STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

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

ORDER ADOPTING A DATA ACCESS FRAMEWORK AND ESTABLISHING FURTHER PROCESS

Issued and Effective: April 15, 2021

TABLE OF CONTENTS

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

At a session of the Public Service Commission held in the City of Albany on April 15, 2021

COMMISSIONERS PRESENT:
John B. Howard, Interim Chair
Diane X. Burman
James S. Alesi
Tracey A. Edwards

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

ORDER ADOPTING A DATA ACCESS FRAMEWORK AND ESTABLISHING FURTHER PROCESS

(Issued and Effective Albany 15, 2021)

BY THE COMMISSION:

INTRODUCTION

Releasing readily available energy-related data by means of useful access mechanisms will support New York in meeting its clean energy goals and facilitate the objectives of the Reforming the Energy Vision (REV) proceeding.[1] The ability of market participants to deliver smart, economically sound energy solutions and the ability of customers to share their energy usage data, will animate markets, facilitate customer choice, and provide systemic benefits to all New Yorkers. In conjunction with useful data access, it is necessary to ensure that the proper protections of information technology (IT) systems, data systems, and customers' privacy exist.

Understanding the importance of data access and associated cybersecurity and privacy protections, the Public

[1] See, Case 14-M-0101, Reforming the Energy Vision.

Service Commission (Commission) adopts a Data Access Framework (Framework) that serves as a single source for statewide data access requirements and provides uniform and consistent guidance on what is needed for access to energy-related data, including the availability of such data. The Framework, as described in detail below, incorporates the existing Commission established data access requirements to date,[2] including cybersecurity and privacy requirements, and establishes data quality and integrity standards criterion to be met by the utility, or data custodian, for application or use case specific purposes. Additionally, the utility will play a role with increasing customers' familiarity with appropriate data sharing options.

BACKGROUND

In its Accelerated EE Order,[3] the Commission announced that a new, comprehensive data proceeding would be instituted and established guiding principles to serve as foundational elements for developing policies that appropriately balance privacy concerns with the rapidly changing energy marketplace. These principles include:

1. increase customers' familiarity with, and consent to, appropriate data sharing;

[2] See Appendix D

[3] 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).

2. move towards improved access by Energy Service Entities[4] (ESEs) to customer energy-related data, consistent with consent requirements;
3. link energy-related data with other sources of building data, energy use drivers, and energy systems data to enable enhanced identification of energy efficiency and Distributed Energy Resource (DER) opportunities; and
4. provide the mechanisms for appropriate access to energy-related data to be implemented in a useful, timely, and quality-assured manner.

The Commission reinforced this view in its order instituting this proceeding, affirming that existing requirements related to data access are inconsistently applied and lack clarity, and requiring the establishment of a Data Access Framework that clearly defines the process for data access and standardizes the necessary privacy, cybersecurity, and quality requirements for access to energy-related data in a way that ensures uniform treatment across various energy-related data use cases.[5] 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 file a whitepaper regarding development of a data access policy

[4] Any entity, including, but not limited to, energy service companies (ESCOs), distributed energy resource suppliers (DERS), and community choice aggregation (CCA) administrators, seeking access to energy related data. In limited circumstances, the utility may also be an ESE.

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

framework that standardizes the necessary privacy, cybersecurity, and quality requirements for access to energy-related data (Whitepaper). The Whitepaper was filed on May 29, 2020.[6]

As proposed by Staff and described in the Whitepaper, the Data Access Framework would serve as a single source for data access policies and provide uniform and consistent guidance on what is needed for access to, and the availability of, energy-related data. In addition, the Data Access Framework would provide a more streamlined approach for access to data, while preserving all the necessary protections, to facilitate the policy goals of the Commission, and would do so by incorporating all of the existing data access requirements, including cybersecurity and privacy requirements.

The Whitepaper also proposed specific actions including the creation of 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 includes a Data Ready Certification process; standard definitions of key data-related terms; development of data quality and integrity standards; defining reporting requirements; and exploring customer consent requirements and opt-out pilot programs.

NOTICE OF PROPOSED RULE MAKING

Pursuant to the State Administrative Procedure Act (SAPA) §202(1), a Notice of Proposed Rulemaking was published in the State Register on June 24, 2020 [SAPA No. 20-M-0082SP1]

[6] Case 20-M-0082, Department of Public Service Staff Whitepaper Regarding a Data Access Framework (filed May 29, 2020).

(SAPA Notice). Additionally, a Notice of Stakeholder Meeting and Soliciting Comments indicated that initial comments on the Whitepaper were due August 24, 2020, with reply comments due September 11, 2020 (Secretary's Notice).[7] Staff held a Stakeholder Information Session on July 21, 2020, where the details of the Data Access Framework were presented and participants were able to submit questions before and during the session. There were ten comments and four reply comments received in response to the SAPA Notice and Secretary's Notice. Appendix E includes a listing of the commenters and a summary of those comments.

LEGAL AUTHORITY

The Commission's authority derives from the New York State Public Service Law (PSL), through which numerous legislative powers are delegated to the Commission. Pursuant to PSL §5(1), the "jurisdiction, supervision, powers and duties" of the Commission extend to the "manufacture, conveying, transportation, sale or distribution of . . . electricity." PSL §5(2) requires the Commission to "encourage all persons and corporations subject to its jurisdiction to formulate and carry out long-range programs, individually or cooperatively, for the performance of their public service responsibilities with economy, efficiency, and care for the public safety, the preservation of environmental values and the conservation of natural resources."

PSL §66(2) provides that the Commission shall "examine or investigate the methods employed by [] persons, corporations

[7] Case 20-M-0082, Notice of Stakeholder Meeting and Soliciting Comments (issued June 30, 2020).

and municipalities in manufacturing, distributing and supplying . . . electricity . . . and have power to order such reasonable improvements as will best promote the public interest, preserve the public health and protect those using such . . . electricity. . .” Further, PSL §65(1) provides the Commission with authority to ensure that “every electric corporation and every municipality shall furnish and provide such service, instrumentalities and facilities as shall be safe and adequate and, in all respects, just and reasonable.”

The Commission also has authority to prescribe the “safe, efficient and adequate property, equipment and appliances thereafter to be used, maintained and operated for the security and accommodation of the public” whenever the Commission determines that the utility’s existing equipment is “unsafe, inefficient or inadequate.”[8] PSL §66(3) further empowers the Commission to “[p]rescribe from time to time the efficiency of the electric supply system.” PSL §4(1) also expressly provides the Commission with “all powers necessary or proper to enable [the Commission] to carry out the purposes of [the PSL]” including, without limitation, a guarantee to the public of safe and adequate service at just and reasonable rates,[9] environmental stewardship, and the conservation of resources.[10] Thus, the Commission may exercise this broad authority to direct

---

[8] PSL §66(5).

[9] See International R. Co. v Public Service Com., 264 AD 506, 510 (1942).

[10] PSL §5(2); see also, Consolidated Edison Co. v Public Service Commission, 47 N.Y.2d 94 (1979) (overturned on other grounds) (describing the broad delegation of authority to the Commission and the Legislature’s unqualified recognition of the importance of environmental stewardship and resource conservation in amending the PSL to include §5).

regulatory standards to execute the provisions contained in the PSL. Additionally, the Commission has the authority to direct the treatment of DER by electric corporations.[11]

DISCUSSION

Data Access Framework

As proposed in the Whitepaper, the purpose of adopting a Data Access Framework is to provide clear and consistent rules to guide implementation, define roles and responsibilities, create confidence in the quality of the data, and ensure that the appropriate ESE is accessing data in a secure manner with cybersecurity and privacy protections being assigned through a risk-based approach. Enabling access to, and appropriate use of, energy-related data with enhanced customer data protections furthers the trust relationship between ESEs and consumers, and enables innovation while also avoiding regulatory fragmentation that could undermine New York State's goals.

A. Party Comments

Energy Technology Savings, Inc. DBA Logical Buildings (Logical Buildings); Advanced Energy Economy, Alliance for Clean Energy New York, and Advanced Energy Management Alliance (Collectively, "AEE"); Mission:data Coalition (Mission:data); the Retail Energy Supply Association (RESA); the City of New York (City); Association for Energy Affordability, Inc. (AEA); Recurve Analytics, Inc. (Recurve); the New York Power Authority (NYPA); and Central Hudson Gas & Electric Corporation, Consolidated Edison Company of New York, Inc. (Con Edison), National Fuel Gas Distribution Corporation, New York State Electric & Gas Corporation, KeySpan Gas East Corporation d/b/a

[11] PSL §§5(2), 66(1), 66(2), 66(3), 66-c, 66-j, and 74.

National Grid, The Brooklyn Union Gas Company d/b/a National Grid NY, Niagara Mohawk Power Corporation d/b/a National Grid, Orange and Rockland Utilities, Inc. (O&R), and Rochester Gas and Electric Corporation (collectively, "Joint Utilities" or "JU") all comment in support of the overall Data Access Framework, with some providing recommendations regarding certain components.

B. Discussion

The Commission adopts a Data Access Framework, as described in the body of this order, to serve as a single source for statewide data access requirements and provides uniform and consistent guidance on what is needed for access to energy-related data, including the availability of such data. The Framework incorporates the existing Commission established data access requirements to date, including cybersecurity and privacy requirements, and establishes criterion to be met for application or use case specific purposes, such as for data quality and integrity standards.

The Data Access Framework encompasses the following key components, with details of each component discussed further herein: Applicability, Enforcement, ESE Data Ready Certification Process, Data Responsibilities and Relationships; Data Access Framework Continuous Improvement; and Customer Sharing of Energy-Related Data. The Framework establishes responsibilities for both the ESE seeking access to data as well as the utility, or data custodian, providing the data.

Data Access Framework Applicability

The Framework was proposed to apply 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, ESEs would need to agree to abide by the terms of a Data Access Agreement,[12] as detailed below. The proposed Framework applicability does not 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.

A. Party Comments

The City asserts that building owners should not be categorized as an ESE and should be excluded from this process, but requests that if building owners are going to have to go through the process for receiving aggregated and anonymized customer data, it should be fast-tracked and not onerous. RESA supports the general applicability of the Data Access Framework to all ESEs and comments that the Commission should ensure that the Framework does not contain any preferences that favor or harm any single market sector, and recommends review by a diverse group of principal stakeholders as the best means to achieve this.

AEE and AEA comment that the definition of ESE should be modified to exclude utility contractors so as to not apply duplicative or conflicting requirements on such contractors who already operate under tight security measures as part of their contractual obligations with the utilities. AEA notes that there doesn't seem to be a distinction between utility implementation contractors and independent, third party

[12] By the condition of seeking access to energy-related data, the Data Ready Certification Provider will require ESEs to agree to abide by the terms of a Data Access Agreement, that reflects the requirements established by the Data Access Framework.

providers, noting that some entities may be both. The Joint Utility reply comments support party comments concerning the need for more clarity of the definition of ESE.

B. Discussion

The Data Access Framework adopted here applies to any ESE seeking access to energy-related data from a data custodian.[13] Based on the comments received regarding which entities do or do not qualify as an ESE, and specifically, concern over the applicability to utility contractors and building owner/managers, the Commission clarifies that, the Framework and the definitions included in it shall apply only to those entities seeking access to energy related data from a data custodian, for the purposes defined under the Access Considerations discussed later in this Order. This does not include entities, such as utility contractors, who are performing a service for the utilities. The utilities have existing processes and agreements with the entities with whom they are contracting with, and those processes are sufficient to protect both the utility IT systems as well as the customer data being shared. Thus, the Framework shall not apply in these circumstances.

Pertaining to building owners and compliance with mandatory building benchmarking or other local law requirements, nothing in the Framework will change the existing ability to comply with these requirements.[14] Because building owners must obtain aggregated customer data to comply with benchmarking and

[13] The data custodian will be any entity where the energy-related data are housed and being accessed, such the utility or a centralized data warehouse.

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

local law requirements, and their data access is more akin to a customer receiving their own data, they will not be considered an ESE for the purposes of Framework applicability. Moreover, the data obtained by building owners, in most instances,[15] is provided pursuant to Commission approved aggregated data privacy screens, thus mitigating the privacy concerns associated with these data transfers. Thus, the processes currently used by building owner/managers to access data will remain in place and continue to be the means by which the data is provided.

Data Access Framework Enforcement

The Whitepaper recommends that the proposed Data Access Framework incorporate the existing enforcement standards, where possible, to provide one concise enforcement process. The point at which an ESE is non-compliant shall determine the appropriate enforcement mechanism. If an ESE is not complying with the requirements for data access, there are existing enforcement mechanisms available, such as those in the Uniform Business Practices (UBP), which are tied into the ESE's ability to be an eligible Energy Service Company (ESCO) in New York State. If an ESE is certified but is not complying with Department of Public Service (Department or DPS) requirements, it is proposed that the combined enforcement mechanisms of the UBP and DPS would be used.

[15] The Commission has provided an exception to its building benchmarking privacy screen for data requests necessary to comply with local laws or ordinances. Cases 16-M-0411 and 14-M-0101, In the Matter of Distributed System Implementation Plans, Order Adopting Whole Building Energy Data Aggregation Standard, p. 11 (issued April 20, 2018) (Building Benchmarking Order).

A. Party Comments

The JU recommend strengthening of the enforcement mechanisms, stating that, currently, the only remedy is for ESEs to lose access to data. RESA comments that the existing enforcements are specific to only the ESCO and DER markets and that the Framework goes beyond the UBP provisions. As such, the UBPs would not be appropriate for use for all ESEs according to RESA. Additionally, RESA continues, the UBPs do not have consistent consequences between them which would lead to ESEs being treated differently under the same offense. RESA recommends that as part of the certification process, an ESE must accept a uniform set of compliance enforcement procedures in order to be certified, stating this would ensure equal treatment to all ESEs and could operate independently from the enforcement mechanisms of the UBP.

B. Discussion

The Whitepaper discusses enforcement of data access requirements, and in response to comments received regarding enforcement of requirements outside of data access, it is necessary to clarify that the discussion here pertains only to the ESE's ability to access data. The Commission approved UBPs have existing processes that will continue to govern the covered ESEs and their ability to serve customers in New York State. The Data Ready Certification process, as described below, will include verification that the ESE is registered and approved by the DPS before beginning the certification process that confirms the ESE has the necessary cybersecurity and privacy protections in place. If an ESE does not have the necessary protections in place they will not be certified and will not be able to access data. The Data Ready Certification Provider (Provider) shall incorporate enforcement processes to suspend or revoke

certification in the event of non-compliance with data access requirements as well as a dispute resolution process as described below, that provides recourse to ESEs as well as the data custodian.

