurate and/or incomplete data, as well as extended delays in receiving data.
- Lack of customer awareness of their rights to control their data.

3. The Key to Unlocking Useful Access to Useful Data

In order to unlock access to energy-related data in New York, a statewide Data Access Framework must be adopted that incorporates the work from existing data access policies, defines the necessary process and requirements for access to energy-related data, introduces requirements for data quality and integrity to facilitate consistent application throughout the State, and enables access while still providing appropriate protections. The proposed Data Access Framework would provide clear and consistent rules and related implementation, define roles and responsibilities, create confidence in the quality of the data, and ensure that the appropriate entity is accessing data in a secure manner. The proposed Data Access Framework would also address the existing requirements related to customer consent and associated improvements upon them.

Adopting the proposed Data Access Framework would create a single source for data access policies and requirements and provide uniform and consistent guidance on what is needed for access to, and the availability of, energy-related data to better support the purposes of existing data policies, while ensuring the appropriate protections are in place. The proposed Data Access Framework provides clear paths that address the roadblocks described above and establishes the necessary foundation to address any new issues that may arise as markets evolve.

To meet these goals, the Data Access Framework would:

- establish a universal approach for any ESE seeking access to energy-related data that would apply statewide, regardless of utility territory, thus removing the need for utilities to spend time and money on individual ESE risk management processes and oversight;

- provide a clear and consistent ESE data access approval process that better supports the purposes of existing data policies by implementing an ESE risk management model with a Data Ready Certification;
- define key terms, key applicability considerations, and requirements for access;
- incorporate all the separate existing data requirements from the Commission and the utilities into one clear set of requirements that appropriately recognizes risk;
- centralize all existing access requirements and ensure that appropriate cybersecurity and privacy protections are in place to protect IT systems and the data they house; and,
- recognize customers' right to consent to share their energy usage data and encourage customer control of their energy-related data.

The proposed Data Access Framework endorses a risk-based approach to managing cybersecurity and privacy risks associated with allowing access to energy-related data. Adoption of a risk-based approach would provide a standardized process, along with defined requirements, for access to energy-related data, while still ensuring the necessary protections are in place. The Data Access Framework also recognizes customers' right to access and share their useful data and enables useful access to energy-related data by ESEs. The Data Access Framework provides an identification of rules, roles, and responsibilities for parties seeking access to energy-related data and ensures uniform treatment of energy data access requests, regardless of where the data are being housed, which provides certainty to customers, utilities, and ESEs. This Data Access Framework, if adopted by the Commission, would become the guiding document for determining the necessary requirements and process for access to energy-related data going forward.

ESE Risk Management and Data Ready Certification

The proposed Data Access Framework would implement an ESE risk management model, as well as creation of a Data Ready Certification program, managed by an outside party. The Data Ready Certification would require an ESE applying for certification to complete DPS registration requirements, detail access consideration information (purpose, transmittal mechanism, and data sets), and have cybersecurity and privacy requirements verified. Under this approach, once an ESE is certified as Data Ready, the ESE would be in position to request access to data from any data custodian, without having to go through each individual data custodian verification requirements because the data custodian would be able to easily confirm the data to which the ESE has been certified for access, and the means by which the data may be accessed.

Taking these actions would resolve the inconsistent implementation issues identified above, remove the need of ESEs to go through duplicative processes with each utility, significantly speed up the ESE verification process, enable access to data while providing assurance that the ESE has the necessary protections in place, and provide a consistent understanding and implementation of a data access program. This standardized ESE approval process would ensure that, before being approved to access

energy-related data, all ESEs have completed the necessary onboarding requirements and have the appropriate cybersecurity and privacy protections in place.

Currently, when a customer wants to share his or her energy usage data with an ESE, the process, and ease in doing so, varies significantly by utility. The ESE with whom the customer consented to share that data must work through onboarding requirements that have been implemented inconsistently amongst the utilities as well as unclear policies and requirements if they want to get access to that data, and possibly provide a benefit to that customer. Commission actions meant to promote customers' right to share their data and enable market offerings, such as GBC, have not been successful to this point because of these ongoing problems. Instead of the utilities evaluating the necessary requirements and the ESE's readiness to access data, an ESE risk management program, as Staff proposes, would ensure that the appropriate risk mitigation controls are in place to protect IT systems and the data they house, and that the requirements are applied in a consistent manner, regardless of the utility.

As illustrated below, the current process may include multiple steps for any ESE seeking access to energy-related data, which has contributed to the limited availability and sharing of energy-related data. The proposed process reduces the number of steps, provides a consistent and uniform treatment of all parties, while still ensuring the necessary cybersecurity and privacy requirements have been met to protect IT systems and the data they house. The Data Ready Certification approval process detailed below would utilize the existing cybersecurity and privacy protections and streamline the approval process while still ensuring those protections are in place. In other words, while Staff proposes a new certification process for data access, the required cybersecurity and privacy protections are not new. This certification would also implement data relationship requirements that provide necessary data quality and integrity standards.

Current ESE Access Process	Proposed Data Ready Certification Process
1) ESE registers with DPS and completes all requirements under applicable UBP (including privacy and cybersecurity). 2) ESE contacts utility to request access to data. 3) ESE must sign a DSA with utility and provide. Verification. 4) ESE must go through onboarding and connectivity testing with utility. 5) ESE must meet any other utility specific obligations. 6) ESE requests data from utility. 7) ESE receives data from utility. 8) ESE must review the data for consistency and verify integrity. 9) ESE works with utility to correct any data issues. 10) ESE must repeat this process for EACH UTILITY from which it seeks to access data.	1) ESE registers for access: a) Provider verifies applicant is an authorized ESE. b) ESE details purpose, transmittal/access mechanism, and data type. c) Necessary ESE cybersecurity and privacy protections, based upon registration information, are validated. ESE is assigned an Access Role that dictates the data they are approved to access and how they can access it. 2) ESE requests data from data custodian (utility, centralized data warehouse, etc.). 3) Data custodian verifies ESE Access Role. 4) ESE receives data from data custodian that is uniform and correct.

While it is a significant change to the current approval process for an ESE seeking access to energy-related data in New York, an ESE risk management program is not a new concept or model. The United Kingdom (UK) implemented its Cyber Essentials Scheme on October 1, 2014 and made it a mandatory requirement for any entity wanting to bid on any central government contract and, going a step further to try to ensure data protections, the UK recommended its use by private sector organizations.[32] The Cyber Essentials Scheme established a centralized certification process that requires verification of specific cybersecurity and/or privacy requirements which are based upon the information (data) that would be shared. The registration process, verification of requirements, and subsequent certification is done by an outside company, IASME Consortium,[33] that provides a web site listing of certified entities, what data they are permitted to access, and by what means. This listing is then used by governmental procurement personnel for verification that an entity has met the required standards to allow sharing of the data with the entity, all without having to perform audits or monitoring on their own.

As another example, beginning in July 2015, Fannie Mae rolled out a similar certification model, managed by BitSight, that provides a portal with a centralized listing of all the registered and tested third parties.[34] The third parties are assigned a security score and a rating of basic, intermediate, or

[32] Available at: https://www.ncsc.gov.uk/cyberessentials/overview.

[33] Available at: https://iasme.co.uk/cyber-essentials/.

