Data Access Framework

Data Access Implementation Plan (DAIP)

Prepared by:
The Joint Utilities of New York

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

Filed on: September 20, 2021

TABLE OF CONTENTS

I. Introduction

On April 15, 2021, the New York State Public Service Commission (Commission) issued its *Order Adopting a Data Access Framework and Establishing Further Processes* (DAF Order),[1] adopting a Data Access Framework (DAF) "to serve as a single source for statewide data access requirements and provides uniform and consistent guidance" for such access.[2] The DAF Order also directed the Joint Utilities[3] to file a Data Access Implementation Plan (DAIP) within 60 days of the effective date of the DAF Order.[4]

This DAIP provides a uniform method for developing statewide data access requirements, a new and untested concept in providing access to utility data. This plan incorporates the information available during the limited plan development period and makes assumptions about how yet-to-be implemented tasks will actually work. The development and implementation of the DAIP depends on the development and completion of several other tasks, many of which are in their infancy. The Commission recognized this in the DAF Order and pointed out that the development of a DAF and DAIP will be an iterative process of continuous improvement.[5] The Joint Utilities plan to begin implementation of the DAIP upon Commission approval of this filing.[6]

This plan requires significant work from the utilities, Department of Public Service Staff (Staff), and other market participants. For example, proposals for a Data Ready Certification (DRC) program provider (DRC Provider) need to be solicited through a Request for Proposal (RFP) process before the DRC Provider can be selected and retained. Further, the associated platform (DRC Platform or Platform), which currently does not exist, needs to be developed and

---

[1] Case 20-M-0082, *In the Matter of the Strategic Use of Energy Related Data* (IEDR Proceeding), Order Adopting a Data Access Framework and Establishing Further Process (issued April 15, 2021) (DAF Order).
[2] *Id*., p. 8.
[3] The Joint Utilities are Consolidated Edison Company of New York, Inc. (Consolidated Edison), Orange and Rockland Utilities, Inc. O&R), Central Hudson Gas & Electric Corporation (Central Hudson), National Fuel Gas Distribution Corporation (National Fuel Gas), The Brooklyn Union Gas Company d/b/a National Grid NY, KeySpan Gas East Corporation d/b/a National Grid and Niagara Mohawk Corporation d/b/a National Grid (collectively, National Grid), New York State Electric & Gas Corporation (NYSEG), and Rochester Gas and Electric Corporation (RG&E).
[4] The Joint Utilities requested a filing extension, which was granted on June 14, 2021, with a new due date of September 13, 2021. A subsequent one week filing extension until September 20, 2021 was also granted.
[5] IEDR Proceeding, DAF Order, p. 59.
[6] The DAF Order requires that the Data Ready Certification program become operational within one year of the filing of the DAIP, *Id*., App. B, p. 1. However, given the DAF Order's requirements that parties be permitted to comment on the DAIP prior to Commission action, *Id*., p. 18, implementing the plan before Commission approval may result in an unapproved process being developed. Thus, the Commission should address the expected length of time for implementation and provide an appropriate implementation date in its order.

implemented. Given the scope of the work, the Joint Utilities are unaware of an existing product or a vendor that provides services such as certifying and verifying users to gain access to sensitive data. The procurement process will be a comprehensive one and there will be legal issues that must be worked through in the selection and hiring of a single DRC Provider to support the Joint Utilities. Notwithstanding these challenges, the Joint Utilities are eager to work with Staff and market participants to develop and implement this process.

II. DAIP Content Requirements

As required by the DAF Order,[7] the DAIP describes:

1. Details of the proposed process and timeline for selecting an entity to enable the DRC program (*i.e.*, DRC Provider).
2. Details, including development timelines, of the services to be performed by the DRC Provider, including:
    a. the necessary processes for checking Energy Service Entities (ESE) Department of Public Service (DPS) registration and verifying that cybersecurity and privacy requirements have been met, including an option for the ESE to a use third-party audit;
    b. timeframes associated with the ESE request, verification, and certification processes;
    c. creation of a user-friendly dashboard on a centralized DRC webpage that includes the listing of certified ESEs, and allows an ESE to submit a request for DRC, check status, and upload necessary documents;
    d. a "help desk" to assist ESEs with the certification process;
    e. a mechanism to allow ESE to digitally agree to the Data Access Agreement (DAA);
    f. a process for ESE suspension or revocation of certification;
    g. maintenance of the ESE listing showing date of certification, and how the re-certification can be facilitated;
    h. creation of the DAA;
    i. reporting on ESE certification metrics; and
    j. a process for each of the Joint Utilities to electronically agree to a single ESE DAA.
3. Proposed terms and conditions (T&Cs) that may be in the agreement between the Joint Utilities and the DRC Provider;
4. Cost breakdown of potential savings each utility may realize by no longer having to verify cybersecurity and privacy requirements for each ESE seeking access to data;

[7] *Id*., App. B, pp. 1-2.