ESE Data Ready Certification Process

A. Generally

The Whitepaper recognizes challenges ESEs have experienced seeking access to energy-related data, including inconsistent implementation and, at times, lengthy and duplicative processes with each utility. The proposed implementation of a Data Ready Certification process, that utilizes a risk-based approach for the assignment of cybersecurity and privacy requirements, is anticipated to remedy some of the challenges experienced to date. A Provider would manage the Data Ready Certification Process based upon the three main components articulated in the Whitepaper: (1) Authorized ESE Verification; (2) Access Considerations; and, (3) Verification of Requirements and Certification. To facilitate this process, Staff proposed the development of a Matrix that maps the existing Commission authorized cybersecurity and privacy requirements to the various combinations of Access Considerations (purpose, access mechanism, and data type). The Matrix would then be used by the Provider to determine what cybersecurity and privacy requirements the ESE would need to demonstrate compliance with, in order to be certified, and would ensure these requirements are consistently applied across all ESEs.

To demonstrate that the ESE has all the necessary cybersecurity and privacy requirements in place, an audit must be performed either by the Provider or through an outside party.

Once an ESE has completed the necessary requirements for approval, the ESE would be certified as Data Ready. The certification would dictate what types of data it may request to access, how they are able to access it, and would apply no matter from which utility, or data custodian, the ESE is seeking data access.

1. Party Comments

RESA and Logical Buildings support a risk-based approach to data access that ensures customer data is only shared with appropriate parties, that is applied to all similarly situated entities in the same manner. RESA comments that parameters for the selection of a Provider need to be proposed and discussed among Stakeholders, and the Commission should clarify who is ultimately responsible for selecting the Provider (such as the Commission itself or a working group), and indicate what degree of independence the Provider would have and to whom it would report. JU comments that the ESE risk management process requires refinement and development.

Recurve argues that more details regarding the process, including time for certification need to be addressed, asserting that delayed certification could create significant costs for market actors and additional procedural burdens for the entity responsible for the certification process. RESA asserts that when establishing a recertification process, the Commission should be mindful of the administrative burdens of preparing recertification submittals and should base the intervals for seeking recertification on the amount of effort required to prepare the submittal.

AEE adds that an ESE that successfully completes an audit should be exempt from additional audits through the length of its certification period unless a breach occurs. AEA asserts

that if an audit will be used to confirm necessary protections are in place, then it should focus on certain aspects and the ESE should then be exempt for the remainder of a certification period. AEE also suggests that a streamlined verification process for several recertification cycles should be considered.

Logical Buildings, NYPA, and Recurve request the Commission consider grandfathering in any currently approved ESEs and exempting them from having to go through a new certification process. They believe that the new certification process should consider previous risk information provided by ESEs, previous Data Security Agreements, and previous system testing, but, Logical Buildings, comments it is fair for supplemental items to be required if they are not confirmed by the preceding information.

AEE, AEA, and RESA submitted comments in regard to various aspects of the audit requirement. AEE and AEA recommend that, after certification, no further audit should occur, with AEE specifying that no audit should be necessary unless a breach has occurred. AEA suggested that the audit only focus on certain aspects but did not include what those aspects were. RESA requested clarification on the audit process itself.

2. Discussion

The Commission agrees that implementation of a Data Ready Certification process will resolve many of the issues that have hampered data access up to this point. The Data Ready Certification process adopted herein will replace the current Data Security Agreement (DSA) and Self Attestation (SA) process that requires an ESE to certify it has the necessary cybersecurity and privacy requirements with each utility from which it seeks access to data. Centralizing this function with a single Provider, instead of the current process of requiring

an ESE to go through the DSA/SA process with each utility, will not only ensure consistent application across all utilities and ESEs but also lead to economies of scale in the resources required to implement such an approach on behalf of the ESEs as well as the utilities. Doing so will ensure equal treatment of similarly situated ESEs, correct assignment of risk, speed up the process by which an ESE can be granted access to energy-related data, and free up utility resources that would be spent on redundant individual utility processes for ESE access requests. 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.

With regard to parties' comments related to audit requirements, the purpose of an audit is to verify that the ESE has all the necessary cybersecurity and privacy protections in place to appropriately address the risk associated with sharing data. While previously, ESE's were able to self-certify that all these protections were in place, this is no longer a sufficient means by which to verify the appropriate protections are in place to safely protect systems and customer privacy. Therefore, the Data Ready Certification process must include verification that an ESE has the required cybersecurity and/or privacy protections. This can be achieved by an audit conducted by the Provider or through the ESE's submission of an independent recognized security controls audit report, such as the SOC-II Type 2 Audit Report. Either of these audit paths will provide verification that, at the time of certification, the ESE has met the necessary requirements.

Regarding the comments requesting to not allow further audits after initial certification, the Commission clarifies

that the verification or audit of necessary requirements process discussed in the Whitepaper pertains only to the Data Ready Certification program, not the audit provision of the previously used DSA. When initially certifying, an ESE will need to have requirements verified by the Provider or provide an audit, as described above, but there is not a requirement for additional verification after an ESE has been certified. The Whitepaper proposed recertification to be completed annually to ensure ESEs have the most up-to-date requirements in place reflecting any changes, and subsequent modifications to necessary requirements, that may have occurred over the previous certification period. However, the Commission finds that annual recertification is not necessary at this time and instead will require recertification upon Commission action that changes or modifies any necessary requirements.

Recertification of requirements upon Commission action on issues, as they pertain to the Data Ready Certification, is consistent with the existing verification of cybersecurity and privacy requirements which do not require ongoing verification. In the event of a data security incident, an ESE may be required to undergo an audit consistent with existing requirements.

Though the Commission does not support the request to grandfather currently certified ESEs, the time and effort that ESEs have already invested in being certified by each utility should not be wasted. If an ESE has already met the requirements of the DSA/SA, they can demonstrate such requirements for certification by the Provider. The certification process is not meant to create further challenges for ESEs seeking access to data nor for the utilities requirement to ensure the data is kept safe.

Regarding the Provider, its role is only to certify that an ESE has the necessary cybersecurity and privacy protections in place based on their specific Access Considerations. The Provider will not determine what the requirements are, will not be facilitating access requests, nor transferring data. The Provider shall facilitate a centralized certification process that includes verification of the requirements, as determined by existing Commission policy as consolidated in the Matrix, discussed herein. Once the Provider has certified the ESE as Data Ready, the Provider will provide a Data Access Agreement specifying the applicable requirements to the ESE and the data custodian for execution, as detailed further below.

To the extent practical, the Data Ready Certification process should be modeled after other existing applications which illustrate the efficiency and consistency of such programs.[16] Understanding the concerns of RESA regarding the selection of the Provider, the Commission will require the details of the proposed Provider selection and implementation process, consistent with the details in Appendix B, to be included in a Data Access Implementation Plan to be submitted by the Joint Utilities for Commission approval. Parties will be able to comment on the proposed Data Access Implementation Plan prior to Commission action. The Joint Utilities are directed to file the Data Access Implementation Plan, within 60 days of the effective date of this Order. The Joint Utilities shall consult with the Long Island Power Authority (LIPA) in development of

[16] See, Fannie Mae, Available at: https://info.bitsight.com/sans-whatworks-case-study-fannie-mae; and, Cyber Essentials, Available at: https://www.ncsc.gov.uk/cyberessentials/overview

the Data Access Implementation Plan in order to explore the potential for cost sharing of the statewide Data Ready Certification Provider.

B. Authorized ESE Verification

As a first step in the certification process, the Whitepaper proposes that the Provider verify that the ESE is authorized and has completed all necessary DPS requirements before going any further in the certification process. To ensure that the ESE has been properly authorized by DPS, Staff proposed to develop an authorization mechanism for any ESE that is not currently subject to registration or authorization requirements through existing Commission orders. To facilitate the Provider's ability to verify this authorization, the Whitepaper proposes the creation of a centralized listing that provides the information regarding all approved ESEs.

1. Party Comments

No comments were received on this issue.

2. Discussion

Under current practices, in order for the Provider to verify an ESE is authorized by the Department, the Provider would need to look at multiple listings[17] to determine if the ESE is registered with the Department. These lists are located on different links on the DPS website, and, in some instances, the Provider may still have trouble verifying whether that ESE is registered with the Department. UBP eligible ESCOs and DER providers must currently complete a registration process with the Department in order to receive data and serve consumers in

[17] See, http://documents.dps.ny.gov/PTC/home. The Power to Choose webpage allows a user to view a listing of all registered DERS or view ESCOs that are offering products in their zip code.

the State, however, experience in other initiatives has highlighted the need to provide a registration process that includes all ESEs, not just those who fall under the two UBPs. To ensure an ESE can be verified by the Provider in an efficient and effective manner, Staff is directed to, within 90 days of the effective date of this Order, develop and implement a registration process for ESEs interested in accessing data that, currently, are not required to register with the Department.[18] The registration process should include, at a minimum, requirements consistent with the Generally Applicable requirements of the UBP DERS and a centralized process and listing to include all registered ESEs, including the current UBP eligible ESCOs and DER providers. Staff shall notice the completion of this process by submitting a letter to this proceeding indicating such.

Access Considerations

The second step of the ESE Data Ready Certification process is for the ESE to detail 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. Each of these access considerations are summarized and addressed below.

A. Purpose

The Whitepaper proposes that, 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. In most instances, having obtained

[18] This would include any ESE not currently required to register under the UBP ESCO or UBP DERS.

customer consent for the requested data access would demonstrate a valid purpose. Upon determining that the ESE either has consent or a valid purpose for requesting unconsented data based upon the access consideration purposes described below, the Provider would determine the data sets that are available for such purpose, as well as the granularity of such data, by referencing the Matrix.

Regarding valid purposes for requesting access to unconsented energy-related data, the Whitepaper proposes that such purposes include: (1) providing or reliably maintaining customer-initiated service; (2) compatible uses related to providing additional 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 Community Choice Aggregation (CCA), or to meet utility operational needs. When an ESE has obtained customer consent for the requested data access, that demonstrates a valid purpose.

The Whitepaper also recommends that unconsented access would require the data to be anonymized[19] or aggregated[20] before

[19] 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.

[20] Aggregated data are a combination of data elements from multiple accounts to create a data set that is sufficiently

access is granted, with the exception of data used for utility operational needs 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 that consent and the customer's choice.

1. Party Comments

RESA comments that ESEs should not be required to disclose the purpose for which they are requesting access to the data as part of the certification process, asserting that requiring disclosure of the purpose for seeking access to energy-related data to the Provider raises concerns about the handling of commercially sensitive information. RESA believes that demonstrating "a valid purpose" for accessing Customer Contact Information Data Set information should not be required when customers have explicitly authorized ESEs to have access to that information. To reduce the administrative burden and time for certification, RESA asserts that those seeking access to data should be required to provide all necessary information for the certification process (e.g., the type of data for which access is sought) all at once, rather than piecemeal for each step in the certification process.

Recurve and Mission:data support the use of differential privacy[21] to add "noise" and aggregate statistics in

anonymized as to not allow for the identification of an individual account or customer.

[21] Differential privacy is a system for publicly sharing information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset.

lieu of using privacy screens for aggregated data. Mission:data believes that the public release of different aggregated datasets should be tailored to the particulars of the use case, mathematically analyzed, and revisited over time as circumstances change. Since these are fundamentally important policy decisions for New York, Mission:data believes this work must be done by the Commission, and not by an integrated energy data resource (IEDR) Program Manager or third-party risk manager. Mission:data is not aware of any mathematical evaluation of the 15/15 rule as to its merits; they suspect its adoption in several jurisdictions is due more to its apparent simplicity and comprehensibility than to its empirical merits. Logical Buildings comments that data linked to a specific customer should not be provided unless the customer has consented, but non-identifiable data (aggregated / anonymized) should be provided without customer consent. The City believe aggregated and anonymized customer data should be excluded from the Framework certification process.

2. Discussion

The Framework is intended to provide a clear and consistent application of access requirements for energy-related data. To achieve this, there must be defined pathways for that access, assurance that the correct requirements are in place, and consideration of customer consent. The Commission determines that obtaining customer consent for data access demonstrates a valid purpose. With respect to unconsented data, the Commission adopts the following valid Purposes as part of the Data Ready Certification Process: (1) providing or reliably maintaining customer-initiated service; (2) compatible uses related to providing additional 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. This list includes all existing purposes for which an ESE would be seeking access to energy-related data. The Purpose access consideration is the starting point for determining what data may be available to an ESE, as well as the necessary requirements for accessing such data.

Disclosing the purpose for which an ESE is seeking access to energy-related data is an existing requirement and necessary to ensure that data is only being released for appropriate reasons. RESA requests to not have to provide its purpose to obtain data ready certification, citing confidentiality concerns. Purpose as it pertains to certification, does not require an ESE to provide the specifics of what program/offering it may be seeking data access for. Instead it is the means by which the Provider identifies what access role the ESE is seeking to be certified for.

The Commission agrees with parties' comments that if a customer has provided consent for access to its energy-related data to an ESE, it is not the Provider's, or any other entity's, role to revisit that customer's decision. When a customer has consented for their data to be shared, the terms of the consent agreement dictates what can be shared with the ESE. An ESE who is seeking access to consented customer data would not need to provide any additional information than it does currently when requesting access to that data from the utility or data custodian.

RESA recommends that in order to reduce the potential administrative burden associated with certification, an ESE should provide all necessary information for certification at one time. For efficiency and to meet the intended benefits of

instituting a centralized certification process, the Commission agrees that the Data Ready Certification process should allow for an ESE to detail all its access consideration when applying and not require and ESE to return to the certification process for each access consideration. An ESE should indicate all its access considerations when applying and request all levels of certification they are seeking during initial certification and upon recertification. In most instances, the ESE should not be going back to the Provider multiple times for changes to its certification.

The Whitepaper proposes that unconsented energy related data should only be released if it has first been aggregated or anonymized. Although both anonymized and aggregated data shall be made accessible without the need for customer consent, there is a difference between the two data privacy protections. To anonymize a customer's identity before data can be released, removing a customer's identifiable characteristics is required. Anonymization could be done through the use of a proxy identification number associated with the record or by masking a customer's identification information, such as has been done with Pilot Integrated Energy Data Resource (PIEDR)[22] which allows the non-aggregated data to be viewed but does not identify the individual customer to whom the data belongs. Aggregating data may also be a means to

[22] Case 18-E-0130, In the Matter of Energy Storage Deployment Program, Order Establishing Energy Storage Goal and Deployment Policy (issued December 13, 2018). The Storage Deployment Order directed DPS Staff and the New York State Energy Research and Development Authority (NYSERDA) to lead coordination efforts with the Joint Utilities, Long Island Power Authority (LIPA), New York Power Authority (NYPA), and other stakeholders to develop and implement a Pilot Integrated Energy Data Resource (PIEDR) with the assistance of a third party platform provider.

create anonymization, however, there are instances when data should be anonymized without the need to combine a customer's usage with another customers' usage. Identifying additional potential mechanisms by which unconsented energy-related data may be shared that does not require aggregation but still provides the necessary privacy protections is still being explored.