[34] Available at: https://info.bitsight.com/sans-whatworks-case-study-fannie-mae.

advanced, based upon the cybersecurity and privacy requirements the third party has in place. Currently, BitSight is providing third-party vendor risk management services to over 1,700 businesses and reportedly can complete vendor assessments in hours, instead of the weeks it would normally take a business to do it on its own.[35]

The need to ensure the appropriate cybersecurity and privacy protections are in place cannot be understated, but the need to determine the most efficient and expedient means to do so is equally important. Centralizing the requirements, as well as the verification of completion of those requirements, would allow for an efficient and consistent process for ESEs to request, and access, energy-related data. Doing so is intended to both ensure that the appropriate protections are in place and reduce the frustration of ESEs and customers seeking data access. Additionally, by establishing a single process, Staff proposes to reduce the time and cost for utilities associated with the current ESE approval processes that are outside the traditional utility business model. This Data Ready certification process would determine the applicability of existing requirements based upon the ESE's purpose for requesting data access, the transmittal or access mechanism utilized, and the data being requested.

Incorporating all existing data access requirements into one Data Access Framework would eliminate inconsistent implementation and application of data access policies and allow for a true dynamic document that upon modification, applies to all entities seeking access to data. This would address current inconsistency issues with the UBPs as well as the CCA DSA.

The CCA DSA was implemented prior to the Cybersecurity Order, as such, it is no longer wholly consistent with the current standards of what is necessary for data access. While work has begun to modify the CCA DSA to ensure its consistency, a mechanism for expedient changes does not currently exist. Under the proposed Data Access Framework any changes going forward would be applied uniformly to all markets and ESEs, at the time of the change, eliminating these types of problems.

The UBPs, while similar, do have differences in the requirements for obtaining access to customer information, and this inconsistency does not provide for a consistent and uniform level of protection. The DER UBP requires: "DER suppliers that obtain customer information from the distribution utility or DSP must have processes and procedures in place regarding cybersecurity consistent with the National Institute of Standards and Technology Cybersecurity Framework" and "DER suppliers that obtain

[35] Available at: https://www.bitsight.com/security-ratings-vendor-risk-management.

customer information from the distribution utility or DSP must comply with any data security requirements imposed by that utility or by Commission rules on ESCOs and/or any data security requirements associated with EDI eligibility."[36] The ESCO UBP, on the other hand, does not define any necessary cybersecurity requirements, or measures, pertaining to obtaining customer information.[37]

Due to a lack of uniformity in what each utility provides, including how it is provided, Staff has received numerous complaints regarding ESEs first having to standardize the data it received before it can be used. This causes an additional burden upon ESEs seeking access to data by now requiring them to take additional steps in order to make the data useful. Platforms to which the utilities provide data, such as the UER and GBC, have also seen inconsistent data standards and output. As previously discussed, GBC implementation was seen as a way to address these concerns by providing a standardized and uniform means for the sharing of data, but due to inconsistent implementation of GBC, these problems still persist. By establishing data quality and integrity standards, as well as enforcement mechanisms, the significant number of problems related to the inconsistency and quality of the data being provided would be resolved.

The recommendation to create a Data Access Framework Application Guide provides an additional mechanism to ensure clear understanding of what the ESE needs to do to be approved for access, the responsibilities of each party, the dispute resolution process, and defines key terms that will be used throughout all energy-related data proceedings. Customers further benefit by having a known and written set of policies and practices that would be employed by utilities and any ESEs that are authorized to obtain customer data. This includes obtaining a notice from utilities and ESEs when data is requested, a contact person at the utility to ask questions, the ability to obtain his or her own information, and the opportunity to dispute and request changes to his or her information.

4. Proposed Data Access Framework

4.1. Purpose

The purpose of this proposed Data Access Framework is to enable access to, and appropriate use of, energy-related data that enhances customer data protections, furthers the trust relationship between ESEs and consumers, and enables innovation while also avoiding regulatory fragmentation that undermines New York State goals.

[36] UBP DERS, Section 2C(F), (G), p. 10.

[37] UPB ESCO, Section 4.

4.2. Applicability

The proposed Data Access Framework applies to any entity seeking access to energy-related data, regardless of where the data are housed. By the condition of seeking access to energy-related data from the data custodian, ESEs would need to agree to abide by the terms of this proposed Data Access Framework. The Data Access Framework is not intended to modify the way that individual utility customers currently access their specific account data and, as such, does not seek to change, or in any way inhibit, an individual customer's right and ability to access his or her own data.

4.3. Enforcement

If an ESE is not complying with the requirements for data access, there are existing enforcement mechanisms available, such as those in the UBPs, which are tied into the ESE's ability to be an eligible New York State energy service provider. Staff recommends the proposed Data Access Framework incorporate the existing enforcement standards, where possible, to provide one concise enforcement process. Depending on at what point the ESE is non-compliant may determine what the appropriate enforcement mechanism may be. For example, if an ESE is not meeting the necessary requirements for Data Ready Certification, they will not be certified and will not be able to access data. If they are certified but are not complying with DPS requirements, the combined enforcement mechanism would be used to suspend an ESE's Data Ready Certification.

4.4. ESE Data Ready Certification Process

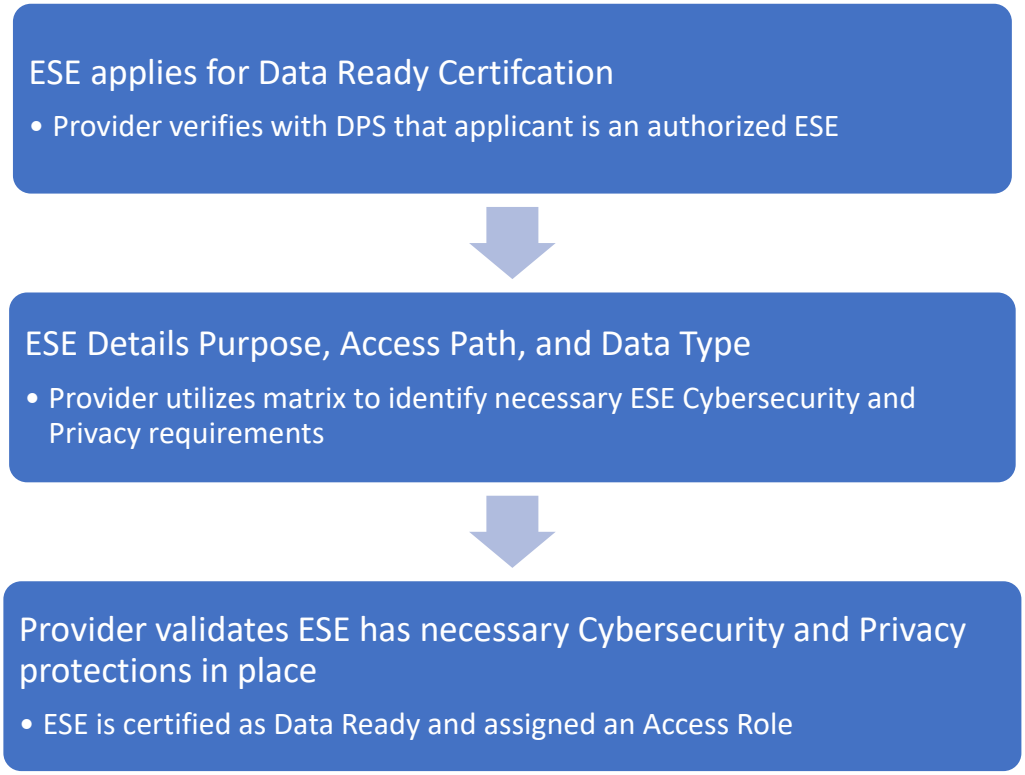
Staff recognizes that there have been challenges for ESEs seeking access to energy-related data. Seeking to address those challenges, Staff proposes an access request process that incorporates all the existing, separate requirements from the Commission and the utilities into one process, and establishes a universal approach for any ESE seeking access to energy-related data that would apply statewide, regardless of utility territory. This process would require verifying that the appropriate cybersecurity and privacy protections are in place, and thus the proposal includes the creation of a Data Ready Certification program. Any entity seeking access to energy-related data, would need to follow the access request process and meet all requirements before being approved and assigned an access role.