5. Proposed cost recovery mechanism and cost sharing among the Joint Utilities for any incremental costs for implementing and maintaining the DRC process;
6. A plan for ESEs currently receiving data from one or more of the utilities to transition to, and complete, the DRC process; and
7. Utility plans for how each will be incorporating the adopted DRC process into existing data access request processes.

III. DAIP Sections

The plan is arranged as follows.

Section IV - Data Ready Certification Processes[8]

Section IV describes the DRC process steps as defined in the DAF Order. Documented DRC processes, roles, and responsibilities are the foundation for the Joint Utilities' proposed DRC Plan within this DAIP.

Section V - Data Ready Certification Plan[9]

Section V describes the Joint Utilities' plan to identify and secure the services of a DRC Provider and stand up the DRC process.

The DRC Plan's workstreams and tasks include:

1. **Legal:** The legal workstream will develop the DRC Provider management strategy, procurement process, contract structure, the DRC Provider contract T&Cs, and the DAA template to be used by the DRC Provider.
2. **Procurement:** The procurement workstream conducted an industry and market assessment to identify potential candidates for the role of the DRC Provider. In addition, the Joint Utilities plan to issue a Request for Information (RFI) from potential candidates to collect written information about the capabilities of various suppliers. Once the DAIP is approved by the Commission, this workstream will develop the solicitation strategy and DRC Provider requirements to be included in a Request for Proposal (RFP), draft the solicitation documents, and conduct the solicitation, evaluation, selection, and contracting with the selected DRC Provider.
3. **Finalize Requirements**: This workstream will refine the business, technical, monitoring, and reporting requirements used in the solicitation process in preparation for the on-boarding of the DRC Provider.

---

[8] *Id.,* App. B, pp. 1-2, item 2.
[9] *Id.,* App. B, pp. 1-2, items 1-3.

4. **Deployment**: The deployment workstream will manage the process for on-boarding of the DRC Provider, including implementing the required detailed business, technical, monitoring, and reporting processes and specifications. This workstream will also include developing cybersecurity and privacy verification processes and specifications.
5. **DRC Provider Preparation**: This workstream consists of developing the DRC Platform and interface specifications and test plans.
6. **Testing**: This workstream will conduct unit and integration tests in both development and production environments.

Figure 1 has been developed by the Joint Utilities to represent the above mentioned steps in the DRC plan.