The Commission has long held that the ability to obtain aggregated customer usage data allows for the development of energy planning, including the offering of innovative products and services, that can potentially provide benefits to customers and further the State's Clean Energy goals. To balance the need for the data with the need to ensure customers' privacy is protected, the Commission has adopted aggregated data privacy screens for several use cases. In its Distributed System Implementation Plan (DSIP) Order,[23] the Commission adopted a 15/15 privacy screen[24] for community-wide aggregated data use cases, which was applied for use in CCA programs and subsequently applied to the Utility Energy Registry[25] (UER) residential sector screen. Recognizing that the 15/15 may have

[23] Case 16-M-0411, In the Matter of Distributed System Implementation Plans, Order on Distributed System Implementation Plan Filings (issued March 9, 2017) (DSIP Order).

[24] This privacy screen dictates that in order for a data set to be sufficiently aggregated so as to preclude the identification of individual customers within the data set, the data must include at least 15 customers, with no one customer accounting for more than 15% of the total consumption.

[25] Case 17-M-0315, et al., In the Matter of the Utility Energy Registry, Order Adopting Utility Energy Registry (issued April 20, 2019) (UER Order).

been a conservative standard, and to ensure community planning and CCA programs were able to receive the quality of data needed, the Commission required each utility or platform provider to monitor, track, and report on the failure rates of the 15/15 aggregated data privacy screen. Regarding building energy management and benchmarking, the Commission found in the DSIP Order that the 15/15 would not be able to be used because it would significantly limit the number of buildings able to report on its building energy consumption and directed the utilities to work with Staff and interested parties to develop an aggregated data privacy screen for whole building aggregated data. For this purpose, a 4/50 aggregated data privacy screen[26] was developed and adopted by the Commission for the release of whole building aggregated data.[27]

Since these aggregated data privacy screens were adopted, there has been significant confusion related to the correct application of aggregated data privacy screens, use case instances of high failure rates, as well as reports that the 15/15 privacy screen is unbalanced, being too restrictive and blocking access to valuable data by preventing the data from being published. For CCA programs that currently have the 15/15 aggregated privacy screen in use, the inability to receive full community data due to high failure rates has led to significant

[26] Similar to the 15/15 privacy screen, the 4/50 standard dictates that in order for a data set to be sufficiently aggregated so as to preclude the identification of individual customers within the data set, the data must include at least four customers, with no one customer accounting for more than 50% of the total consumption.

[27] See, Building Benchmarking Order. The Commission also adopted an exemption to the 4/50 privacy screen for data requests made in compliance with local laws.

issues with implementation of the programs and, in some instances, CCA program administrators have turned to the UER to try and analyze the missing CCA data. However, due to the UER's high privacy screen failure rates, this has not been a workable solution.

On December 30, 2019, NYSERDA filed a UER Status Report[28] as directed by the Commission in the UER Order. The UER currently uses two different privacy screens[29] and, as detailed in the UER Status report, when applied result in a significant amount of data being withheld from the UER. As reported, only 47% of communities have access to a complete 12-month residential and non-residential data set, and only 28% percent of communities have access to a complete 12-month data set needed to estimate CCA load. Though it is vital to balance the benefits of data transparency and customer privacy, if data is not available to a given community due to imbalanced privacy screens, the UER has limited value to that community. The UER Status report recommended that in order to increase access to community-wide aggregated data, a screen that relied solely on a customer count of 4 should be applied.

The 15/15 aggregated data privacy screen adopted in the DSIP Order was clearly identified as being a starting point and the Commission recognized then that this screen may need to change based upon actual implementation and use. With the feedback from CCA program administrators, market participants,

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

[29] The residential sector screen is 15/15. If there are less than 15 accounts, or if one account is more that 15% of the total, the entire sector is withheld. The screen for non-residential sectors is 6/40.

and the UER Status report all identifying issues related to the current privacy screens, the Commission finds the 15/15 aggregated data privacy screen must be modified to allow community energy planning data to be made available at a level that ensures it can be used for its intended purpose. In evaluating alternative approaches, the 4/50 whole building aggregated data standard has demonstrated a balance between the protection of customer's identities and the broader interest of the public. For that reason, the Commission hereby establishes a statewide aggregated data set privacy screen of 4/50 to be applied generally to all aggregated data sets reporting monthly or annual energy usage totals. The 4/50 privacy screen will replace all existing Commission approved privacy screens and become the starting point from which use case specific screens may be developed. In the case where a data access application or initiative, such as the UER or IEDR, adopts a privacy screen distinct from the 4/50 privacy screen, that differentiated privacy screen shall be applied solely to that use case or application addressed, unless otherwise directed by the Commission. All aggregated data sets that pass the 4/50 privacy screen shall be made accessible upon request.[30]

B. Transmittal or Access Mechanism

The Whitepaper asserts that cybersecurity protections need to be in place for access to energy-related data, but that there are varying degrees of cybersecurity risk depending on the

[30] In its DSIP Order, the Commission adopted a 15/15 privacy screen for aggregated data sets, requiring the utilities to furnish aggregated data which satisfies that privacy screen. The Commission now modifies the 15/15 privacy screen for aggregated data set use cases to match the 4/50 screen adopted in the Building Benchmarking Order.

mechanism used for accessing or transmitting the data. Regarding the transmittal or access mechanism, the Whitepaper states that data is able to be transmitted by either electronic or non-electronic means. The means by which data is being shared determines what, if any, cybersecurity protections are necessary to protect the data custodian's IT system. The identified transmittal or access mechanisms are: (a) direct connection to the data custodian's IT system; (b) secure platform/portal; (c) public platform/portal; and (d) email or other non-direct electronic connection.

1. Party Comments

No comments were received on this issue.

2. Discussion

As the Commission recognized in its Cybersecurity Order,[31] there is a difference in the cybersecurity risk associated with the mechanism by which data are being shared. Direct connection to the utility, or data custodian's, IT system presents a higher risk and, as such, would require more protections be in place before access is allowed. A secure platform/portal, such as Green Button Connect (GBC), when properly implemented, is typically located on a separate server from that containing any highly confidential personal information and may have protections built into the platform. Access to publicly available platforms/portals, such as the UER, would not require an ESE to have cybersecurity protections as it is not directly connected to the data custodian's IT system.

[31] Case 18-M-0376, et al., Proceeding on Motion of the Commission Regarding Cyber Security 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).

Consistent with the Cybersecurity Order, An ESE seeking access to data via email or other non-direct electronic connection would not be required to have its cybersecurity protections verified by the Provider.

The Commission adopts the following transmittal and access mechanisms for use in the Framework, and incorporated into the Matrix: (1) direct connection to the data custodian's IT system; (2) secure platform/portal; (3) public platform/portal; and (4) email or other non-electronic connection.

C. Data Type Requested

With respect to the data type requested, the Whitepaper states that the type of data an ESE is requesting access to would determine what the necessary privacy requirements should be, as defined in the Matrix. Data are initially considered in two separate categories, Customer Data and System Data. In addition to the evaluation of the privacy risk associated with the data type being requested, customers' right to choose to share their data must also be recognized and considered.

1. Customer Data

To empower customers and enable access to data in a uniform and consistent manner, the Whitepaper recommends adoption of defined customer data sets to be used by the Provider when determining the necessary privacy requirements for ESE access to energy-related data. Those data sets are the Customer Energy Usage Data Set, the Customer Contact Data Set, and the Customer Billing Data Set. While there are many data points included in each data set, no highly confidential personal information, such as social security number or banking

information, is available or included in any of these defined Data Sets.

a. Party Comments

Mission:data wants to know more about the types of data to be provided to customer-authorized third parties. It believes the data types outlined in the UBP-DERS are inadequate to animate DER markets, and propose additional data points including: historical and ongoing energy usage; historical and ongoing line items on bills; the rate each customer is on; and any information necessary to determine eligibility for, or participate in, a demand response, energy efficiency, or renewable energy program. RESA also believes that the Customer Billing Data Set information should include bills themselves as this information will help ESEs respond to customers who have questions about the ESE components on utility consolidated bills and about how ESE products affect their bills. RESA believes the Commission should consider a period of at least twenty-four months of historical data in the Customer Energy Usage Data (CEUD) Set so that ESEs can see changes in annual usage patterns. Additionally, RESA asserts that all ESEs and other market participants should have access to AMI meter data on the same basis.

b. Discussion

The Commission adopts the following data sets associated with the Customer Data Type: Customer Energy Usage Data Set, Customer Contact Data Set, and Customer Billing Data Set as detailed in Appendix A, for use in the Framework. This allows for the categorization of multiple data points already available, as well as any new data points that may become available under each set. All existing customer data points currently available to ESEs, as defined by the governing UBP,

have been incorporated into the three defined customer data sets of the Customer Data Type, and are detailed in Appendix A. This will ensure that all ESEs have equal access to currently available data points, regardless of company type. Multiple comments were received requesting expansion of the available data points included in both data types. Modification to the data sets included in the Framework is discussed in the Continuous Improvement section below.

2. System Data

For system data, except for those pieces of system data that may impact customer privacy or critical infrastructure protection, the Whitepaper proposes that there should be no protections on the availability of such data, since it is aggregated data itself. Also, since it is not CEUD, it is not subject to customer consent and, therefore, system data should be made available to the public. Currently, some of the utility's hosting capacity maps are public, while others require user registration with the utility. The Whitepaper recommends that users should not be required to register with the utility prior to accessing hosting capacity maps.

a. Party Comments

The Joint Utilities comment that with respect to types of data, the Whitepaper defines three categories of data (i.e., highly confidential/sensitive not to be shared, other types of data to be shared with consent, and anonymized data). They comment that these categories appear to be aimed at customer data and recommend a stakeholder process to define a standardized set of data access roles. They believe the stakeholder process should be used to develop a set of classifications to apply to system data. They also state that the current no-fee registration, requiring an email address, for

access to Hosting Capacity Maps should be continued because it allows for (1) relevant communication of operational information between utilities and users; (2) transparency into the number of users and the manner of use that can inform system improvements; and, (3) perhaps most importantly, gives the utility a means to shut off bad actors. The Joint Utilities request that this aspect of the Framework be modified, and users be required to continue to register with an email address.

b. Discussion

The Commission adopts System Data as the second of two data types for use in the Framework. The Commission agrees with the proposal in the Whitepaper that there should be no protections on the availability of Hosting Capacity data, since it is aggregated data itself and does not contain CEUD. The Commission disagrees with the Joint Utilities' comments regarding requiring ESEs to register as a user prior to gaining access to Hosting Capacity Maps. Within 30 days of the effective date of this Order, all distribution utilities shall remove the current user registration requirement to access Hosting Capacity Maps. Finally, as future applications, initiatives, and use cases containing system data are developed, specific policies pertaining to system data access shall be developed accordingly within this proceeding.

D. Verification of Requirements and Certification

After the ESE has provided the necessary access consideration details, the Provider would advise the ESE what cybersecurity and privacy requirements would apply. To facilitate the certification process, the Whitepaper 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 Framework. The Whitepaper envisions the Matrix to be used by the Provider to determine what cybersecurity and privacy requirements an ESE would need to demonstrate compliance, through testing or audit, in order to be certified.

Once the Provider verifies that the ESE has the necessary cybersecurity and privacy requirements in place, the ESE would be certified as Data Ready and the certification access role would identify the types of data it may request access to, as well as the transmittal mechanisms it is able to utilize. The access role is based upon the access considerations and the verification of meeting the necessary requirements.

1. Party Comments

AEE supports the certification process, but states that the Framework is unclear how confirmation of the privacy and cybersecurity requirements will be done. AEA, JU, and Mission:data comment that utility liability needs to be addressed. Recurve comments that there needs to be a clear liability framework for all market actors (custodians, users, customers). AEE believes that utilities are currently not motivated to provide data as they are liable for third-party data breaches and do not financially benefit from data sharing. The Commission has not addressed liability of the utilities in the event of a data breach, leaving the utilities to be overly cautious, according to AEE. AEE recommends a two-part indemnification where the Commission states that utilities bear no liability for third-party negligence or wrongdoing and provides financial indemnification through cost recovery of any legal fees and settlements.

AEA and AEE support the development of a risk-based matrix for data access and believe that data access requirements

should be based on potential risk rather than a one-size fits all approach. RESA states that the development of any cybersecurity requirement based on the Matrix should not favor one market participant over another. Joint Utilities identify the matrix as a key component of cybersecurity and privacy guidance but claim that the development process for the Matrix is unclear and assert that until further work is accomplished, the identification of appropriate roles is premature. AEA, AEE, and Joint Utilities all call for stakeholder working groups, meetings, and/or a review process to develop the Matrix. RESA recommends that qualified personnel work on developing the components of the security matrix and that they should not be affiliated with any market participants.

The Joint Utilities recommend further stakeholder discussions regarding the relationship between cybersecurity and transmittal or access mechanisms and privacy requirements, asserting that cybersecurity and privacy requirements cannot be easily separated.

2. Discussion

The Commission finds that to facilitate the certification process, a Matrix that maps the existing Commission authorized cybersecurity and privacy requirements to the various combinations of purpose, access mechanism, and data type is necessary to ensure consistent application of the Framework throughout the State and across ESEs. The Matrix shall be used by the Provider to determine what cybersecurity and privacy requirements an ESE would need to demonstrate compliance, through testing or audit, in order to be certified. In its Cybersecurity Order, the Commission recognized a clear separation between what requirements are necessary when seeking access to data by requiring cybersecurity protections for direct

IT system connection to the data custodian and privacy requirements for certain types of customer data. Therefore, to create the Matrix that will recognize this distinction and go a step further by ensuring these requirements are not applied as a one size fits all approach, Staff is directed to separate the cybersecurity and privacy protections and correctly assign them to the applicable access consideration. The Commission finds this separation of existing requirements to be consistent with previous Commission actions and in line with the risk-based approach adopted herein to facilitate access to data in a protected manner.