Staff recommends implementation of an ESE risk management program that provides a Data Ready Certification. The program is to be managed by a risk management solution provider (Provider) who would build the Data Ready Certification model based upon this proposal. The Provider would utilize a matrix that defines the existing cybersecurity and privacy requirements based upon the ESE access considerations below. The Data Ready Certification would require confirmation/testing that ESE cybersecurity and privacy requirements are in place, which may be done directly with the Provider or as an audit. When an ESE applies for Data Ready Certification, the Provider would only be responsible for confirming all the requirements have been met and would not be determining what those requirements are. The necessary cybersecurity and privacy requirements would be included in the matrix, which will compile all existing requirements, as discussed below. In addition to the verification of the existing

requirements, Staff recommends a requirement for annual re-certification. This would ensure that ESEs are remaining current with the necessary protections. Failure to complete the annual re-certification would result in the ESE losing its certification and, consequently, its ability to access energy-related data.

Once an ESE has completed the requirements for approval, the ESE would be certified as Data Ready. That certification provides the assigned access role which dictates what types of data it may request to access, and how they are able to access it. This certification would apply no matter from which utility, or data custodian, the ESE is seeking to access data. There would no longer be a need for utilities to oversee or confirm the appropriate protections are in place, saving them a significant amount of time and resources that have been dedicated to this type of oversight role.

Data Ready Certification Process



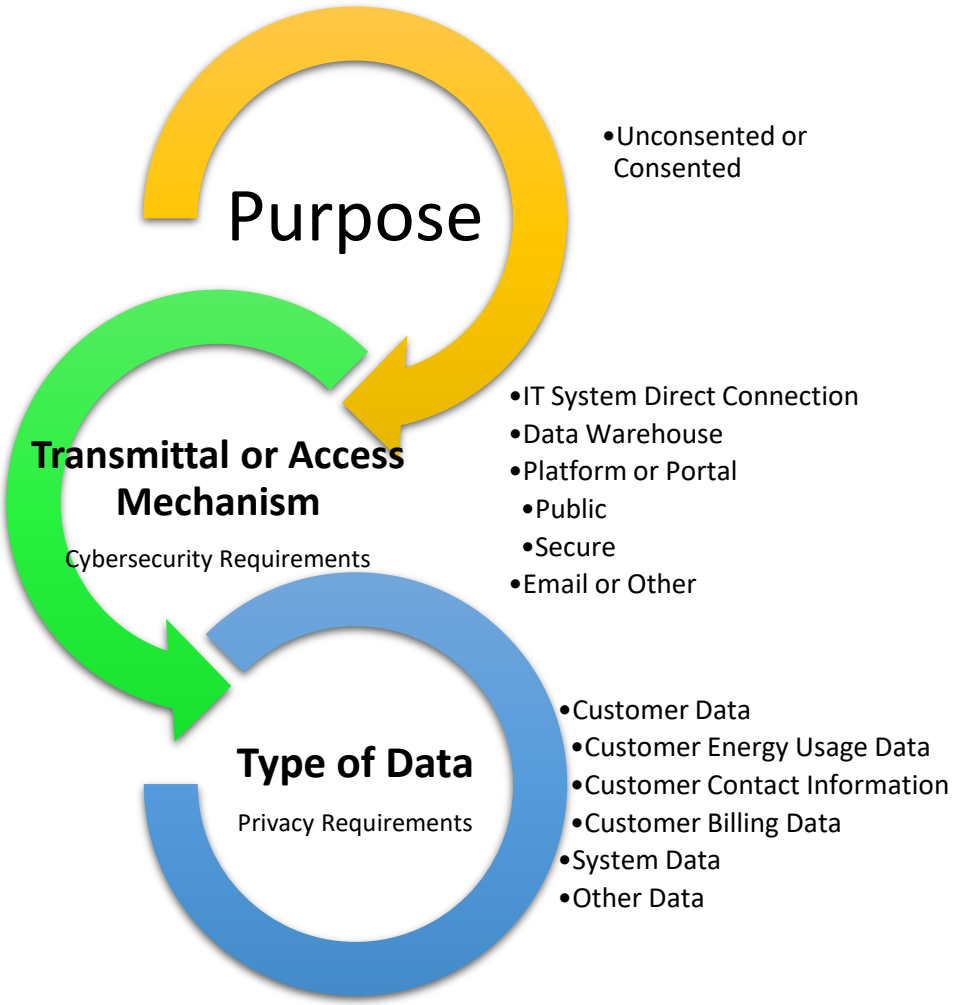
4.4.1. Authorized ESE Verification

Upon receiving an ESE certification request, the Provider would first verify that the applicant is an authorized ESE. The applying ESE will have to have completed all necessary DPS requirements before the ESE will be approved as an authorized ESE. To ensure that any ESE that is seeking access to energy-related data has been properly authorized by DPS, Staff proposes to develop an authorization mechanism for any ESE that is not currently subject to registration or authorization requirements

through existing Commission Orders. Currently, there is not a centralized listing that provides the information for all approved ESEs. However, there are market-specific listings available. Staff proposes to evaluate the creation of such a listing or other means by which the Provider could verify the applying ESE has been authorized to provide service(s) to utility customers.

4.4.2. Access Considerations

The necessary cybersecurity and privacy requirements for access to energy-related data should be determined by the following access considerations: the purpose for accessing the data, the mechanism by which the data are being accessed or transmitted, and the data type for which access is being requested.



As can be seen above, the second step in the approval request requires an ESE to provide the details of the purpose of accessing the data, how they will be accessing the data, and the type of data they are requesting. The necessary cybersecurity protections would be determined based upon the access or

transmittal mechanism and the privacy protections would be determined based upon the data type being accessed. In some instances, there may be privacy requirements but not cybersecurity requirements, or vice versa.

4.4.2.1. Access Considerations: Purpose

When requesting access to energy-related data, an ESE would first detail for what purpose the data are being sought and whether the ESE has obtained customer consent. Upon determining the ESE request is valid, the Provider would use this information to determine the data sets available, as well as the granularity of such data, by using the matrix.

Valid purposes for requesting access to unconsented energy-related data include: (1) providing or reliably maintaining customer-initiated service; (2) including compatible uses in features and services to the customer that do not materially change reasonable expectations of customer control and ESE data sharing; or (3) disclosure pursuant to Commission Order and/or State, Federal and Local Laws or regulations. Examples of these actions include, among other things, issuing a bill for energy consumption, implementing a demand response program, implementing an Energy Efficiency (EE) program or other Commission authorized program like CCA, or to meet utility operational needs.