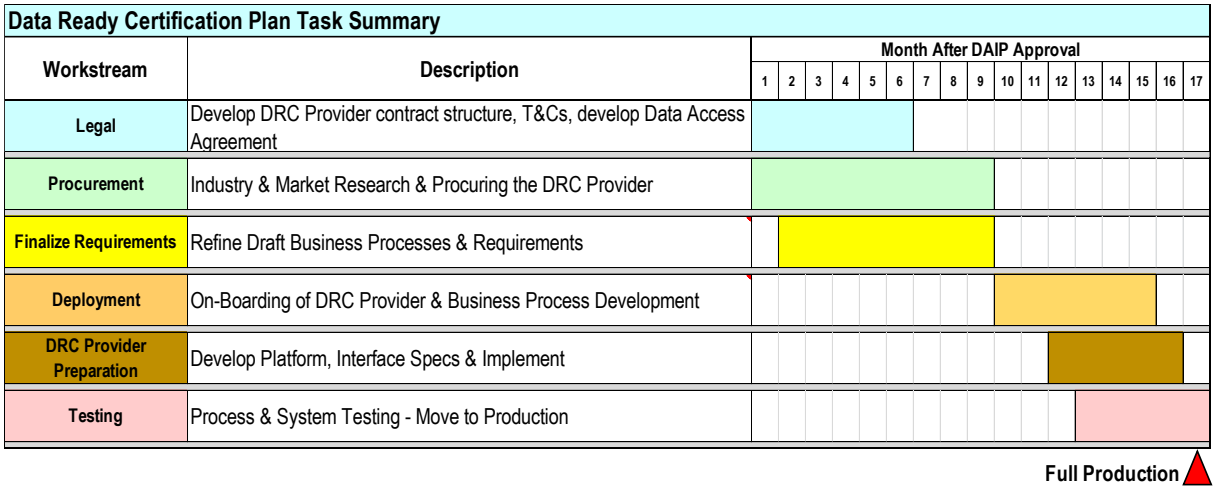

Figure 1 – DRC Plan Timeline and Workstream Summary

Section VI - DRC Cost Savings[10]

This section describes the Joint Utilities' assessment of their current processes and associated costs for the ESE application management process and verification of cybersecurity and privacy requirements to identify cost reductions, if any, that might be achieved by implementing the DRC process.

[10] *Id*., App. B, pp. 1-2, item 4.

Section VII - DRC Cost Recovery[11]

This section describes the Joint Utilities' proposed approach for cost recovery and cost sharing mechanisms associated with the development, implementation, and maintenance of the DRC platform and DRC Provider.

Section VIII - Data Ready Certification Transition Plan[12]

This section describes how the Joint Utilities will notify existing ESEs currently receiving data from one or more of the utilities about the new DRC process and the DRC process implication for data access, as well as incorporate the DRC process into existing utility data access request processes.

Section IX - Data Access Performance Metrics Reporting[13]

This section includes the proposed process for the Joint Utilities to report on Data Access Performance Metrics as applicable to the specific data access use cases and applications.

[11] *Id.*, App. B, pp. 1-2, item 5.
[12] *Id*., App. B, pp. 1-2, items 6 and 7.
[13] *Id.*, p. 54.

IV. DRC Processes

The DRC process, including the required DAA, will be managed by the DRC Provider. This process will replace the current individual utility ESE registration process to access certain energy-related data, including the execution of the Data Security Agreement (DSA) and Self-Attestation (SA), which is referred to as the business onboarding process.[14] In addition, the DRC process includes new activities that will be managed and implemented by the DRC Provider in coordination with the Joint Utilities, as described further in the DRC Plan. The DRC process does not replace the individual utility ESE technical onboarding and testing requirements[15] for access to utility-specific data access platforms after the ESE receives DRC approval.

Ideally, the DRC process will be managed by the DRC Provider via a Software as a Service (SaaS)[16] platform through a newly developed DRC Platform. This platform will be procured under a SaaS subscription as opposed to a custom development and build. ESEs and utilities will access the DRC Platform via a web browser that will allow for:

- the review of ESE applications;
- the ability to track application status;
- documentation submittal status;
- automatic DAA generation with required digital signatures;
- status notification to ESE applicants or utilities, and;
- the update of DRC public listing on the DRC website.

The DRC Provider will post its contact information for assistance with the DRC process on the DRC website, via the Application Status Portal, Support Tools, and "Help Desk" as shown in Figure 2.

A summary of the DRC Provider responsibilities is expected to include but not be limited to:

- Development and deployment of a DRC Platform to support the various DRC processes;
- Ongoing management and support, including upgrades and patches, of the DRC Platform;

---

[14] Business onboarding is the process by which an entity gains approval for access to energy-related data by agreeing to data security and privacy requirements. Business onboarding is a prerequisite to commencing technical onboarding.

[15] Technical onboarding and testing are utility-specific processes that an ESE will complete after receiving a DRC. The ESE works with each utility from which they wish to obtain data to make electronic connections with the utility platforms that will provide the data the ESE has been certified to access. Testing by each utility assures that the ESE data access is working correctly and securely for that utility-specific data delivery mechanism.

[16] Software as a Service (SaaS) is a method of software delivery and licensing in which software is accessed online via a subscription, rather than bought and installed on individual computers.

- Verification of ESE cybersecurity and privacy requirements and continuous oversight and monitoring of compliance with DAA (the DRC Provider has the authority to revoke the DRC for any ESE for non-compliance matters, cyber incidents, or data breaches).
- DRC Process Performance Reporting

The Joint Utilities have developed high level DRC processes based on the requirements described in the DAF Order.[17] These DRC processes are briefly described below and will be used as the basis for developing the more detailed initial business and technical requirements that the Joint Utilities will use in the RFI and/or RFP in pursuit of a DRC Provider.