While parties provide support for the use of the Matrix, some suggest that the Matrix be developed through various forums, with the JU asserting that cybersecurity and privacy cannot be easily separated or related to the access considerations. As described in the Whitepaper, the Matrix is not creating or modifying the existing cybersecurity and privacy requirements. Simply put, the components of the existing statewide DSA and SA, as well as the use case specific agreements, will be incorporated into the Matrix, and those same requirements, as separated in the Cybersecurity Order, will likewise be distinguished in the Matrix. Therefore, the Commission rejects JU's assertions as this separation currently exists today. With regard to parties' comments calling for more involved processes to enable the creation of the Matrix, we find this to be unnecessary and could, potentially, lead to further delays in developing the Matrix that will serve to facilitate the actions taken in this Order, without corresponding benefit. That said, we acknowledge parties' comments and agree with the objective of wanting to ensure the Matrix is properly created and maintained to support our objectives. To address these

comments, Staff is directed to file, within 30 days of the effective date of this Order, the Matrix that shows how each existing cybersecurity and privacy requirement has been mapped to an access consideration and allow Stakeholders the opportunity to provide feedback. Staff will then review the stakeholder comments and file an updated version of the Matrix that shall then be applied by the Provider when determining Data Ready Certification of an ESE.

Several comments were received regarding liability and the Commission agrees that liability must still be addressed in any data access agreements. The sections of the previously used DSA that were not cybersecurity or privacy protections, including liability, are incorporated into the Data Ready Certification and will be included in the Data Access Agreement that an ESE will have to agree to. The Data Access Agreement requirements are discussed further below.

The process for an ESE to receive its Data Ready Certification from the Provider is meant to facilitate access to data in a uniform, singular process for verification of the necessary cybersecurity and privacy requirements. The Commission adopts the proposed Data Ready Certification process and requires the JU to include the details, consistent with this Order and the details provided in Appendix C, in the Data Access Implementation Plan.

As part of the Data Ready Certification Process, the ESE will be provided with an electronic Data Access Agreement that details the terms of the agreement and includes the necessary cybersecurity and privacy requirements that must be maintained for certification. This agreement will be generated by the Provider and provided to the ESE and data custodian for

execution. The Data Access Agreement shall include, at a minimum:

- ESE name, designated contact, phone number, and email;
- Provider contact information;
- Agreement between parties and the general terms taken from the currently in-use DSA;
- Applicable cybersecurity requirements;
- Applicable privacy requirements;
- Notice of re-certification requirements and results of failure to comply; and
- The dispute resolution processes detailed below.

Dispute Resolution Processes

The parties shall in good faith use reasonable efforts to resolve any dispute before invoking these processes. The Data Access Agreement between the parties shall identify the processes used to resolve disputes and shall refer to the dispute resolution processes described in this Section as acceptable processes to resolve disputes.

A. Standard Process

The parties shall use a method to send documents described in this paragraph that will verify the date of receipt. Any distribution utility, ESE, or Direct Customer[32] may

[32] Section 1 of the ESCO UBP defines a Direct Customer as an entity that purchases and schedules delivery of electricity or natural gas for its own consumption and not for resale. A customer with an aggregated minimum peak connected load of 1 MW to a designated zonal service point qualifies for direct purchase and scheduling of electricity provided the customer complies with NYISO requirements. A customer with annual usage of a minimum of 3,500 dekatherms of natural gas at a

initiate a formal dispute resolution process by providing written notice to the opposing party and Department Staff. Such notice shall include a statement that the Data Access dispute resolution process is initiated, a description of the dispute, and a proposed resolution with supporting rationale. Department Staff may participate in the process at this or any later point to facilitate the parties' discussions and to assist the parties in reaching a mutually acceptable resolution.

No later than ten calendar days following receipt of the dispute description, if no mutually acceptable resolution is reached, the opposing party shall provide a written response containing an alternative proposal for resolution with supporting rationale and send a copy to Department Staff.

No later than ten days after receipt of the response, if no mutually acceptable resolution is reached, any party or Department Staff may request that the parties schedule a meeting for further discussions. The parties shall meet no later than 15 calendar days following such request, upon advance notice to Department Staff, unless the parties and Department Staff agree upon another date. The Department may assign one or more Staff members to assist the parties in resolving the dispute.

If no mutually acceptable resolution is reached within 40 calendar days after receipt of the written description of the dispute, any party may request an initial decision from the Department. A party to the dispute may appeal the initial decision to the Commission. If the parties reach a mutually acceptable resolution of the dispute, they shall provide to

---

single service point qualifies for direct purchase and scheduling of natural gas.

Department Staff a description of the general terms of the resolution.

B. Expedited Process

In the event that an emergency situation arises to justify immediate resolution of a dispute, any party may file a formal dispute resolution request with the Secretary to the Public Service Commission asking for expedited resolution. An emergency situation includes, but is not limited to, a threat to public safety or system reliability, or a significant financial risk to the parties or the public. The filing party shall provide a copy of the request to other involved parties and Department Staff. The request shall describe in detail the emergency situation requiring expedited resolution, state in detail the facts of the dispute, and, to the extent known, set forth the positions of the parties.

Data Responsibilities and Relationships

The Whitepaper acknowledges that 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 Whitepaper considers these responsibilities in three ways: data access fees, data quality and integrity, and reporting.

A. Data Access Fees

The REV Track Two 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.[33] The basic level of customer data that is to be provided free of charge is defined as the usage for each applicable rate element, including usage bands specified in the applicable tariff. The REV Track Two Order explained that this is the level of data necessary to render, reconstruct, and understand the customer's bill, which will ensure that customers have ready access to information necessary to fully understand how their energy usage affects their energy bill. 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 Commission permitted utilities to charge a fee for access to aggregated community load data, as well as the customer information needed to facilitate CCA opt-out mailings.

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

[33] Case 14-M-0101, supra, Order Adopting a Ratemaking and Utility Revenue Model Policy Framework (issued May 19, 2016) (REV Track Two Order).

create a centralized and automated process for data access, Staff recommends abolishing all data fees, including the fees for CCA related data.

1. Party Comments

Logical Buildings agrees that no fees should be associated with a customer or a third-party obtaining access to customer utility data as data is necessary for development of new energy products, and access fees would discourage such development. Additionally, Logical Buildings asserts that access fees would drive up costs for customers complying with existing energy usage reporting regulations. RESA strongly supports abolishing data access fees. AEE recommends that fees for data should only be applied to special data requests that may impose unique costs on the utility, and that in those cases, the price should be cost-based.

2. Discussion

Utility system capabilities have evolved over time and are now able to automate data processing, eliminating the basis for utilities being permitted to charge fees for energy-related data. Within 60 days of the effective date of this Order, and with the exception provided below, all distribution utilities shall modify their current tariffs to remove all established fees associated with the release of customer data, including CCA data, and system data. However, the Commission recognizes that certain data requests, particularly those requesting data for an extended historical time period, may impose additional costs on utilities if the data requested has been moved to an alternate server, or is archived. Thus, the Commission hereby limits requests for free-of-charge historical energy usage data to the most recent 24 months of customer usage. The utilities are permitted to charge cost-based fees for provision of historical

energy usage data in excess of 24 months, if the process to complete that request is not able to be automated.

B. Data Quality and Integrity

As previously discussed, 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. The Whitepaper acknowledges that each utility is operating with different IT systems, and concludes that such differences should not prevent the ability to provide standardized data as an output. The Whitepaper describes that energy-related data should be portable, and in order for customers to have the ability to share their data with any ESE, through whatever means they have chosen, available energy usage data should be provided in a standardized manner. Along these lines, the Whitepaper sought 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 being met.

1. Party Comments

AEE supports the standardization of data formats to facilitate third party entry and lower overall implementation and customer acquisition costs. AEE notes that it can take time and effort to ensure that all actors have worked on and developed a standardized data format, and points to the delays and difficulty in implementing Green Button Connect in New York. As such, AEE recommends that substantial cooperation between utilities, software vendors, and users will be needed. Since development of these standards will likely take time, immediate focus should be on those standards most needed, including the

identification of most likely use cases, before moving to future needs.

Mission:data comments that utilities, not third parties, are responsible for data quality and that the Whitepaper misunderstands the challenges associated with GBC platforms. Mission:data notes that data quality is an absolute challenge for the utilities and an area that will need to continuously be addressed.

NYSERDA notes the importance of data standardization. However, NYSERDA states that "there must be a clear regulatory mandate and protocols for the regulated utilities in New York to make grid-related and customer energy consumption data available ensuring the spatial and temporal granularity to create useful data sets."[34] The City recommends that data be available in its preferred data format; the U.S. Department of Energy's Building Energy Data Exchange Specification (BEDES).

AEA states that existing data protocols should be maintained and not become more costly. Additionally, provision of data should continue while a new system is being considered and implemented, according to AEA.

Joint Utilities suggests that lessons learned from existing data access programs should be used to inform future data access mechanisms. Joint Utilities also request clarification on the scope of the data quality and standardization purpose. They note that data is collected for a particular purpose so "data quality and integrity require that the use of data be aligned with the manner and purpose for which the data were collected."[35] Joint Utilities also raise questions

[34] NYSERDA comments, p. 4.

[35] Joint Utilities comments, p 21.

regarding the development of data quality and integrity standards at this time when further refinement is needed.

RESA supports making data available to all stakeholders in a standardized manner. Logical Buildings agrees on importance of having data quality and integrity standards so that there is trust in the accuracy of the data, while still making the data available in a flexible format.

2. Discussion

The Commission agrees that the utilities, not third parties, are responsible for data quality and integrity since they are, at this time, the custodian of the data being accessed by the ESE. In other words, whomever the data custodian is will be the entity responsible for ensuring the data is compiled and provided in conformance with any established data quality and integrity standards.

The purpose of establishing data quality and integrity standards is to ensure that all data transmitted from the data custodian is provided in a reliable, standardized, and usable format to market participants. Having access to data that may not be accurate or requires time consuming work to make it usable is contrary to the purpose of providing access to the data to begin with. Data quality and integrity standards will ensure that, amongst other requirements, the data is accurate and transferred in a timely manner, that technical support is available, and that the data format is in conformance with applicable standards.

While the actual standards may vary from one use case or application to another, all data transfers should include accurate data, free of redundant or extraneous entries, that is sufficiently up to date for its intended use. There are also a number of data quality and integrity categories that would apply

universally. The Commission adopts the following data quality and integrity categories in the Framework:

1. Adherence to a standardized data format specific to the data access mechanism;
2. Maximum percentage of data that includes redundant or extraneous entries;
3. Maximum percentage of data errors;
4. Maximum amount of time it will take to transfer data;
5. Maximum amount of time to acknowledge a reported data error;
6. Maximum amount of time to resolve a data error;
7. Notification of data access mechanism outage or downtime;
8. Conformance to application standard, including 3rd party certification, if one exists, such as for GBC;[36] and,
9. Technical support information, such as contact and maximum amount of time to respond to and resolve issues that arise.

These Data Quality and Integrity Standard categories will act as statewide guidelines that shall be applied, at a minimum, to all data access applications or use cases. To fully understand what the current state of data access mechanisms are for each utility, the Commission directs each utility to file a complete listing of its current data access use cases and applications and include current status of the above discussed Data Quality and Integrity Standard categories, and for any data access mechanisms still in development, the anticipated

[36] Green Button Alliance certification.

completion date. Such filings shall be made within 90 days of the effective date of this Order. These filings shall be filed in this proceeding as well as the use case or application's associated proceeding, if one exists.

C. User Agreement

The Commission finds that most, if not all, agreements and requirements imposed on data access to date have focused solely on the responsibilities of the ESE seeking data access and have not addressed the expectations and responsibilities of the data custodian, currently the utilities. This one-sided approach is not acceptable nor will it further the Commission's goals with regard to the strategic use of energy data. The expectations and responsibilities placed upon both the ESE and the utility or data custodian must be clearly identified and mutually accepted.

The Commission will require use case specific User Agreements[37] to be created that shall include, compliance to standards associated with the data quality and integrity categories included in the Framework, as well as any other terms the data custodian and ESE must comply with. The Commission envisions the User Agreement to be facilitated in an electronic manner as a pop-up box displayed on a data custodian's online data access application or portal. The terms of the User Agreement will be displayed in the box and by clicking the box, an ESE will indicate they have read, understood, and agree to the terms and conditions of the agreement. This practice is

[37] An agreement between a utility or data custodian and an ESE that establishes the responsibility between parties, including, among other things, the applicable data quality and integrity standards applicable to that use case or application.

currently being used in PIEDR and has shown to be an effective means by which an ESE is provided the application specific details for that platform.

As detailed in the Whitepaper, the success of GBC has largely been hampered by inconsistent implementation by the utilities, ESE onboarding problems, and the lack of transparent terms and conditions that apply to both the ESE and the utility. In its Accelerated EE Order, the Commission directed Staff to work with stakeholders and the utilities in developing the terms and conditions necessary for GBC and, in the event that stakeholders and utilities were unable to come to an agreement, propose terms and conditions for consideration by the Commission, based on those utilized in other jurisdictions. Stakeholder meetings were held on February 21, 2019, and March 26, 2019, to discuss what should be included in the terms and conditions, however discussions were not able to move past cybersecurity and privacy requirements as, at that time, the Commission had yet to take action establishing these requirements.[38] On October 15, 2019, the Joint Utilities filed a Green Button Report, providing a status of the discussions.[39] The utilities asserted in this report the GBC terms and conditions were integrally dependent upon the Commission's action on a form of the DSA. Given the timing of a Commission

[38] At the time of the GBC collaborative the Commission was considering the requirements of the Data Security Agreement (DSA) in Case 18-M-0376, Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place. The Joint Utilities had filed a form of DSA in this proceeding on February 4, 2019.

[39] Case 18-M-0376, et al., Joint Utilities Status Report on Green Button Connect My Data® (filed October 15, 2019) (Joint Utility Green Button Report).

action was unknown at the time, and some utilities had already implemented GBC, the report provided the terms and conditions in place for Con Edison and Orange & Rockland. These terms and conditions consisted of two basic requirements: (1) a signed DSA, including a self-attestation; and (2) a detailed ESE on-boarding process. The report and the described terms and conditions contained therein were silent on the performance characteristics the ESE should expect from the utilities or the process for addressing any data quality or access issues. ESE's disagreed with the Joint Utilities' position, stating that GBC has protections built into the platform and as such, ESEs should not be required to additionally sign the DSA/SA. The disagreements over the necessary cybersecurity and privacy requirements will now be settled by the adoption of the ESE Data Ready Certification process and by requiring the filing of use case specific User Agreements, as detailed herein, for Commission consideration.

At the time of the Joint Utility Green Button Report, customers in Con Edison and Orange & Rockland territories were able to share their data with two ESEs, with another twenty-five ESEs in various stages of the onboarding process. The Commission finds this level of progress, particularly given Con Edison's GBC has been active since 2017, unacceptable and wholly insufficient for meeting the needs of customers looking to engage in the DER markets and for ESEs to meet these needs.

In order for GBC to move forward in a meaningful way, clearly defining the responsibilities of each party is necessary. Therefore, the individual utilities are directed to file a GBC User Agreement that includes the details of the data quality and integrity standards defined above within 60 days of the effective date of this Order. The Commission directs the

utilities to develop the functionality to execute the GBC User Agreement in an electronic manner facilitated through a pop-up window on their GBC webpage. The Commission will adopt the terms of a GBC User Agreement after public comment.