Unconsented data would be anonymized or aggregated before access is granted, with exception for data used for utility operational need or data required to be available, pursuant to Commission Order and/or State, Federal and Local Laws or regulations. In the event customer consent is received after receiving unconsented data, the ESE purpose, and requirements, would then change to be consistent with customer consent and the customer's choice.

Aggregated Data

Aggregated Data are a combination of data elements from multiple accounts to create a data set that is sufficiently anonymized as to not allow for the identification of an individual account or customer. As previously discussed, the Commission has adopted different privacy screen standards for different use cases such as community wide planning, CCA, UER reporting, and building benchmarking.

Anonymized Data

Anonymized Data are data sets containing individual sets of information where all identifiable characteristics and information including, but not limited to, name, address, or account number, are removed (or scrubbed) so that one cannot reasonably re-identify any individual customer within the data set.

4.4.2.2. Access Considerations: Transmittal or Access Mechanism

When considering what cybersecurity protections need to be in place for access to energy-related data, it is necessary to evaluate the means in which that data will be transmitted or accessed. There are varying degrees of risk, all dependent on the mechanism used for accessing or transmitting the data. In many cases, current utility processes do not recognize these differences and instead, assign the same level of risk regardless of how the data are being accessed. Cybersecurity protections are controls that are put in place to address the risk to IT systems and the data they house. The electronic transmittal or access to data can be done through a direct connection between IT systems or through a system platform or portal.

Direct Connection to Data Custodian IT System

Having a direct electronic connection to the IT system of a data custodian, such as the utility or a data warehouse, increases the risk to those systems and, as a result, the data they house. Though the data custodian should have proper risk mitigation controls implemented, the ESE connecting directly into the system (not through a data sharing portal, such as GBC) must have the appropriate cybersecurity protections to limit the risk from their side as well. In many instances, though a direct connection should be limited in what it is able to access, it is a connection that may come in behind the customer information system firewall, which increases the risk associated with access. Properly implemented system controls require separation of information to reduce the risk, but the risk of a breach remains. These direct connections are most often done by EDI or Application Programming Interface (API) transfer protocols and are typically associated with customer enrollment and the billing of a customer account. In most instances, this type of connection will require the highest level of cybersecurity requirements.

Centralized Data Warehouse

A centralized data warehouse is an alternative location for all energy-related data to be stored and accessed from. While New York does not currently have this resource available, the development of such a resource is being evaluated and will be discussed in a companion Staff whitepaper in this proceeding. If an ESE is seeking access to energy-related data from a centralized data warehouse, the requirements would be based on how the data will be accessed – through a direct connection or through a platform or portal.

Secondary Access: Platform or Portal

Secondary access may be through a public-facing or secure platform or portal, and the requirements will vary for each. Electronically accessing data through a secondary access point may require the ESE have cybersecurity protections in place. However, what the cybersecurity requirements are can vary depending upon the protections built into the platform as well as whether the data are publicly available. The primary difference between secondary access and direct connection access is where

exactly the ESE's IT system is connecting to the data custodian's IT system. When obtaining data through a secondary access point, though it may back trace into the data custodian's IT system, it is not a direct connection – meaning the platform or portal sits in-between the data custodian IT system and the ESE IT system. Properly implemented cybersecurity plans would require controls by the data custodian on the backend of that connection to limit the possibility of unauthorized access. Additionally, consideration should be given to cybersecurity controls that may already be part of the platform and to whether the data being provided are publicly available. Staff notes that there are existing public portals that provide system data and aggregated data, many of which do not require cybersecurity or privacy protections.

Public Platform

Those seeking access to energy-related data from a public platform are able to do so without needing to meet any Commission or utility requirements. Publicly available data are inherently protected, when necessary, before being made available to the public through anonymization and aggregation standards. As an example, the UER provides aggregated community level usage information but does not require ESE registration or any cybersecurity and privacy protections to access it. Public platform use should not require any certification.

Secure Portal or Platform

The other type of secondary access may be through a secure portal or platform, such as GBC. These access points, when properly implemented, reside separate from the servers that house any highly confidential personal information. A secure platform may represent a lower risk due to that separation and because many of these secure access points have been designed with cybersecurity and privacy controls built in. For example, when properly implemented, GBC includes requirements for, among other things, data transmittal that separates the data streams. This type of integrated control could meet the requirement that would otherwise need to be implemented by the ESE. Each secure platform or portal would be evaluated to determine if there are built-in protections and, if so, if they meet the requirements that are necessary to protect the IT systems and the data they house.

4.4.2.3. Access Considerations: Data Type Requested

The data type to which an ESE is requesting access would determine what the necessary privacy requirements should be. Data are initially considered in two separate categories, customer data and system data. In addition to the evaluation of the risk associated with the data type being requested, customers' right to choose to share their data must also be recognized and considered.

With the intention to empower customers and enable access to data in a uniform and consistent manner, Staff recommends adoption of the specific data sets defined below when determining the necessary privacy requirements for ESE access to energy-related data. In considering what data should

be included in what sets, Staff looked to the CCA Framework Order as a successful example of energy-related data sets that have been used for controlled access to energy-related data. The CCA Framework Order data sets were developed in a way that allows for release of specific data sets for different purposes during the implementation of an opt-out CCA program. The available data were defined in three separate categories: (a) aggregated customer and consumption (usage) data to support procurement; (b) customer contact information used to send opt-out letters; and, (c) detailed customer information for the purpose of enrolling and serving each customer.[38] Whilst there are many data components included in these three categories, no data are available other than what is necessary to facilitate the ESE program. In other words, no highly confidential personal information, such as social security number or banking information, is available or included under these defined categories.

The utilities IT systems record, and house, a significant amount of data, much of which is outside what is needed by ESEs. Staff recommends that highly confidential personal information, such as social security number or banking information, not be made available or shared for any purpose. Adopting a similar model to what was implemented for CCA programs would best enable useful access to useful data, while still providing strong privacy protections by limiting what data is made available. Any customer data sets not included in a data category below would not be available for sharing. However, as needs change, each data set and the data they include, could be addressed through the continuous improvement process discussed below in Section 4.8.

Customer Data Sets

Eligible customer data are separated in three different data sets, each of which has a different level of risk associated with allowing access to that data. The necessary requirements to protect that data would be assigned based upon that risk. However, these requirements may be modified upon customer consent for release of his or her data. A customer's right to share his or her energy-related data should be recognized and is a necessary consideration in determining the necessary ESE protections of that data. These details are discussed later in a separate section on customer consent.

Customer Contact Information Data Set

This data set contains information that is specific to the individual and should only be available for ESEs that are requesting access for a valid purpose including: (1) providing or reliably maintaining customer-initiated service; (2) including compatible uses in features and services to the customer that do not materially change reasonable expectations of customer control and ESE data sharing; or (3) providing pursuant to Commission Order and/or State, Federal and Local Laws or regulations, or upon customer consent. The following data elements are to be considered part of the Customer Contact Information Data Set: customer of record's name(s); service address; mailing address; phone number; and primary language, if available, as well as any customer-specific alternate billing name, address, and phone

[38] CCA Framework Order, p. 43.

number. The separation of this data set provides the necessary details to facilitate the request for customer consent while protecting customer privacy and recognizing a customer's choice to share his or her data.