1. DRC Process – Initial Request

The DRC process steps for an initial ESE request are described in Figure 2. The DRC Provider will manage the ESE application review, verification, and approval process through the DPS ESE Registry. The ESE will request data under all its access considerations in the initial application and not be required to make separate requests for each access consideration.[18] The DRC Provider will verify the ESE's cybersecurity and privacy requirements for the data access requested using a prescribed methodology or alternatively reviewing a valid third-party certification from a qualified entity. The proposed cybersecurity and privacy requirements verification process is based on industry best practices and standards and is described further in Section V.

Once the DRC Provider approves an ESE's DRC application, the public listing on the DRC webpage will be updated with the ESE information as to the date first certified, what Access Roles the ESE is certified for, and when the ESE is due for the next certification. The Joint Utilities will be able to consult the public DRC listing to verify the ESE level of certification before starting a technical onboarding process to share energy-related data through their individual data access mechanisms.

[17] IEDR Proceeding, DAF Order, App. C, pp. 1-2.

[18] *See id*., p. 25, where the Commission states: "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."

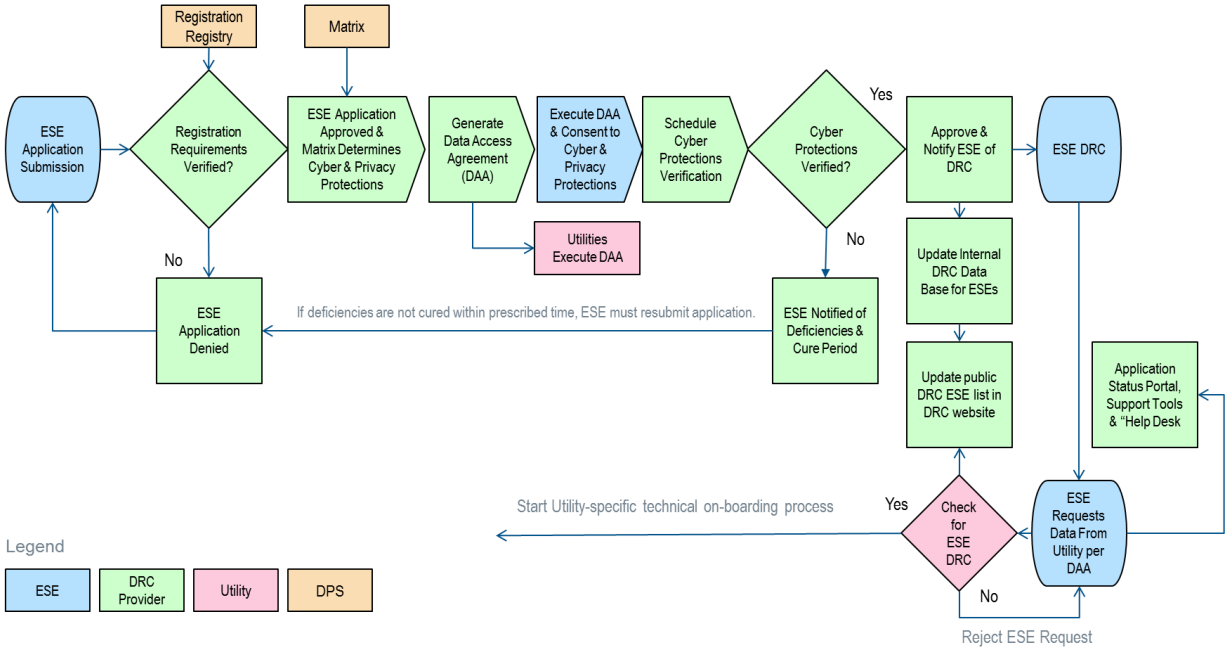

Figure 2 – DRC Process

In addition, the DRC Provider will update an internal database with all pertinent ESE compliance information (*i.e.*, certification date, application date, and data types requested, method of access, vintage of applicable DAF Matrix parameters, and certification granted) to identify ESE's that may be impacted by changes to the DAF Matrix, thus triggering an ESE re-certification requirement as described below and illustrated in Figure 4. The ESE's DRC will stay in effect until the cybersecurity and privacy requirements change in the DAF Matrix[19] or if a cybersecurity incident or data breach is detected.