The User Agreement shall not include the cybersecurity and privacy requirements necessary for GBC as those will be handled through the ESE Data Ready Certification process and reflected in a Data Access Agreement, as described herein. The Commission notes that nothing required in this Order should result in the suspension of data currently being provided through existing GBC platforms. Additionally, to ensure consistency amongst utility implementations and equal treatment from Commission directives, the User Agreement must include that the utility GBC platform has been certified by Green Button Alliance[40] as being compliant with the GBC Standard.

Accompanied by the filed GBC User Agreement, the Joint Utilities shall file details regarding the GBC third party on-boarding process, including associated timelines, specific to each utility's onboarding procedures. Going forward, the GBC collaborative's work will become part of this proceeding.

D. Earning Adjustment Mechanisms and Performance Metrics

The Whitepaper sought comments on the type of performance metrics to use to determine if the Data Quality and Integrity Standards, once established, are working.

1. Party Comments

As a way to encourage utilities to increase data transfers and improve customer engagement, comments were received in support of establishing Earning Adjustment Mechanisms (EAMs) for data access. AEE states that utilities

[40] https://www.greenbuttonalliance.org/certification.

should be financially motivated to want to share customer usage data and establishing an EAM based on greater customer engagement and transfers with authorized third parties would result in encouraging utilities to provide an improved user experience. Furthermore, according to AEE, an EAM would be better than setting up a fee-per-transaction structure since AMI and associated infrastructure are already recovered in rates, setting up rate structures outside of a monopoly service model can be contentious, and any fee ultimately adopted may be prohibitive to third parties.

Mission:data states that New York utilities have no financial incentives to support or provide successful mechanisms to enable sharing of customer data. Mission:data describes the existing incentives for a utility as creating a process that no one uses but meets the minimum requirements for cost recovery. Mission:data recommends the Commission create an EAM that rewards utilities for greater customer utilization of Green Button Connect.

Mission:data notes that the following metrics could form the basis of an EAM, as they are equally applicable to the IEDR as they are to an individual utility's GBC platform: (1) the number of completed data-sharing authorizations; (2) time elapsed for a random sample of customers to complete a data-sharing authorization with a third party; (3) the percentage of data-sharing attempts that are successful (searchable timeframe); (4) average and maximum data delivery time (seconds) following customer authorization (searchable timeframe); (5) GBC system availability (uptime); (6) Number and type of errors generated, if any; (7) number and type of issues raised by third parties and customers, including severity, mean and max acknowledgment time, and mean and max resolution time; (8)

number of complaints received from third parties, including type and severity; (9) number of customers with one-time and ongoing data-sharing authorizations; and, (10) time to complete third party technical and administrative onboarding.

2. Discussion

With regard to parties' comments requesting EAMs to motivate utilities to improve data access performance, the Commission agrees with the objective sought – improved utility performance in customer engagement and third-party access to data. However, at this time, the Commission disagrees that EAMs are the appropriate path to achieve this objective. In general, EAMs should be reserved to motivate and reward utilities for exceptional performance above and beyond certain metrics, not for merely performing a job expected of them and in compliance with Commission orders. The actions taken in this Order are meaningful in providing clear direction to the utilities as to the expectations placed upon them by the Commission. Upon implementation of the Data Access Framework and the adoption of User Agreement(s) that will clearly articulate Data Quality and Integrity Standards and other applicable terms, for the first time, the Commission will have standards for which Data Performance Metrics shall be reported and tracked to properly assess utility performance in this area. As with many other regulatory requirements, these standards/metrics could be incorporated into specific performance mechanisms in the future with associated negative revenue adjustments for non-compliance.

Data Performance Metrics will differ depending on the use case or application. As an example, GBC or other consent mechanisms will be required to report on data-sharing authorizations while other use cases that contain aggregated or anonymized data, such as building benchmarking or CCA, will not

be applicable to consent metrics. Data Performance Metrics shall be established for all data access use cases and applications with the exception of public facing use cases and applications, such as UER and Hosting Capacity Maps. Public facing applications publish aggregated data in a transparent manner which is open and available to the public and therefore, will not be required to establish Data Performance Metrics as the data being shared is not being transferred from a data custodian to an ESE.

Data Performance Metrics to be used to track and assess utilities performance in greater customer engagement and third-party data access shall include, if applicable, but not be limited to, the following:

1. The number of completed data-sharing authorizations, including the number of customers with one-time and ongoing data-sharing authorizations;
2. Time elapsed for a random sample of customers to complete a data-sharing authorization with a third-party;
3. The percentage of data-sharing attempts that are successful;
4. Average and maximum data delivery time (seconds) following customer authorization;
5. Number and type of errors generated, if any;
6. System availability (uptime), GBC applicable;
7. Unplanned Outages (downtime), not related to scheduled system maintenance, date, reason, length of outage, and whether notification of outage and/or restoral was provided;
8. Number and type of data issues raised by third parties and customers, including severity, mean and max acknowledgment time, and mean and max resolution time;

9. Number and type of access mechanism issues or complaints received from third parties, including type and severity;
10. Time to complete third-party technical and administrative onboarding;
11. Number of third parties in various stages of onboarding;
12. Accuracy of data transferred; and
13. Percentage of data that includes redundant or extraneous entries.

The Joint Utilities shall include a proposed process for reporting on these metrics in the Data Access Implementation Plan.

E. Reporting, Auditing, and Accountability

Annual reporting requirements for data access 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, the Whitepaper proposes to incorporate all the reporting requirements into one primary report to ensure that all the necessary components are available for the proper evaluation of access to energy-related data. The Whitepaper sought input from stakeholders as to the frequency of any required reporting, as well as whether there were specific metrics that should be captured for determination of the success of the Data Access Framework.

1. Party Comments

RESA supports streamlining reporting by incorporating disparate reporting requirements into a single annual report to replace existing annual reporting requirements and to coincide with the annual Data Access Market Participant Input Session. RESA further states that the single report should be filed reasonably in advance of the annual Input Session to allow the

meaningful review of report before the session and to inform participant discussions.

The City of New York recommends that entities seeking ESE Certification should document and submit to the Commission a report that explains the time and effort they spent to achieve ESE Certification to allow the Commission to set a benchmark for the process.

2. Discussion

There is significant value to the components and metrics included in reporting requirements that can facilitate evaluation of programs and highlight areas that may benefit from modification. RESA recommends incorporating requirements into a single annual report to coincide with the Data Access Market Input Session, as described below. The Commission agrees that, once established, requiring the report to be filed annually prior to the Data Access Market Input Session would allow parties to discuss and potentially make recommendations for modification. The Data Access Market Input Session, discussed below in the Continuous Improvement section, will be an annual stakeholder conference that will be established, by Secretary's Notice, in a subsequent phase of this process once the Data Ready Certification is operational.

While the Whitepaper proposes incorporating all the existing data access reporting requirements into one report, the Commission finds further evaluation and identification of these existing reporting requirements must first take place. To this end, Staff is directed to identify the required data related reporting requirements and file an outline for a single report

prior to the initial Data Access Market Input Session.[41] This will allow time for review and facilitate discussion on this topic by all parties at the Data Access Market Input Session.

In addition to the establishment of a single report, the whitepaper also sought input on Framework specific metrics, as well as the frequency of such reporting. The City of New York recommended individual ESEs file reports detailing the time and effort it took for certification. Understanding the potential impact that the Data Ready Certification process may have on ESEs is essential for evaluating whether the process is creating efficiencies as intended or may need modification. However, requiring reporting from all ESEs could be burdensome. Instead of placing additional requirements on all ESEs seeking access to data, Staff shall, prior to the initial Data Access Market Input Session, provide a survey to ESEs that includes, among other things, questions regarding the Data Ready Certification process.

Regarding metrics and reporting on the Provider side, the Commission finds that initial reporting metrics should be established that encompass the steps within the Data Ready Certification process. These metrics should include, but not be limited to, the following:

- number of ESEs registering for Data Ready Certification;
- number of ESEs who have completed certification;
- number of ESEs who are at each stage of certification;
- number of ESEs who have discontinued the certification process;

[41] As noted above, the initial Data Access Market Input Session will be scheduled at a future date once the Data Ready Certification is operational.

- average time to complete each step of process; and
- average time it takes an ESE to complete the process from registration to certification.

The Data Ready Certification process should be evaluated under these metrics annually and the results filed by the Provider, previous to the Data Access Market Input Session, and should be included in the Provider requirement section of the Data Access Implementation Plan.

Data Access Framework Continuous Improvement

The proposed Framework is designed to be flexible when it comes to the changing needs of markets and customers. The Framework is grounded in a risk-based approach to cybersecurity and privacy which requires continuous review and modification to address new threats or risks, and the necessary protections to mitigate these risks. In the Whitepaper, Staff recommends annually convening a Data Access Market Participant Input Session to allow input and collaboration from ESEs, utilities, and other market participants on the components of the Framework. Data Access Consideration, including data sets not included in Appendix A, were proposed to be addressed through this process. DPS Staff would then make recommendations, if needed, for modifications to the proposed Data Access Framework to the Commission based upon those meetings.

A. Party Comments

The Joint Utilities would like more information on the continuous improvement process relating to specific revisions in access roles and the Matrix. They believe the Matrix must

specify the cybersecurity and privacy requirements that apply to the availability of specific types of data.

RESA notes that technology moves quickly, and it may be necessary to update the Framework regularly, so the stakeholder working group should be a standing working group that can address these changes in a timely manner. RESA believes that in the event of an immediate need for a change to the Framework, the Commission could take short term measures to address items that pose a security concern and cannot wait until the next scheduled Commission session.

As previously summarized above in the ESE Data Ready Certification Process section, RESA and Mission Data request expansion of the available data points included in the data type requested access consideration.

B. Discussion

The Commission finds that instituting a process by which modification to the statewide requirements of the Framework is necessary to ensure that these existing data access requirements are able to be refined to facilitate data access now, and into the future. To that end, once the Data Ready Certification process is operational, Staff will convene an annual Data Access Market Participant Input Session. Future Commission action on the Data Access Implementation Plan will be necessary prior to the Data Ready Certification process becoming operational, thus it would be premature to schedule the initial Data Access Market Participant Input Session in this Order. The timing of the Data Access Market Participant Input Session, as well as the reporting requirement discussed above, will be establish in a subsequent commission order addressing the Data Access Implementation Plan.

Once established, this process should allow stakeholders an opportunity to provide input on the current Framework, including access considerations, and provide Staff an opportunity to review the application of the Framework and closely monitor its' usefulness. To permit the evolution of data access, Staff shall work closely with the utilities to ensure the proper data access requirements are in place. For data access to evolve, Staff will continuously review the appropriate application of existing requirements and will propose developments to the application of the Framework for Commission consideration, as necessary.

RESA and Mission:data requested expansion of the data points currently available in the data sets and while there may be merit in their requests, this Order is not where those requested changes will be addressed. The Framework is adopting the use of data types, and their associated data sets included in Appendix A, to determine that the correct privacy requirements are in place at the time access is considered. To be clear, the Framework is not adopting the specific data points that make up a data set, only the use of the Customer and System data types and their associated data sets. To further explore the possibilities of additional data points being available, the Joint Utilities are required to make a filing within 60 days of the effective date of this Order identifying any available data points that were omitted from the data sets identified in Appendix A. Staff will update the data sets to include additional data points, if any, once the filing is received and reviewed by Staff. As new data points become available, they will automatically be incorporated into the available data sets and included in the adopted data types, providing they fit the description of the data type and sets described. In the event,

a data set, and corresponding data points, become available that do not fit into the currently defined data sets, the Commission would need to take action to adopt the new data set under the applicable data type of the Framework. The listing of the data sets and their associated data points will be included in the Data Access Framework Application Guide discussed below, which will be located on the Department webpage and updated by Staff when any modifications occur. The Joint Utilities should include in their filing a process for notifying Staff of the availability of additional data points related to the Framework's adopted data type access consideration.

The Framework establishes statewide default data access requirements covering the existing data use cases authorized by the Commission. Additions or modifications to statewide data access requirements included in the Framework will require future Commission action. If the Commission establishes or modifies requirements for specific use cases or initiatives, either in the use case's proceeding or this proceeding, the Matrix will be updated accordingly at that time.

Customer Sharing of Energy-Related Data

The Data Access Framework, 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.

A. Consent Process and Customer Choice

While there has been a substantial amount of work put into establishing the UBPs' consent requirements, including the process of obtaining consent, these requirements generally only

govern the interaction between customers and specific ESEs for purposes of enrollment and billing. The consent discussions within the Whitepaper pertain to a customer's ability to consent for additional purposes, other than these general purposes, through alternative means. Currently, there are no guiding documents or policies that establish overall requirements that apply for consent outside of general purpose use.

The terms of the consent agreement are between the customer and the ESE, and 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, the Whitepaper recommends establishing a universal consent mechanism 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. The Whitepaper recommends that the standardized mechanisms, or requirements, for consent should be developed to ensure a common application and process for customers, ESEs, and utilities across New York State. The requirements should apply to both a web-based process along with other consent options for those who do not have electronic means available or who choose to use alternative methods.

The Whitepaper recommends that 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.

The principle of customer control should be considered when evaluating the types of data and various uses of customer data. As proposed in the Whitepaper, customers should be able to condition the use of their data beyond whatever is needed to provide utility service. Customers should also 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.

1. Party Comments

Mission:data notes that the Framework should consider options for customer consent based on the user experience with the consent process. They note that some of the more detailed, practical questions have already been addressed in California and that New York should consider those actions as they develop their own consent process. Additionally, Mission:data comments that a consent process that is reliant upon data that the customer likely does not have or remember, such as utility account number, will not promote increased customer consent. Mission:data references work done elsewhere that provides customers with alternative verification technique to validate a customer consent request, which makes it easier for a customer to provide consent to the sharing of their usage information with a third party.

RESA states that customer consent should be done equitably and fairly. Notably, utilities should not have access

to data that they are not already directed by statute or regulation to obtain. According to RESA, if they are seeking data they are not otherwise directed or allowed to access, then the utility also needs to go through the consent process.

Joint Utilities state that ESEs that seek to obtain data must provide customers with information on the type of data, who will get the data, how data will be used, and length of consent. Logical Buildings states that having an easy process for customers to access their data and consent to others to access their usage data must be paired with robust customer education programs.