Customer Billing Data Set

The Customer Billing Data Set includes the necessary account information to facilitate enrollment and billing of the customer's account. There are existing requirements for what data must be included for billing and enrollment of accounts through, for example, the UBPs. These required data components can be combined under one Customer Billing Data Set that provides the necessary information regardless of market.

The Customer Billing Data set is a master listing of the available data and includes components that may be part of other data sets or only applicable for an electric or gas account. This data set includes:

- Customer's service address, and billing address, if different;
- Account number;
- Electric and/or gas account indicator;
- Meter reading date or cycle and reporting period;
- Billing date or cycle and billing period;
- Customer's number of meters and meter numbers;
- Rate service class and subclass or rider by account and by meter, where applicable;
- Description of usage measurement type and reporting period;
- Budget billing indicator;
- Electric and load profile reference category or code, if not based on service class, whether the customer's account is settled with the New York Independent System Operator utilizing an 'hourly' or a 'class shape' methodology, or Installed Capacity (ICAP) tag, which indicates the customer's peak electricity demand;
- Life support equipment indicator;
- Gas pool indicator, for gas accounts only;
- Gas capacity/assignment obligation code;
- Customer's location based marginal pricing zone, for electric accounts only;
- Sales tax district used by the distribution utility and whether the utility identifies the customer as tax-exempt;
- Whether the customer receives any special delivery or commodity "first through the meter" incentives, or incentives from NYPA;
- The customer's Standard Industrial Classification (SIC) code;
- Usage type (e.g., kWh), reporting period, and type of consumption (actual, estimated, or billed);
- Whether the customer's commodity service is currently provided by the utility;
- 12 months, or the life of the account, whichever is less, of customer data and, upon separate request, an additional 12 months, or the life of the account, whichever is less, of customer data, and, where applicable, demand information. If the customer has more than one meter

associated with an account, the distribution utility or DSP shall provide the applicable information, if available, for each meter;
- Electronic interval data in summary form (billing determinants aggregated in the rating periods undera distribution utility's tariffs), and if requested in detail, an acceptable alternative format;
- Date of gas profile; and,
- Weather normalization forecast of the customer's gas consumption for the most recent 12 months or life of the account, whichever is less, and the factors used to develop the forecast.

Customer Energy Usage Data (CEUD) Set

CEUD is the data generated by a meter, for example, that describes a customer's usage. This data can be in kilowatts, kilowatt-hours (kWh), or any other data that the meter collects, such as voltage or current. This information can also include the rate a customer is on, and other billing determinants, such as bill cycle. In and of itself, the simple kWh amount will not provide much information about the customer. However, the CEUD becomes more valuable when paired with other data about a customer. CEUD can inform an ESE on potential energy efficiency investments that may be worthwhile, or whether a customer may be better off on a different rate design, or to generate the amount of compensation for any demand response product. CEUD reflects an individual customer's measured energy usage but does not identify the customer on its own.

With the rise of AMI, CEUD has become more valuable. Whereas before, with monthly meter reads, that information provided some high-level details about a customer, with AMI, which can collect data in 15-minute increments, much more granular information about customer behavior can be identified. For example, if a customer is not home during a peak hour time period, then perhaps the customer would be better off on a different rate based on his or her load profile. As discussed below there are several types of CEUD.

<u>Historical Data</u>

Historical data are the most recent Customer Energy Usage Data, preferably while at the same address and for at least 12 months. Historical data are used to analyze impacts of a particular technology or program and extrapolate that into the future. Historical data can be used to analyze impacts of a particular technology or program and extrapolate that into the future. It is important to have a full 12 months of data in order to account for any seasonal changes in a customer's usage. Historical data can be provided at one time since historical data are used for a baseline measurement or to run an analysis of usage. Historical data can also be at a specific granularity, if available. For example, an authorized ESE could ask for 12 months of 15-minute data, 12 months of hourly data, or 12 months of monthly data depending on the need for such data, and as authorized by the customer.

Real Time Data

AMI often collects data at a higher rate than what is provided back to the utility. While AMI collects data in 15-minute increments, for example, and sends that information to the utility every 6-8 hours, it is also possible for the customer to obtain data much more frequently. Typically, AMI contains a second radio to support the Home Area Network (HAN) access. For customers that have technology to communicate with the meter over the HAN, it may be possible to receive data every 8 seconds. In order to set up the process for the HAN, additional steps need to be taken by the utility to ensure the data are going to an authorized device. This may include a process for a customer to provide the utility with the Media Access Control (MAC) address of the device and be part of commissioning the device with the meter. To address cybersecurity risks of the HAN, it is possible to architecturally minimize the risks by implementing the standard in a way that does not allow two-way communication between the device and the meter or disables other functions of the communication standard.

Other Types of AMI Data

It is important to note that there are other data that can also be made available. For example, advanced meters collect more than just usage. These meters may also monitor current, frequency, voltage, and var, all of which are capable of being provided to customers via the HAN or collected by the utility over AMI networks. These data can provide customers or other third parties with more information about the impacts that other devices, technology, or usage patterns may have on their own usage, or as it impacts the grid. Existing standards may already contain fields allowing for that information to be shared. For example, GBC is currently capable of sharing these data sets if the data are capable of being shared. While not the immediate focus of this whitepaper, recognizing that there is additional information that is capable of being collected and shared with a customer or its authorized ESE shows the importance of a pathway for data access and the need for a data access Data Access Framework to ensure that these use cases and opportunities are not ignored.

System Data

System data are information about components and activity at the distribution system level. Most system data do not allow for identification of individual customers. However, there may be some system data that, while not CEUD, may still identify an individual customer. In those limited circumstances, system data can be aggregated with other local circuits to create an aggregated set of data that sufficiently reduces the risk of reidentification.

System data also include maps identifying the hosting capacity of circuits and the types of distribution circuits across a service territory. These maps can provide the market with important information about the potential ability of a resource to successfully interconnect at a location. Information about the operation of the electric system is generated by devices located across the system. This information includes performance of the distribution system collected from distribution transformers, distribution substations, and information to generate hosting capacity analysis. The accessibility of system data is

imperative for creating the benefits as envisioned under REV and in support of the State reaching its clean energy goals. For example, development of non-wires alternatives requires more data about the system in order to target solutions and technologies to meet a non-wires alternative request. Developers need better insight into the hosting capacity of the distribution system in order to better understand locations across the grid with a higher likelihood of success in the interconnection process. Alternatively, the same data can be used by demand response, energy efficiency, or energy storage developers as possible locations to alleviate a constraint or congestion, i.e., areas where the value of distributed energy resources may be higher.

For system data, except for those pieces of system data that may impact customer privacy or critical infrastructure protection, there should be no protections on the availability of such data, since it is aggregated data itself. Since it is not CEUD, it is not subject to customer consent. System data should also be made available to the public. Some of the utility's hosting capacity maps are public, while others require user registration with the utility. Users should not be required to register with the utility prior to access.

4.4.3. Determination of Risk-Based Cybersecurity and Privacy Requirements

After the ESE has provided the necessary access consideration details, the Provider would determine what existing cybersecurity and privacy requirements would apply. The necessary cybersecurity and privacy requirements applicable to the combination of ESE purpose, access mechanism, and data type would be determined by applying existing Commission requirements. Though there are multiple Commission documents that reference data access requirements, the primary documents pertaining to requirements for an ESE to access energy-related data, and that detail the responsibilities of the ESE to the customer and to the utility, are the ESCO and DER UBPs, and the cybersecurity and privacy requirements adopted by the Commission in its Cybersecurity Order. To facilitate this process, Staff proposes the development of a matrix that maps the existing cybersecurity and privacy requirements to the various combinations of purpose, access mechanism, and data type that can result from application of the Data Access Framework. This matrix would then be used by the ESE risk management Provider to determine what cybersecurity and privacy requirements and ESE would need to demonstrate compliance with to be certified.

When enabling access to energy-related data, it is necessary to consider the risk to IT systems and the risk to the privacy of the data they house. The primary goal of instituting privacy and cybersecurity protections is to reduce that risk but in order to do so, we must first understand what is at risk, and how significant that risk is. Risk management is an essential component of the Data Access Framework and ensures that any risk to confidentiality, integrity, and availability is identified, analyzed, and maintained at acceptable levels. Implementing a risk-based Data Access Framework is consistent with Commission-authorized requirements, current utility implementation strategies, and industry actions.

The proposed Data Access Framework incorporates requirements that have been determined through implementation of risk management frameworks and models. There are a multitude of possible cybersecurity and/or privacy controls that can be implemented as a way to mitigate the risks associated with data access, for example:

- Allowing CEUD to be made available, but not highly confidential personal information, is a risk-based approach.
- Recognizing that aggregated and anonymized data have different levels of risk and, when appropriately compiled, have less risk of re-identification, balances privacy risks with societal benefits.
- Adopting a statewide Data Access Framework and single process reduces risk by ensuring that uniform standards are being adhered to across the State.

The ESCO UBP and DER UBP (UBPs)

The UBPs detail the necessary requirements for an ESCO or DER to provide service to New York consumers and define the obligations between the utility and the ESE pertaining to, among other things, the data-sharing timeframes and data sets transmitted. The UBPs include the Department's registration process for their respective industries. The UBPs include similar, and in some areas identical, requirements for the transactions between the ESE and customer. It is important to note that the UBPs do include areas that would be outside of what is proposed to be incorporated into the matrix, such as Marketing Standards, EDI Requirements, Registration and Eligibility Requirements, Billing and Payment Processing, and Creditworthiness standards. This proposal does not include any recommendations pertaining to the processes and requirements associated with eligibility, registration, or compliance that have been established in the UBPs. The UBPs define necessary requirements for the interactions with customers. These requirements are controls meant to ensure customer consent is obtained, protect customer privacy, and ensure that customers receive notice of changes to their service. These requirements are generally, but not completely, consistent between the two documents.

The Cybersecurity Order

The Cybersecurity Order provides defined cybersecurity and privacy requirements that are meant to serve as risk mitigation controls. These controls overlap in some areas within the Order, as well as with the requirements of the UBPs and other Commission proceedings. There are two aspects of the privacy controls required – those that specifically define the requirements of the ESE with their interactions with the customer, and those ESE requirements to implement controls that minimize data privacy risk generally. The privacy requirements also define what can be done with the data and how it is categorized. Cybersecurity requirements include, but are not limited to, actions needed at all levels of the ESE and include policies, as well as data handling requirements.

The proposed Data Access Framework should also recognize that existing state, federal and/or local legislation will need to be considered when making data access decisions. For example, the State's Stop Hacks and Improve Electronic Data Security (Shield) Act broadens the scope of consumer privacy and places requirements on protecting personal data for organizations that collect information on New York residents.[39] Additionally, utilities must remain in compliance with their respective Critical Infrastructure Cybersecurity Plans which may restrict access to certain data components.

4.4.4. Verification of Requirements and Certification

Verification that the ESE has the necessary cybersecurity and privacy requirements is the last step for an ESE to become certified as Data Ready and assigned an Access Role that identifies the types of data they may request to access, as well as identifying the transmittal mechanisms they are able to utilize. The access role is based upon the access considerations and the verification of meeting the necessary requirements.

4.5. Certified ESE Data Request

Once an ESE has received its Data Ready Certification, the ESE would be able to request access to data defined under its assigned Access Role. The Access Role provides the data sets and access mechanisms for which the ESE has been certified to have the appropriate cybersecurity and privacy requirements in place.

As an example, an ESE requests EDI direct IT system connection for Customer Billing Data set. The Data Custodian confirms the ESE is Data Ready and that its Access Role allows for that data set to be transmitted through a direct connection, either through a manual or automated review of Data Ready Certified ESE listing. Once confirmed, the Data Custodian allows the data to be accessed.

4.6. Utility Connection Requirements

While the ESE Data Ready Certification program would provide a centralized process for seeking access to energy-related data, it would not address the requirements for utility connectivity testing. If an ESE is seeking direct connection into the utility IT systems, whether by EDI, API, or other means, the ESE would still need to complete the required testing and connectivity requirements. These requirements should only be for direct system-to-system connection and should not include requirements outside of testing that connection. This system-to-system connectivity testing may also apply when the data custodian is not the utility, such as with a data warehouse direct connection.

[39] Chapter 117 of the Laws of 2019.

4.7. Data Responsibilities and Relationships

While there are defined responsibilities for an ESE interaction with the utility, and the customer, the responsibilities of the utilities to the ESEs seeking access to data have yet to be established in a way that promotes meaningful data quality standards. The Commission acknowledged this in its Cybersecurity Order, stating "notably absent from the DSA are the obligations of the utility for service levels and processes when they are providing data to ESEs."[40] The need for such standards is supported by market participant feedback where, in multiple proceedings, requests have been made for development of utility-side requirements and responsibilities to the ESEs for data access. Staff has worked with parties trying to resolve issues with, among other things, data time frames, onboarding problems, data quality and integrity concerns, inconsistent platform implementation, and difficulties with getting assistance with technical or data quality issues.

4.7.1. Data Access Fees

Access to system data – such as hosting capacity, distributed generation queued for interconnection, installed distributed generation and other previously mentioned available system data – are available without a fee. The UER populates community wide aggregated energy usage information and is available to the public free of charge. Staff believes that access to this information increases transparency to the market and lowers barriers to entry for new products and programs. In connection with the proposed Data Access Framework, which would create a centralized and automated process for data access, Staff recommends abolishing all data fees, including the fees for CCA related data.

4.7.2. Data Quality and Integrity

Defining the necessary steps and requirements for an ESE to obtain access to energy-related data is necessary to enable the sharing of useful energy data. However, without establishing requirements for the quality and the integrity of the data being shared, the usefulness of that data may be lost. While Staff acknowledges that each utility is operating with different IT systems, the differences in how the data are being recorded on the utility side does not necessarily prevent the ability to provide standardized data as an output. Energy-related data should be portable, and customers need to have the ability to share their data with any ESE, through whatever means they have chosen. For that to happen, available energy usage should be made available in a standardized manner. Along these lines, Staff seeks stakeholder input as to what data quality and integrity standards should be considered, as well as what type of metrics can be used as a means to determine if these standards are working.

[40] Cybersecurity Order, p. 64.

4.7.3. Reporting

Accountability and Auditing

As with data access, annual reporting requirements have been established in multiple proceedings and in some cases, like GBC reporting, the requirements have been included in rate case proceedings. In consideration of the many areas that may have existing reporting requirements, Staff proposes to incorporate all the reporting requirements into one primary reporting matrix. This would ensure that all the necessary components are available for the proper evaluation of access to energy-related data. Staff seeks input from stakeholders as to the frequency of any required reporting, as well as whether there are specific metrics that should be captured for determination of the success of this Data Access Framework.