2. Discussion

The Commission, in establishing this proceeding, identified increasing customers' familiarity with, and consent to, appropriate data sharing, and movement towards improved access by ESEs to customer energy-related data, consistent with consent, as two of the foundational principles of this proceeding. To deliver on these principles, the utilities, with their ability for ongoing direct communication opportunities with their customers, must play a role in increasing customers' familiarity with data sharing options. To that end, the utilities are directed to file a proposed Customer Consent Engagement Plan that details, at a minimum, communication plans that include draft documents informing customers of available options and benefits, timeline of the plan, and multiple methods of engagement. This plan should be filed in connection with the Consent Process Assessment discussed below.

The Commission agrees that the establishment of standardized consent requirements are necessary to ensure a common application and process for customers, ESEs, and utilities across New York State. The Commission believes a

certified GBC platform provides a reliable protocol for customer authorization that will be a valuable tool for customers to easily consent to, and, share their data by initiating consent at the ESE website. Nevertheless, alternate means of obtaining customer consent may be useful under certain circumstances. The Joint Utilities shall be responsible to ensure that additional consent means do not deter, or provide a disincentive for, customers from using GBC, but rather offer additional ways to help increase customers' familiarity with consent and data access.

The Joint Utilities are required to file a Consent Process Assessment within 90 days of the effective date of this order. This filing shall detail each utility's current consent process(es), including but not limited to: how customers are made aware of the ability to consent to the sharing of their data; what options are available for consent; what information is required for consent; the length of time it takes for the utility to process the consent request, and the annual success rate of authorized consents. The filing shall clearly identify the consistencies and differences among each utilities approach. As discussed above the filing shall also include a Customer Consent Engagement Plan. The filing shall also address an assessment of the standardized consent requirements set forth below. The standardized consent requirements shall include the following:

1. Consent process must be available in two options - web-based and non-web-based. For clarity, the web-based option is outside of the customer's ability to consent via GBC. The non-web-based option must include the ability for a customer to sign a form and return it to the utility or the ESE for processing, such as via mail, fax, or e-mail. A

customer must have the ability to provide their consent by whichever means they have available.

2. Consent language and requirements must be universal, with each utility only customizing for inclusion of their company name. Language and consent requirements, when possible, shall not substantively differ between the web-based and non-web-based process.
3. Consent process shall comply with the applicable UBP requirements regarding customer consent, including, but not limited to, providing the information in a customer's native language.
4. When using GBC, consent process should be compliant and certified to the Green Button Standard.
5. Customer's will be allowed to consent to share their data by the means of an alternative verification technique, such as two-factor authentication, and shall not be required to use their utility account number to consent, with the exception of consent consistent with UBP requirements.
6. Consent form must provide customers with information on type of data being shared, who is receiving data, for what purpose, and length of consent. The length of consent should be consistent with the UBP requirements when consent has been received for providing commodity service. Consent to share data without service will not require an end date but must include annual consent notification to the customer.
7. Consent process must allow customers the ability to easily revoke consent.
8. Require additional consent for any purpose outside what the original consent was obtained for.

9. Consent process must allow customers an option to share with all authorized ESEs, a subset of authorized ESEs, as well as the ESE seeking consent.

This consent related filing, containing the Consent Process Assessment and Customer Consent Engagement Plan, shall be filed with the Commission and issued for public comment prior to Commission action.

B. Customer Opt-Out

The Whitepaper requests further input as to the situations in which customers should be afforded the opportunity to opt-out of having their data used in certain instances. The first instance is for a customer to opt-out of having their data included in a larger aggregated dataset that maintains customer anonymity. The second instance is for use by the utility, or a third party, to develop new products and services. With regards to the second instance, the Whitepaper sought comments and criteria for the viability of conducting an "Opt-Out Pilot" in which customers would be provided the opportunity to decline participation rather than proactively seek it - for the purpose of sharing CEUD to advance clean energy goals. The Whitepaper asks for market participant input on how to develop such a pilot including criteria to use to ensure consumers are provided appropriate notice and opportunity to opt-out.

1. Party Comments

RESA, the City of New York, AEE, and AEA do not support allowing customers to opt-out of aggregated or anonymized data sets. As AEE notes, once customer data is sufficiently aggregated and anonymized data then it no longer becomes customer data and is no longer subject to the same types of risks associated with customer identifiable data. If the

aggregated data samples contain several customers within that aggregation that have opted-out, then that data set becomes less useful. Mission:data believes that customers should not be able to opt-out of aggregations so long as aggregations sufficiently prevent re-identification of any individual and are conducted solely for the purpose of providing a regulated service such as electricity delivery or an energy efficiency or demand management program overseen by the Commission. If these conditions are met, then Mission:data believes opting out is unnecessary and would diminish the public benefits stemming from aggregated energy analysis.

The City of New York believes the Commission should avoid opt-out programs for non-aggregated/anonymized customer data. They agree with statements in the Whitepaper that mechanisms to facilitate customers' ability to easily consent to share their data and educate and engage customers to encourage customer consent to data sharing must be created beforehand. If opt-outs must be used for an energy offering or program, then the customer's opportunities to opt-out should be frequent and prominent.

Mission:data believes an "opt-out pilot" is neither necessary nor valuable. If the Commission wants customers to enroll in DER services provided by a utility or as part of a Commission-authorized program, then Mission:data believes it would be more appropriate to discuss those topics in proceedings devoted to efficiency or demand management utility programs.

Logical Buildings believe customers who do not want to receive information should be allowed to opt-out. The Joint Utilities support allowing customers to opt-out of their identifiable data being shared and further do not support developing an opt-out pilot.

2. Discussion

The purpose of aggregating and anonymizing customer energy use data is so that no one individual customer can be identified through their usage. Aggregated and anonymized usage data has been, and continues to be, an important tool in understanding overall usage patterns that facilitate energy planning. The usefulness of this information is diminished if it is not a complete record of all relevant customers. Given the safeguards that are in place for the protection of customer privacy, the Commission agrees that customers should not be allowed to opt-out of aggregations if the customer's energy-related data is sufficiently aggregated and anonymized.

The Commission agrees with the City of New York that this Framework will initially focus on facilitating customers' ability to easily share their data and educate and engage customers to encourage customer consent. Once the standardized consent requirements are developed and in use, Staff shall closely monitor the performance metrics tied to customers authorizing to share their data.

Opt-out strategies have been successfully utilized in a number of other industries and policy arenas. At this time, no parties have advocated for implementing an opt-out pilot, and the Commission declines to implement such a program here. However, the Commission is not foreclosing the option to explore this type of approach in the future.

Data Access Framework Application Guide

The Whitepaper proposes the creation of a Data Access Framework Application Guide that outlines the necessary steps to obtain access to energy-related data in a uniform and consistent manner.

A. Party Comments

Joint Utilities raise questions regarding the development of Data Access Framework Guide, notably who will write it.

B. Discussion

To facilitate the transition to the Data Access Framework and Data Ready Certification process, the Commission directs Staff to create a Data Access Guide that clearly explains the components of the Framework and details the Data Ready Certification process that will be developed with the Provider. Though guidelines for the program and certification programs are included below, the specifics will not be available until the Data Access Implementation Plan has been approved and the program developed with the selected Provider. Staff is directed to file a completed Data Access Guide after the details of the program have been approved but before the program is operational. Development of the Data Access Guide shall occur after Commission decision of the Joint Utility Data Access Implementation Plan described above. The guide should also be made available on the Department's website, utility websites, and the Data Ready Certification website.

Alternative Account Identification

In the Whitepaper, Staff recommends that the Joint Utilities be required to file 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.

A. Party Comments

No comments were received on this issue.

B. Discussion

Account numbers have long been used to not only correlate data to a specific account for utility side operations but for ESE customer transactions with the utility and as a means by which the customer identifies their account for interactions with both the utility and any chosen ESE. The UBPs require an ESE to obtain, and provide, a customer account number as verification for enrollment. However, the use of an account number as primary identifier of a customer and their data is a practice that is quickly evolving and changing, primarily in recognition of the privacy concerns associated with the release of customer account numbers. While an account number does not provide access to an individual customers personal information, in some instances, it may be used to initiate transactions on a customer account with the utility or an ESE, such as enrollment with an ESCO. Recent Commission initiatives have begun moving away from the use of the account number for specific uses, such as with PIEDR and in CCA programs. When customer data is being shared with an ESE via PIEDR or with a CCA program, the account number is not included, instead a proxy ID# has been used in place of the account number or the customer's identifiable information shared with an ESE after consent, omitting account numbers all together. The proxy ID# is established on the utility side and, for CCA, this proxy ID# is maintained for the life of the account. This change in how an account number is viewed has also led to modification in customer side requirements in CCA. A customer is no longer required to provide an account number for opt-in or opt-out purposes, using only their name and address to facilitate the transaction. While CCA is outside the normal operating procedures due to the CCA having a master listing of eligible residents to match with the customer name and address, the purpose of moving away from

the use of account numbers has validity. As such, the Commission directs the Joint Utilities to file a proposal, within 90 days of the effective date of this Order, for an alternative method of account identification for completing ESE customer transactions that have previously relied on the customer account number. This proposal should also consider the ability to implement a solution both at an individual utility level as well as a statewide level that may be necessary once a statewide data platform is available.

CONCLUSION

The Data Access Framework adopted in this Order will serve as a single source for data access policies and provide uniform and consistent guidance on what is needed for access to, and the availability of, energy-related data. Moreover, the Framework will promote data access, while preserving all the necessary protections, to facilitate New York State's policy goals.

The Commission Orders:

1. The Data Access Framework proposed in the Department of Public Service Staff Whitepaper Regarding a Data Access Framework is adopted, consistent with the discussion in the body of this Order.

2. Central Hudson Gas & Electric Corporation, Consolidated Edison Company of New York, Inc., National Fuel Gas Distribution Corporation, New York State Electric & Gas Corporation, KeySpan Gas East Corporation d/b/a National Grid, the Brooklyn Union Gas Company d/b/a National Grid NY, Niagara Mohawk Power Corporation d/b/a National Grid, Orange and Rockland Utilities, Inc., and Rochester Gas and Electric

Corporation (collectively, "Joint Utilities") are directed to file, within 60 days of the effective date of this Order, the Data Access Implementation Plan for Commission approval, consistent with the discussion in the body of this Order and Appendix B.

3. The Joint Utilities shall, within 60 days of the effective date of this Order, make a filing identifying any available data points that were omitted from the data sets identified in Appendix A to this Order.

4. The Joint Utilities shall, within 90 days of the effective date of this Order, to file a proposal for an alternative method of account identification for completing Energy Services Entity customer transactions that have previously relied on the customer account number.

5. The Joint Utilities shall, within 90 days of the effective date of this Order, file a Consent Process Assessment consistent with the discussion in the body of this Order. This filing shall also include a Customer Consent Engagement Plan consistent with the discussion in the body of this Order.

6. The individual utilities listed in Ordering Clause No. 2 shall, within 90 days of the effective date of this Order, file a complete listing of its current data access use cases and applications, including the current status of the data quality and integrity standards discussed in the body of this Order. This filing shall also include any data access use cases and applications still in development, and the anticipated completion date of such development.

7. The individual utilities identified in Ordering Clause No. 2 shall, within 60 days of effective date of this Order, file a Green Button Connect User Agreement that includes

the data quality and integrity standards consistent with the discussion in the body of this Order.

8. Department of Public Service Staff (Staff) is directed to, within 90 days of the effective date of this Order, develop a registration process for ESEs interested in accessing data that, currently, are not required to register with the Department of Public Service (Department).

9. Staff is directed to, within 30 days of the effective date of this Order, file the Matrix that shows how each existing cybersecurity and privacy requirement have been mapped to each access consideration.

10. Prior to the initial Data Access Market Input Session that will be scheduled at a future date, Staff is directed to file (1) an outline of a single report combining existing data related reporting requirements, and (2) a survey to be provided to Energy Service Entities regarding the Data Ready Certification process.

11. All New York distribution utilities that publish Hosting Capacity Maps shall, within 30 days of the effective date of this Order, remove the user registration requirement for their Hosting Capacity Maps.

12. All New York distribution utilities shall, within 60 days of the effective date of this Order modify their current tariffs to remove all established fees associated with the release of customer data, except those cost based fees associated with requests for historical energy usage data in excess of 24 months, consistent with the discussion in the body of this Order. The tariff revisions shall be filed, on not less than one day’s notice, to become effective on or before June 13, 2021.

13. The requirements of Public Service Law Section 66(12)(b) as to newspaper publication of the tariff revisions filed in accordance with Ordering Clause No. 12 are waived because the process in this proceeding and this Order give adequate notice of the changes.

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

15. This proceeding is continued.

By the Commission,

(SIGNED) MICHELLE L. PHILLIPS
Secretary

APPENDIX A: 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.

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 under a 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 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. Each data set includes the data points available to be shared as part of that data set. These data points will be updated/expanded as new data points become available or as Commission directives, Federal, State, or Local Law require.

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. The CEUD data set includes historical data, real time data, and other types of AMI data, as defined below.

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.

Real Time Data

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

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.

Cybersecurity Protections

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

Data Access Agreement

By the condition of seeking access to energy-related data, the Data Ready Certification Provider will require ESEs to agree to abide by the terms of a Data Access Agreement, that includes the requirements established in the Data Access Framework.

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 from the data custodian, for the purposes defined under the access requirements. This does not include entities, such as utility contractors, who are performing a service for the utilities.

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.

Privacy Protections

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

System Data

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

User Agreement

An agreement between a utility or data custodian and an ESE that establishes the responsibility between parties, including, among other things, the applicable data quality and integrity standards applicable to that use case or application.

APPENDIX B: PROVIDER DETAILS FOR DATA ACCESS IMPLEMENTATION PLAN

1) Details of the proposed process and timeline for selecting a Provider that will enable the Data Ready Certification program to be operational within one year of the filing date of the Data Access Implementation Plan;
2) Details, including timelines, of the services to be provided by the Provider including:
   a) all the steps of the certification process, including how the Provider will be verifying that DPS registration requirements have been met and how the Provider will verify cybersecurity and privacy requirements have been met and what 3rd party audit options, such as those discussed previously, will be available;
   b) timeframe associated with the ESE request, verification, and certification;
   c) the creation of a user-friendly dashboard on a centralized, independent Data Ready Certification webpage that includes the listing of certified ESEs, allows an ESE to submit a request for Data Ready Certification, check-on status, and upload any necessary documents;
   d) how the Provider will provide its contact information for assistance with the certification process;
   e) mechanism that allows the ESE to agree to the Data Access Agreement;
   f) a process for suspension or revocation of the certification;
   g) how the listing of certified ESEs will be kept up to date, showing date of certification, and how re-certification will be facilitated;
   h) the creation of the Data Access Agreement, as detailed in Appendix B;

i) requirement for reporting of ESE certification metrics, as further detailed below; and
j) a process for the utilities to electronically agree to a single ESE Data Access Agreement.

3) Proposed terms that will be included in the agreement between the Joint Utilities and the Provider;
4) Cost breakdown of how much each utility would be saving by no longer having to use its resources for the verification of each ESE cybersecurity and privacy requirements and how that current funding will be allocated to the ESE risk management and certification program implementation and operation;
5) Proposed cost recovery mechanism(s), including cost sharing among the Joint Utilities for any incremental costs net of savings opportunities identified;
6) A roll-out plan, including timeframes, for how each ESE currently receiving data from one or more of the distribution utilities will be notified of its need to complete the Data Ready Certification; and,
7) Utility plans for how each will be incorporating the adopted Data Ready Certification process into the existing utility data access request processes.

APPENDIX C: ESE CERTIFICATION PROCESS

The ESE certification process will be as follows:

1) The ESE registers on the Data Ready Certification webpage to request certification and includes what access roles (based upon the access considerations) it is seeking certification for.
2) The Provider verifies the applicant is an authorized ESE that has completed any necessary DPS requirements by confirming eligibility on the Department's website.
3) Once verified, the Provider approves the application and the ESE is provided with an electronic Data Access Agreement that details the terms of the agreement and includes the necessary cybersecurity and privacy requirements that will be required for certification.
4) Upon readiness, the ESE will provide electronic consent to the Data Access Agreement and its consent to have the requirements verified by the Provider or submit an independent recognized security controls audit report, such as the SOC-II Type 2 Audit Report, that has been performed in the last 30 days for review.
5) When received, the Provider will schedule testing/confirmation of the necessary cybersecurity and/or privacy protections being in place to meet the requirements of the Data Access Agreement. If any of the requirements are unable to be verified, the Provider will notify the ESE where they are deficient, and the ESE will not receive certification. The ESE application will remain active for X days, allowing ESE time to address the deficiencies. If deficiencies are not addressed during that time the ESE will need to begin the process anew.

6) After the Provider has verified the ESE has the necessary requirements in place it will issue an approval to the ESE and update the public listing on the Data Ready Certification webpage showing the ESE as certified and include: the date first certified, what access roles they are certified for, and when they are due for the next certification.

Once the ESE is certified they will remain so until such time that the requirements change or are modified by Commission action. At such time, the Provider will send a re-certification notice to all currently certified ESE's which details the change in requirement and provides the timeframe in which the ESE must complete recertification. If an ESE does not recertify prior to the compliance date, the Provider must change the ESE certification status to suspended and update the Data Ready Certification webpage listing. An ESE that does not have current certification will not be allowed to obtain access to data. The ESE will have X days from suspension to re-certify before they will have to begin the process anew.

When a certified ESE seeks access to data from any data custodian, the data custodian will verify from the Data Ready Certification webpage that the requesting ESE has the necessary cybersecurity and privacy requirements in place for that request.

APPENDIX D: EXISTING DATA ACCESS REQUIREMENTS

The Framework incorporates existing access requirements from:

1. Case 98-M-1343: Energy Service Company Uniform Business Practices
2. Case 15-M-0180: Distributed Energy Resource Supplier Uniform Business Practices
3. Case 14-M-0224: Community Choice Aggregation
4. Case 18-M-0376: Cybersecurity Protections and Protocols
5. Case 17-M-0315: Utility Energy Registry
6. Case 18-M-0084: Comprehensive Energy Efficiency Initiative
7. Case 16-M-0411: Distributed System Implementation Plans
8. Case 14-M-0094: NYSERDA Data Order
9. Case 14-M-0101: Reforming the Energy Vision

APPENDIX E: STAKEHOLDER COMMENT SUMMARY

Entities that Commented on Motion of the Commission Regarding Strategic Use of Energy Related Data

1. Advanced Energy Economy, Alliance for Clean Energy New York, and Advanced Energy Management Alliance (AEE)
2. Association for Energy Affordability, Inc. (AEA)
3. The City of New York (City)
4. The U.S. Environmental Protection Agency (EPA)
5. Flux Tailor LLC (Flux Tailor)
6. Central Hudson Gas & Electric Corporation, Consolidated Edison Company of New York, Inc.(Con Edison), National Fuel Gas Distribution Corporation, New York State Electric & Gas Corporation, KeySpan Gas East Corporation d/b/a National Grid, The Brooklyn Union Gas Company d/b/a National Grid NY, Niagara Mohawk Power Corporation d/b/a National Grid, Orange and Rockland Utilities, Inc.(O&R), and Rochester Gas and Electric Corporation(Joint Utilities)
7. Energy Technology Savings, Inc. DBA Logical Buildings (Logical Buildings)
8. Mission:data Coalition (Mission:data)
9. The New York Power Authority (NYPA)
10. Recurve Analytics, Inc. (Recurve)
11. The Retail Energy Supply Association (RESA)

Initial and Reply Comment Summary

Proposed Data Access Framework

Logical Buildings appreciates and agrees with many of the proposals in the DAF Whitepaper while stressing the importance of: a simplified third party authorization process, a streamlined process for companies' access to customer data, a single point of access to data for customers and third parties, and timely access to data presented in useful intervals.

RESA supports the creation of a Data Access Framework that will allow easier access to energy-related data and recommends the development of an experienced working group and selection

process that remains active for the duration of the DAF's existence.

Applicability

AEE believes that "Energy Service Entities (ESEs)" in the Framework are defined broadly and recommends that the commission modify the definition of ESE so that it excludes utility contractors. Utility contractors that perform functions on behalf of utilities and not in direct pursuit of their own business interests are fundamentally different from third parties who lack the same strong data security requirements. AEE thinks that these requirements are likely higher than what is required in the Framework and cites a 2010 case that was reaffirmed in 2018 where the Commission believed contractual safeguards between two utilities and a behavioral efficiency provider were strong enough to allow the contracts to govern the cybersecurity and privacy requirements with the contractor. They also refer to examples in the UBP where the Commission exempted some transactions between DER suppliers and utilities that were already governed by program rules and utility contracts.

NYPA supports consolidation of existing data requirements and ESE verification through the Data Ready Certification Program, however they implore the commission to recognize that certain ESEs, (including state entities such as NYPA), transfer data under unique circumstances that would not fit neatly into the DAF. These include data transfers that account for delivery of NYPA power to NYPA customers, load profiles, and capacity tags provided by the utility, all of which render NYPA unable to comply with generic statewide DSAs. NYPA and other state entities have collaborated with the Joint Utilities to develop custom DSAs for these scenarios.

RESA supports fair and equal applicability of the framework to all entities seeking access. The commission should not allow the structure of the final framework to contain preferences that favor or harm any single market participant sector.

Enforcement

The Joint Utilities recommend that Staff strengthen enforcement mechanisms described in this section.

RESA believes that UBPs' enforcement mechanisms would not be appropriately tailored to instances of Framework noncompliance by all entities expected to access data through the Framework. Additionally, entities of different types that receive the same access to the same information should be subject to the same consequences for identical instances of noncompliance in their handling of the information.

ESE Data Ready Certification Process

AEA believes that utility contractors should not have to duplicate efforts already required by their utility contracts in order to access data.

AEE supports the Data Ready Certification process proposed in the Whitepaper believing it will provide quicker access to data and mitigate duplicative efforts between utilities. They would like to know more about the confirmation of privacy and cybersecurity requirements and the process taken by a risk management solution provider. They suggest an audit focusing on documentation of data handling, storage, and other cybersecurity practices before further steps are considered. This would include a streamlined verification process for several recertification cycles as well as additional thought given to an incremental requirement certification for ESEs.

The City of New York submits that building owners should not be required to become an ESE and go through the framework certification process to obtain aggregated whole building data, as there is a low degree of risk, both from a transmittal and/or access perspective to receiving such data. They also believe aggregated and anonymized customer data should be excluded from the framework certification process.

The EPA believes special consideration should be given to building owners/operators as they do not fall neatly into the category of customer or ESE. Building owners/operators will be the customers of record for any energy consumption data under a landlord-paid account and third parties with relation to any energy consumption data under tenant-billed accounts. It may not be entirely appropriate to label building owners/operators as ESEs, nor to require the same level of authorization or certification for data access that would be required a competitive energy supplier, making them a special case. The EPA acknowledges this topic has been addressed in section 4.4.2.1. Going forward, the EPA would like to see plans for specific scenarios regarding requests from building owners/operators when tenant numbers exceed or fall below certain thresholds, when prior tenant-level authorization does not exist, and when tenant-level authorization exists in the forms of lease language, a utility-level release form, or some other recognized format.

The Joint Utilities recommend further stakeholder discussions regarding the relations between cybersecurity and transmittal or access mechanisms only and privacy requirements only to type of data. Cybersecurity and privacy requirements cannot be separated so simply.

Logical Buildings agrees that consideration should be given to the type of system access required to provide customer data, the type of data requested, and whether customer authorization to obtain data has been given. Data linked to a specific customer should not be provided unless the customer has consented, but non-identifiable data (aggregated / anonymized) should be provided without customer consent. Logical Buildings understands that ESEs with direct connections to the utility system should have a higher level of cybersecurity protections than those with indirect connections, with the determining factor in level of security being the type of data being provided.

NYPA believes they should only have to validate that they have in place the cybersecurity and privacy protections already

required under their Legacy Agreements. This would allow them to fulfill without interruption their core statutory obligations as both a generator of electricity and a Load Serving Entity, as well as not develop new cybersecurity and privacy requirements for ESEs. Not permitting the NYPA DSA to be used in the Data Access Framework would be contrary to the Commission's recognition that State entities must access energy-related data but also must be granted flexibility regarding compliance with the DSA requirements.

Recurve would like to see more information about the expected timing of the certification process. Delayed certification could create significant costs for market actors and additional procedural burdens for the entity responsible for the certification process. The Commission should consider grandfathering in vendors with previously established Data Security Agreements in place. They encourage DPS to keep the potential costs to vendors seeking certification in check by establishing clear rules and focusing on specifying use-case guidelines, while still maintaining industry standards for data privacy and security.

RESA has concerns over the risk management solution provider. The request that parameters for the selection of the Provider should be proposed for consideration and that the Commission should establish certain threshold requirements that candidates for the Provider role are required to meet. Additionally, they would like clarification the auditing process regarding who the auditor would be, their scope, and their review process.

Access Considerations: Purpose, Data Type Requested, and Transmittal or Access Mechanism

AEA supports the development of a risk-based matrix for data access but believe there should be opportunity for further stakeholder input given the details matter and the white paper did not provide matrix details.

Mission Data wants to know more about the types of data to be provided to customer-authorized third parties. They believe the data types outlined in the UBP-DERS are inadequate to animate DER markets, and propose additional data types including: Historical and ongoing energy usage, historical and ongoing line items on bills, the rate each customer is on, and any information necessary to determine eligibility for, or participate in, a demand response, energy efficiency or renewable energy program.

RESA supports a risk-based approach to data access, transmittal, and storage that is applied to all similarly situated entities in the same manner. RESA believes that demonstrating "a valid purpose" for accessing Customer Contact Information Data Set information should not be required when customers have explicitly authorized ESEs to have access to that information. They also believe that Customer Billing Data Set information should include bills themselves as this information will help ESEs respond to customers who have questions about the ESE components on utility consolidated bills and about how ESE products affect their bills. RESA believes the Commission should consider a period of at least twenty-four months of historical data in the CEUD set so that ESEs can see changes in annual usage patterns. All ESEs and other market participants should have access to AMI meter data on the same basis.

Determination of Risk-Based Cybersecurity and Privacy Requirements

AEA believes that data access requirements should be based on potential risk rather than a one-size fits all; the matrix proposal makes sense but, before adoption, the stakeholders/market participants should review and comment further on the details.

AEE believes that utilities are currently not motivated to provide data as they are liable for third-party data breaches and do not financially benefit from data sharing. The Commission has not addressed liability of the utilities in the event of a data breach, leaving the utilities to be overly cautious. AEE

recommends a two-part indemnification where the Commission states that utilities bear no liability for third-party negligence or wrongdoing and provides financial indemnification through cost recovery of any legal fees and settlements. AEE also believes that an Earnings Adjusted Mechanism is a better choice for providing an earnings opportunity for data access rather than a fee per transaction with margin. Routine data request payments could prohibit third parties from participating while incremental costs of a data transfer would be negligible through the process of AMI deployment.

AEE would like to know more about the content of the matrix. They believe that current data policies have a one-size-fits-all approach and strongly support the adhering of a risk-based approach that the Framework Whitepaper describes. They also point out that the risk of a breach of personal information varies based on the number of customers served by an ESE. As the development of the matrix will be detailed work with significant ramifications for market participants, AEE recommends that Staff develop the matrix in consultation with a stakeholder group and submit it for comments.

The Joint Utilities would like staff to elaborate on the inadequate address of the actual risk associated with various types of data access or the customer's choice regarding data sharing. They also suggest stakeholders be involved in the determination of underlying data required to complete the cybersecurity and privacy matrix. Liability and insurance within ESE risk management is not adequately described, and the JUs request more clarity concerning how ESEs will update certification. Additionally, they would like to know who would write The Data Access Framework Application Guide, and how would penalties be imposed for infractions?

Logical Buildings supports a risk-based approach as it ensures customer data is only shared with appropriate parties and allows utilities to transmit data to ESEs through their own systems. Logical Buildings has spent considerable time and effort in the past to work their way through the onboarding process with the

utility in order to obtain access to customer data via Green Button Connect. They believe that the new certification process should consider previous risk information provided by ESEs, previous Data Security Agreements, and previous system testing, but also believe it is fair for supplemental items to be required if they are not confirmed by the preceding information.

Mission Data is concerned that the Framework does not address the fundamental incentives and disincentives relating to a utility sharing customer energy data with third party DERs. Utilities currently believe that they have a significant disadvantage when sharing customer data as they have broad liabilities for a third party's behavior. Mission Data also points to the lack of an earnings adjustment mechanism as one of the reasons for GBC's shortcomings. They recommend an EAM that rewards utilities for greater customer utilization of their GBC platforms.

Recurve supports the concept of a risk-based approach and encourages DPS to adopt a use-case specific framework that can leverage the best practices in cybersecurity and privacy protection in the matrix. They also support the use of differential privacy to add noise and aggregate statistics. This makes determining the contribution of any individual to the overall result more difficult, and is quickly becoming an industry practice, significantly enhancing the options considered within the DPS "matrix". Attached to their comments, they have included a research paper titled "Differential Privacy for Expanding Access to Building Energy Data". Recurve would like to see more information regarding liability of data transfers.

Utility Connection Requirements

RESA supports proposed testing of direct utility connections by ESEs.

Data Access Fees

The Joint Utilities support no-fee registration because it allows for relevant communication of operational information between utilities and users, transparency into the numbers of users, and gives the utility a means of shutting off bad actors.