4.8. Data Access Framework Continuous Improvement

The proposed Data Access Framework is designed to be flexible when it comes to changing needs. This Data Access Framework is grounded in a risk-based approach to security and privacy which requires continuous review and modification to address new threats or risk, and the necessary protections to mitigate these risks. Staff recommends annually convening a Data Access Market Participant Input Session to allow input and collaboration from ESEs, utilities, and other market participants. Staff could then make recommendations for modifications to the proposed Data Access Framework to the Commission based upon those meetings if necessary. In the event there is an immediate need for a modification to the proposed Data Access Framework, the Commission could take short term measures to allow immediate action on items that pose a security concern and are unable to wait for the annual review process.

4.9. Customer Sharing of Energy-Related Data

The proposed Data Access Framework, as discussed above, would not meet its full potential of enabling useful access to useful data without first establishing mechanisms that (a) facilitate customers' ability to easily consent to share their data and (b) educate and engage customers as a means to encourage customer consent to data sharing. Additionally, further exploration of opt-out strategies could prove to be beneficial. The power of unlocking useful data lies in the customer's hand. Staff's recommendations on this topic considers a balance between informed consent and the value of sharing data. The Commission's Cybersecurity Order recognized that the data are the customers' data and that customers have a right to direct or consent to the use of their data. Simply put, they are the ones who determine what happens with their data, not the data custodian.

While there has been a substantial amount of work put into establishing the UBPs' consent requirements, including the process of obtaining consent, these requirements only govern the interaction between customers and ESEs for general purposes (enrollment and billing). The existing requirements include, among other things, ensuring that the ESE is providing the necessary information

for the customer to provide informed consent, and for such consent to be deemed valid. The discussions below do not address these existing requirements found in the UBPs. Instead, the discussions around consent pertain to a customer's ability to consent for other purposes, through alternative means. For example, a customer may use GBC to consent to share his or her data with an energy efficiency provider for the purpose of identifying potential products or services the customer may benefit from. The customer and ESE interaction options and requirements in this example would not be determined by the UBP. Currently, there is no guiding document or policy that establishes overall requirements that apply for consent outside of general purposes.

Need for Consent

To enable the market for new products and services, there is a need for CEUD. To maintain the privacy of customer data, the data custodian (e.g., the utility or a data warehouse) must have the necessary cybersecurity and privacy protections in place to adequately maintain the security of customer data. Highly confidential personal information, such as social security numbers and financial information should never be shared, however, an authorized ESE can be provided with customer contact information and usage information upon the consent of the customer.

Since the terms of the consent agreement are between the customer and the ESE, the need or purpose of that data request need not be provided to the data custodian. The ESE's purpose for accessing data would be validated through the Data Ready Certification process. To facilitate this consent process, some states, such as Texas and California, have a common consent form across the utilities. Staff recommends establishment of universal consent mechanisms that would ensure all participants in the process, including the customer, have a clear and common understanding of terms and requirements for informed consent that allows energy-related data to be shared. Consent mechanisms should not be implemented in a way that imposes unreasonable barriers to customer choice. Without specific requirements that ensure consistent processes and treatment, regardless of utility, mechanisms established to enable customers to easily consent to share their data will not be effective. As such, standardized mechanisms for consent, should be developed to ensure a common application and process for customers, ESEs, and utilities across New York State.

While utilizing a web-based process with as few steps as possible is preferred, would keep the customer engaged, and would facilitate the consent process, other consent options should be developed for those who do not have electronic means available or who choose to use alternative methods. While providing consent through traditional means (i.e. signing an agreement and mailing it in) may delay the customer process and can result in a customer having a less convenient experience, the option should be made available for those who choose to use these means.

Options should be explored for development of multiple standardized options for a customer to provide consent. For example, many customers are familiar with internet-based commerce and permissions.

Customers can login to secure web sites using authentication from other sources, such as using a Google or a Facebook password. Therefore, rather than requiring customers to use their account numbers for authentication, customers could instead potentially use their utility log-in information. This method of authentication maintains the customer consent process because each landing page throughout the process requires information only held by the customer.

Expectations of Consent

Expectations of privacy and consent are evolving. A customer who is uninterested in new apps, services, or offerings may be unlikely to support having his or her data be made available and provide consent. A customer interested in the newest technology offerings may have less concerns about the privacy of his or her CEUD. The consent agreement should be developed in a way that enables customers to exercise control over their consent by: addressing customer choice; defining the data being shared, for what purpose, and for how long; allowing the customer the ability to revoke consent; requiring additional consent for any purposes outside what was originally specified; and ensuring consistency with requirements existing under the Data Ready Certification model. Other requirements that would traditionally be dictated by the consent agreement would be incorporated into requirements under the Data Ready Certification. This would reduce the necessary information a customer will have to read and understand in order to complete a consent agreement. An authorized ESE might only need monthly data for the past six months, in which case, the customer should be made aware and ensure that only six months of monthly data are provided to the ESE subject to his or her consent.

Customer Options

The principle of customer control should be considered when evaluating the types of data and various uses of customer data. Customers should be able to condition the use of their data beyond whatever is needed to provide utility service. Customers should be able to choose to allow their data to be shared with individual authorized ESEs as well as afforded the option to choose to share their data openly with all authorized ESEs. Empowering utility customers in these ways reflects the changing cultural perspectives on the value of customer data and recognizes an increased consumer understanding of their rights to control what happens with their data. Nevertheless, customers should be made aware of their right to opt-out of having their data shared in certain situations. For a utility to provide service, it must do several things - forecast demand, contract for electricity, generate a bill, install a new meter, maintain service and equipment, and so forth. A utility may also develop other customer programs or evaluate existing programs which will make use of customer data. Staff seeks further input as to the situations in which customers should be afforded the opportunity to opt-out of having their data used, including use by the utility to develop new products and services, as well as having their data included in a larger aggregated dataset that keeps the customer's identity anonymized.

Opt-Out Approaches

Utilities play a critical role in achieving on New York's ambitious clean energy policy objectives, delivering robust programs to reduce carbon emissions, increase system reliability, and save money for participating consumers. Opt-out strategies, or providing to consumers an opportunity to decline participation rather than proactively seek it, have been successfully deployed to increase the participation rates for various programs and policy objectives. For example, New York's CCA program has demonstrated how opt-out enrollment can benefit both customers and the communities they reside in. To date, CCAs, on average, have offered savings in energy supply costs, allowed for a cleaner energy supply and, perhaps most importantly, have helped customers become informed consumers. CCAs in New York State saw a 16.5% opt-out rate during program initiations.[41]

Staff proposes further piloting this concept for the purpose of sharing CEUD to advance clean energy goals. Any such pilot must have a well-defined duration, must clearly communicate to consumers what data will be shared, with whom and for what purpose it will be shared, and must have a clear process for allowing consumers to decline participation or opt-out. Possible approaches may include providing an opt-out opportunity at the time service is established, when a customer signs up for a time-of-use (TOU) rate or community distributed generation (CDG) program, when a customer makes a purchase from a utility's marketplace, or when a customer participates in a rate-payer funded energy efficiency program. Staff seeks market participant input on how best to develop such a pilot including criteria to use to ensure consumers are provided appropriate notice and opportunity or opt-out.

5. Implementing the Solution

The proposed Data Access Framework defines the process for access to energy-related data, recognizes customers' right to consent to share their energy usage data, encourages customer control of their energy-related data, supports the requirements of in the Commission's Cybersecurity Order, provides standard definitions of key data-related terms, establishes and ensures data quality and integrity standards, and creates an easy to understand Data Access Framework Application Guide that outlines the necessary steps to obtain access to energy-related data in a uniform and consistent manner.

Only through addressing and including all the components detailed above, will the true value, and benefits of, access to energy-related data be fully unlocked. The implementation of the proposed Data Access Framework is designed so as to not place burdensome requirements upon any party.

As discussed throughout this whitepaper, the necessary cybersecurity and privacy requirements have already been determined throughout numerous proceedings. These requirements have already

[41] Consumers residing in a CCA municipality are provided notice that a CCA will be instituted and provided an opportunity to decline participation.

received Commission approval for use, and the existing roadblock is not the accuracy of the requirements, it is in the accurate assignment of risk and inconsistent implementation of such requirements. Implementation and application of this Data Access Framework will require actions of both Staff and utilities for it to be successful. A necessary output of the framework is a mapping of the existing cybersecurity and privacy requirements to the various combinations of purpose, access mechanism and data type that can result from application of the Data Access Framework (i.e. the matrix). Creation of such cybersecurity and privacy requirement matrix will require a detailed examination of all existing requirements, accounting for duplicative and inconsistent requirements, and reviewing for correct risk assignment. This matrix would then be used to determine the required cybersecurity and privacy protections for Data Ready Certification and would replace the existing utility side requirements for ESEs seeking access to energy-related data. Staff proposes that the cybersecurity and privacy matrix compile existing requirements and identify and assign the necessary requirements for ESE access to energy-related data.

Staff notes that the proposed Data Access Framework does not place additional requirements upon utilities for the determination of necessary requirements or validation of the requirements being met. Adoption of the Data Access Framework is expected to reduce the amount of time and resources the utilities would need to allocate in order to ensure an ESE has the appropriate protections in place. The implementation of the proposed risk-based ESE Data Ready Certification program completely removes the utilities informal oversight role and correctly moves it to the Provider, for a uniform and consistent application.

6. Closing

This proposed Data Access Framework would establish a clear set of requirements that must be implemented to ensure the appropriate protections are in place for access to energy-related data while also enabling the means by which customer access and data sharing can occur. Staff believes that this Data Access Framework would provide utilities, customers, and ESEs with a set of expectations on process which would support a marketplace of ideas and innovation. This would further ensure that the experiences and expectations of the customers and ESEs are substantially the same throughout the State. This would allow ESEs to craft one set of business practices that can be used across the State rather than crafting individual business practices for each utility service territory, thus potentially reducing ESE costs related to customer acquisition and implementation of cybersecurity and privacy controls.

Staff is asking the Commission to adopt a statewide Data Access Framework that includes the following:

- A framework that serves as a single source for data access and provides uniform and consistent guidance on what is needed for access to, and the availability of, energy-related data. This framework would incorporate all existing data access requirements, including cybersecurity and privacy requirements.

- A Data Access Framework Application Guide that conveys the necessary steps for obtaining access to data.
- The implementation of an ESE risk management program that provides a Data Ready Certification. The ESE risk management program would be responsible for the verification and certification of ESE cybersecurity and privacy requirements.
- Standard definitions of key data-related terms.
- The development of data quality and integrity standards.
- Customer consent requirements.
- An Opt-out pilot program.
- Reporting requirements.

If the proposed Data Access Framework is adopted, Staff recommends that each utility should be directed to make a compliance filing that includes the details and verification of how each has updated all existing policies and requirements to be consistent with the Data Access Framework.

In addition to the individual utility compliance filing, Staff recommends a subsequent Joint Utilities filing, for Commission review and approval. The joint filing should include:

- a proposal for an alternative method of account identification when completing ESE customer transactions that have traditionally relied on the customer account number for that purpose;
- an implementation proposal for the ESE risk management program, managed by a Provider, and includes the Data Ready Certification program; and
- an implementation plan detailing how the JU will implement a centralized certification model that any ESE will be able to access, and that will only have to be done once, regardless from which data custodian the ESE is seeking to access data, until the ESE risk management program and Data Ready Certification is fully operational.

Finally, Staff intends to file with whitepaper for public comment. When submitting comments, Staff urges stakeholders to utilize the organizational structure of this whitepaper in order to facilitate the analysis of issues presented in each section.

Definitions of Key Data-Related Terms

Access Role

The access role is determined through the Data Ready Certification process and details the exact data sets and transmittal/access methods through which the ESE is approved to access energy-related data.

Aggregated Data

Aggregated Data are a combination of data elements from multiple accounts to create a data set that is sufficiently anonymized as to not allow for the identification of an individual account or customer.

Anonymized Data

A data set containing individual sets of information where all identifiable characteristics and information including, but not limited to, name, address, or account number, are removed (or scrubbed) so that one cannot reasonably re-identify any individual customer within the data set.

Customer Billing Data Set

The Customer Billing Data Set includes the necessary account information to facilitate enrollment and billing of the customer's account.

Customer Contact Information Data Set

This data set contains information that is specific to the individual and should only be available for ESEs that are requesting access for a valid purpose including: (1) providing or reliably maintaining customer-initiated service; (2) including compatible uses in features and services to the customer that do not materially change reasonable expectations of customer control and ESE data sharing; or (3) providing pursuant to Commission Order and/or State, Federal and Local Laws or regulations, or upon customer consent. The following data elements are to be considered part of the Customer Contact Information Data Set: customer of record's name(s); service address; mailing address; phone number; and primary language, if available, as well as any customer-specific alternate billing name, address, and phone number. The separation of this data set provides the necessary details to facilitate the request for customer consent while protecting customer privacy and recognizing a customer's choice to share his or her data.

Customer Data Sets

Eligible customer data are separated into three different data sets: customer contact information, customer billing, and customer energy usage.

Customer Energy Usage Data (CEUD) Set

CEUD is the data generated by a meter, for example, that describes a customer's usage. This data can be in kilowatts, kilowatt/hours, or any other data that the meter collects, such as voltage or current. This information can also include the rate a customer is on, and other billing determinants, such as bill cycle.

Cybersecurity Protections

Risk mitigation controls implemented to address the risk to IT systems and the data they house.

Data Custodian

Where the energy-related data are housed and being accessed, such as from the utility or from a centralized data warehouse.

Energy Service Entities (ESEs)

Any entity (including, but not limited to, ESCOs, DERs, and CCA Administrators) seeking access to energy related data. In limited circumstances, the utility may also be an ESE.

Highly Confidential Personal Information

Highly sensitive information specific to an individual that could be used to identify the individual, such as social security number, banking information, or driver's license. This information should not be shared under any purpose and is not used for transactions related to access to energy-related data.

Historical Data

Historical data are the most recent Customer Energy Usage Data, preferably while at the same address and for at least 12 months. Historical data are used to analyze impacts of a particular technology or program and extrapolate that into the future.

Privacy Protections

Risk mitigation controls that are implemented to address the privacy risks of the data.

Real Time Data

Data collected via Advances Meter infrastructure that is presented in 15-minutes increments, or less.

System Data

System data are information about components and activity at the distribution system level.