Logical Buildings agrees that no fees should be associated with a customer or a third-party obtaining access to customer utility data as data is necessary for development of new energy products, and access fees would discourage this. Additionally, access fees would drive up costs for customers complying with existing energy usage reporting regulations.

RESA strongly supports abolishing data access fees.

AEE recommends that fees for data should only be applied to special data requests that may impose unique costs on the utility, and in those cases, the price should be cost-based.

Data Quality and Integrity

AEA believes existing data access protocols, such as those used in NYC to satisfy local laws relating to building energy use, should continue and not become more costly or burdensome under any newly adopted frameworks.

AEE believes increasing standardization will decrease repetitive costs of utilities' individual data interface systems. Developing these standards will require detailed coordination between the utilities, their software vendors, and potential users of the datasets, so the most immediate and widespread use cases should be developed first.

Logical Building supports Staff's comments in Section 3 Page 20 of consistent data quality and integrity standards so that ESEs can rely on the data provided to them without needing to check accuracy.

Mission Data is concerned that the DAF Whitepaper makes third parties responsible for data quality, when in fact utilities are solely responsible. Since the utilities have a monopoly on electric delivery services, "data quality" is not a problem of customer-authorized third parties that the Commission needs to solve, and its inclusion in the Framework is misplaced. Mission Data has proposed Service level agreements that guarantee uptime of the platform and responsiveness to IT defects, reporting metrics for accountability, requirements of data accuracy labels, compliance with best practices and the GBC standard, and versioning and sunsetting requirements to ensure smooth transitions during system upgrades. In addition, they propose the following metrics be required:

1. The number of completed data-sharing authorizations
2. Time elapsed for a random sample of customers to complete a data-sharing authorization with a third party
3. The percentage of data-sharing attempts that are successful (searchable timeframe)
4. Average and maximum data delivery time (seconds) following customer authorization (searchable timeframe)
5. GBC system availability (uptime)
6. Number and type of errors generated, if any
7. Number and type of issues raised by third parties and customers, including severity, mean and max acknowledgment time, and mean and max resolution time
8. Number of complaints received from third parties, including type and severity
9. Number of customers with one-time and ongoing data-sharing authorizations
10. Time to complete third party technical and administrative onboarding

RESA supports making data available to all stakeholders in a standardized manner.

Reporting

RESA supports streamlining reporting by incorporating disparate reporting requirements into a single report.

Data Access Framework Continuous Improvement

The Joint Utilities would like more information on the Continuous Improvement process relating to specific revisions in access roles and the security risk matrix. They believe the matrix must specify the cybersecurity and privacy requirements that apply to the availability of specific types of data.

RESA believes that in the event of an immediate need for a change to the Framework, the Commission could take short term measures to address items that pose a security concern and cannot wait until the annual session.

Customer Sharing of Energy-Related Data

Mission Data stresses that customer consent is not binary, and believes the definition is not fully expanded upon. They point to California's "Customer Data Access Committee" as a reference for industry best practices and believe the Commission should make it easy for customers to share energy data.
RESA supports requiring customer consent to access data that identifies particular customers, however customers should not be permitted to opt-out of having their information included in Aggregated Data.

Additional Questions

1) Regarding efforts to ensure data quality and integrity, 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?

The City of New York suggests that the Commission conform the terms, definitions, and data field formats in the framework to the U.S. Department of Energy's Building Energy Data Exchange Specification ("BEDES") wherever possible.

EPA stresses the importance of two specific considerations. First that aggregate whole-building consumption data for entry into Portfolio Manager be accompanied by descriptive information regarding the constituent meters that have been "rolled up" in

the calculation of the aggregated whole-building consumption total. This information would enable the data requestor to ensure that the aggregate consumption values received from the IEDR accurately reflect all energy consumption being tracked for a given property. Second, that the consumption value delivered from the IEDR to the requestor represents the "gross" amount of electricity received by the building from the grid, and not just "net-metered" consumption so that building owners/operators can differentiate between consumption of electricity that was received from the grid, and the consumption of electricity that was generated onsite and consumed onsite.

2) In evaluating the success of the proposed Data Access Framework, what reporting requirements should be established, including frequency of any required reporting, as well as any specific metrics that should be captured to evaluate success?

The City of New York recommends that entities seeking ESE Certification should document and submit to the Commission a report that explains the time and effort they spent to achieve ESE Certification to allow the Commission to set a benchmark for the process.

3) Under what situations should customers 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?

AEE recommends the Commission not allow opt-outs for aggregated data as there are not privacy concerns when data is aggregated to a certain level. They also do not believe there are privacy concerns with sharing anonymized individual customer usage data, however, there are likely to be fewer negative data integrity and planning consequences if customers are allowed to opt-out of sharing anonymized individual customer usage data.

The City of New York does not support a data access paradigm wherein customers are permitted to optout of having their data used for larger aggregated datasets that keep the customer's identity anonymized. This would create a significant barrier to achieving important energy reduction and decarbonization goals.

Mission data believes that customers should not be able to opt-out of aggregations so long as aggregations (1) sufficiently prevent re-identification of any individual and (2) are conducted solely for the purpose of providing a regulated service such as electricity delivery or an energy efficiency or demand management program overseen by the Commission.

Logical Buildings believes that an opt-out process would be the most efficient way to accomplish the goal of having customers easily share their usage data with third party providers.

4) Regarding the development of an opt-out pilot program, how should such a pilot be structured and what criteria should be included to ensure consumers are provided appropriate notice and opportunity or opt-out.

AEA believes anonymized and aggregated energy use data is critically important to achievement of New York's climate goals and we, therefore, are concerned about the proposed opt-out proposal for consumers for those data sets (but, of course, strongly support the privacy of individual account information).

The City of New York believes the Commission should avoid opt-out programs for non-aggregated/anonymized customer data. They agree with statements in the Data Access Framework Whitepaper that mechanisms to facilitate customers' ability to easily consent to share their data and educate and engage customers as a means to encourage customer consent to data sharing must be created beforehand. If opt-outs must be used for an energy offering or program, then the customer's opportunities to opt-out should be frequent and prominent.

Mission data believes an "opt-out pilot" is neither necessary nor valuable.

DATA ACCESS FRAMEWORK

Single source for statewide data access requirements. Provides uniform and consistent guidance on what is needed for access to energy-related data.

(6) AREAS OF DAF ADOPTION

1) Applicability
2) Enforcement
3) ESE Data Ready Certification Process
4) Data Responsibilities and Relationships
5) Data Access Continuous Improvement
6) Customer Sharing of Energy-related Data

APPLICABILITY

DAF applies to any entity seeking access to energy-related data from the data custodian*.

*Any entity where the energy-related data are housed and being accessed (utility or centralized data warehouse)

ENFORCEMENT

DAF enforcement only pertains to ESE's ability to access data. Data Ready Certification Program validates ESE is registered and approved by Department. If ESE does not have necessary protections in place, they will not be certified. ESE Risk Management Program will incorporate policies to revoke or suspend certification, as well as a dispute resolution process.

ESE DATA READY CERTIFICATION

Details on page 2

DATA RESPONSIBILITIES AND RELATIONSHIPS

Details on page 3

CONTINUOUS IMPROVEMENT

Details on page 4

CUSTOMER SHARING OF ENERGY-RELATED DATA

Details on page 5

Areas of DAF Adoption
JU Filing/ Action
Staff Filing/ Action
Agreement Between Parties
Data Ready Certification

DATA ACCESS FRAMEWORK

ESE DATA READY CERTIFICATION PROCESS

Energy Service Entity (ESE) Data Ready Certification Process will be managed by a Provider. Provider's role is to certify that an ESE has the necessary cybersecurity and privacy protections in place for the access they are requesting certification.

DATA ACCESS GUIDE

Staff creates a Data Access Guide that clearly explains the components of the Framework and details the Data Ready Certification process that will be developed by the Provider. The guide will be available on the Department's website, utility websites, and the Data Ready Certification website.

AUTHORIZED ESE VERIFICATION

Provider verifies an ESE is authorized by the Department to request and access data.

ESE REGISTRATION PROCESS

Within 90 days of Order, Staff develops a registration process for ESEs who are not currently registered with the Department.

Process will be centralized and include a listing of all registered ESEs, including the current UBP eligible ESCO and DER suppliers. Provider will use this list to verify an ESE authorization.

ACCESS CONSIDERATIONS

ESE Details whether consent was obtained and:

1) Purpose for accessing unconsented data
2) Mechanism by which data are being accessed or transmitted:
   a. Direct connection to data custodian's IT system
   b. Secure platform/portal
   c. Public platform/portal
   d. Email or other non-electronic connection.
3) Data type for which access is being requested:
   a. Customer data
   b. System data

STATEWIDE AGGREGATED DATA PRIVACY SCREEN

DAF adopts statewide aggregated data privacy screen of 4/50. Directs all aggregated data that passes privacy screens to be made available upon request.

HOSTING CAPACITY MAPS

System Data - directs utilities to remove user registration requirement from Hosting Capacity Maps within 30 days of Order.

VERIFICATION OF REQUIREMENTS AND CERTIFICATION

After the ESE provides their access considerations, Provider uses the Matrix to advise the ESE what cybersecurity and privacy requirements apply.

MATRIX

Within 30 days of Order, Staff is directed to file the Matrix that shows how each existing cybersecurity and privacy requirement has been mapped to an access consideration. Filing allows Stakeholders the opportunity to provide feedback. Staff will then review the stakeholder comments and file an updated version.

DATA ACCESS AGREEMENT

ESE will be provided with an electronic Data Access Agreement that details the terms of the agreement and includes the necessary cybersecurity and privacy requirements that will be required for certification. This agreement will be generated by the Provider and provided to the ESE and appropriate data custodian for execution.

DATA ACCESS IMPLEMENTATION PLAN

JU to file within 60 days of Order. Implementation Plan to include, but not limited to - details of the Data Ready Certification process to be developed with the Provider that includes all the steps of the certification process.

See Appendix B of Order for more Data Access Implementation Plan details.

DATA READY CERTIFICATION

ESEs will become certified once they have completed the necessary requirements for approval and have an executed Data Access Agreement. Certification dictates what type of data ESE can request, and how they can access it. Certificate would apply across utilities or data custodians.

Areas of DAF Adoption
JU Filing/ Action
Staff Filing/ Action
Agreement Between Parties
Data Ready Certification

DATA ACCESS FRAMEWORK

DATA RESPONSIBILITIES AND RELATIONSHIPS

Establishes the responsibilities of the utilities to the ESEs seeking access to data in a way that promotes meaningful data quality standards.

DATA ACCESS FEES

Utility system capabilities are now able to automate data processing, eliminating the basis for utilities being permitted to charge fees for energy-related data > 24 months old.

UTILITY TARIFFS

Within 60 days of Order, utilities to modify their current tariffs to remove all established fees associated with the release of customer data, including CCA data, and system data.

DATA QUALITY AND INTEGRITY STANDARDS

Standards will ensure that the data is accurate and transferred in a timely manner, that technical support is available, and that the data format is in conformance with applicable standards. DAF established categories for data quality and integrity standards. Specific details of data quality and integrity standards will depend on the individual use case or application. Performance metrics will be used to determine if these standards are being met.

LISTINGS OF DATA ACCESS USE CASES AND APPLICATIONS

Within 90 days of Order, utilities to file a complete listing of their current data access use cases and applications and include current status of DAF data quality and integrity standard categories.

REPORTING

Staff is directed to identify the required data-related reporting requirements, including Data Ready Certification requirements, and file an outline for a single report prior to initial Data Access Market Input Session.

DATA USER AGREEMENT

Agreement between data custodian and ESE that includes, among other things, applicable data quality and integrity standard applicable to use case or application. Data User Agreements will be the means in which the data custodian will confirm to an ESE that the data being transferred meets applicable standards.

GBC USER AGREEMENT

Within 60 days of Order, utilities to file a GBC User Agreement including Data Quality and Integrity standards for Commission consideration. Each utility will also file their GBC third party onboarding process.

- *Areas of DAF Adoption*
- *JU Filing/ Action*
- *Staff Filing/ Action*
- *Agreement Between Parties*
- *Data Ready Certification*

DATA ACCESS FRAMEWORK

Single source for statewide data access requirements. Provides uniform and consistent guidance on what is needed for access to energy-related data.

DAF CONTINUOUS IMPROVEMENT

DAF is designed to be flexible when it comes to the changing needs of markets and customers. For data access to evolve, Staff will continuously review the appropriate application of existing requirements and will propose developments to the application of DAF for Commission consideration, as necessary.

DAF is adopting the use of customer and system data, and their associated data sets included in Appendix A, to determine if the correct privacy requirements are in place at the time access is considered. Data points that make up a data set will be continuously incorporated into the available data sets.

DATA ACCESS MARKET PARTICIPATION INPUT SESSION

Staff to establish an annual Data Access Market Participation Input Session to allow Stakeholders an opportunity to provide input of the current Framework, including access considerations and applicable access requirements.

AVAILABLE DATA POINTS

Within 60 days of Order, utilities are required to identify any available data points that were omitted from the data sets identified in Appendix A.

Areas of DAF Adoption
JU Filing/ Action
Staff Filing/ Action
Agreement Between Parties
Data Ready Certification

DATA ACCESS FRAMEWORK

Single source for statewide data access requirements. Provides uniform and consistent guidance on what is needed for access to energy-related data.

CUSTOMER SHARING OF ENERGY-RELATED DATA

The Strategic Use of Energy-Related Data proceeding defined (2) foundational principles as ways to improve an ESE's access to data.

1. Facilitate customers' ability to easily consent to share their data
2. Educate and engage customers to encourage customer consent

DAF establishes Standardized Consent Requirements to ensure a common application and process for customers, ESEs, and utilities which will afford a customer greater control over their rights of what happens with their data. DAF prevents a customer from opting out of having their data shared in aggregated data that passes privacy screen.

CONSENT PROCESS/ ENGAGEMENT PLAN

Within 90 days of Order, utilities to file a proposed Customer Consent Engagement Plan and a Consent Process Assessment. The proposed Consent Engagement Plan will include communication and engagement plans to increase customers' familiarity with data sharing options. The Consent Process Assessment will include how customers are currently made aware of their ability to consent, what options are available for consent, what information is required for consent, the length of time it takes the utility to process consent, the annual success rate of authorized consent., and an assessment of the DAF established Standardized Consent Requirements.

ALTERNATIVE ACCOUNT INFORMATION

Within 90 days of Order, Joint Utilities to file a proposal for an alternate method of account identification for completing ESE customer transaction.

Areas of DAF Adoption
JU Filing/ Action
Staff Filing/ Action
Agreement Between Parties
Data Ready Certification