2. DRC – Additional or Incremental Data Request

Although unlikely as the Commission requested that ESEs request all levels of certification desired, an ESE with an existing DRC may seek to obtain access to additional data sets and/or utility data access mechanisms.[20]

The proposed process for managing this type of ESE request is shown in Figure 3.

---

[19] *Id*., p. 17.

[20] The Commission clearly encouraged ESE's to "request all levels of certification they are seeking during the initial certification and recertification." *Id*., p. 25.
However, there may be situations where an ESE decides to access additional data not specifically identified in the initial request and this process supports that use case.

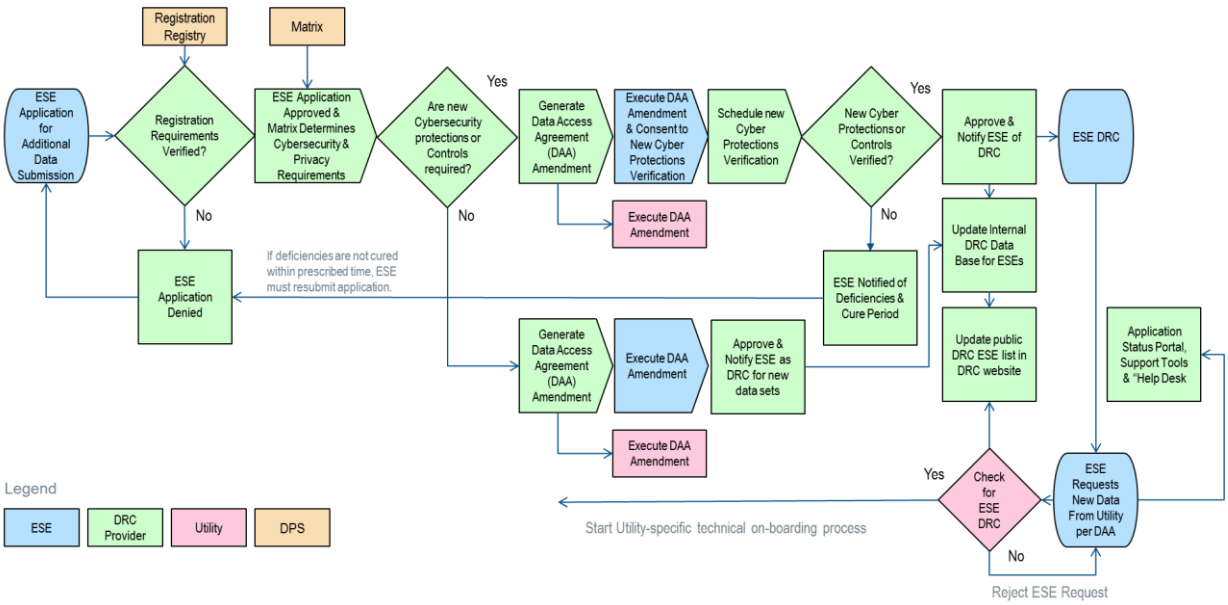

Figure 3 – DRC Process for ESE to Request Additional Data Sets

The ESE will submit the new data set request via the DRC Platform. The ESE will provide the required information (Access Roles, data set requested, purpose, etc.). The DRC Provider will verify that the ESE is registered with DPS, confirm any existing DRC the ESE has and determine (using the DAF Matrix) if the requested additional data will trigger any incremental cybersecurity or privacy requirements not covered in the ESE's current DRC.

If no additional cybersecurity or privacy requirement verifications are needed, the DRC Provider will generate an amended DAA for digital review and execution by the ESE and the applicable utilities. Once the DAA is fully executed, the DRC Provider will notify the ESE that the DRC covers all data requested and update the ESE DRC listing in the public DRC webpage. The ESE can then approach the applicable utilities with the revised DRC to begin the process of accessing the new authorized data (*i.e.*, business and technical onboarding).

If the additional data requested mandates the ESE to implement additional cybersecurity or privacy requirements, the DRC Provider will update necessary compliance requirements and generate an amended DAA which will include the additional verification requirements. The amended DAA is digitally generated for review and execution by the ESE and applicable utilities and the ESE will schedule and go through the verification steps for the new requirements following the same process as the ESE's initial DRC.

3. DRC – Recertification with Change in DAF Matrix

The DRC process described in Figure 4 is required when there is a change in any aspect of the DAF Matrix.

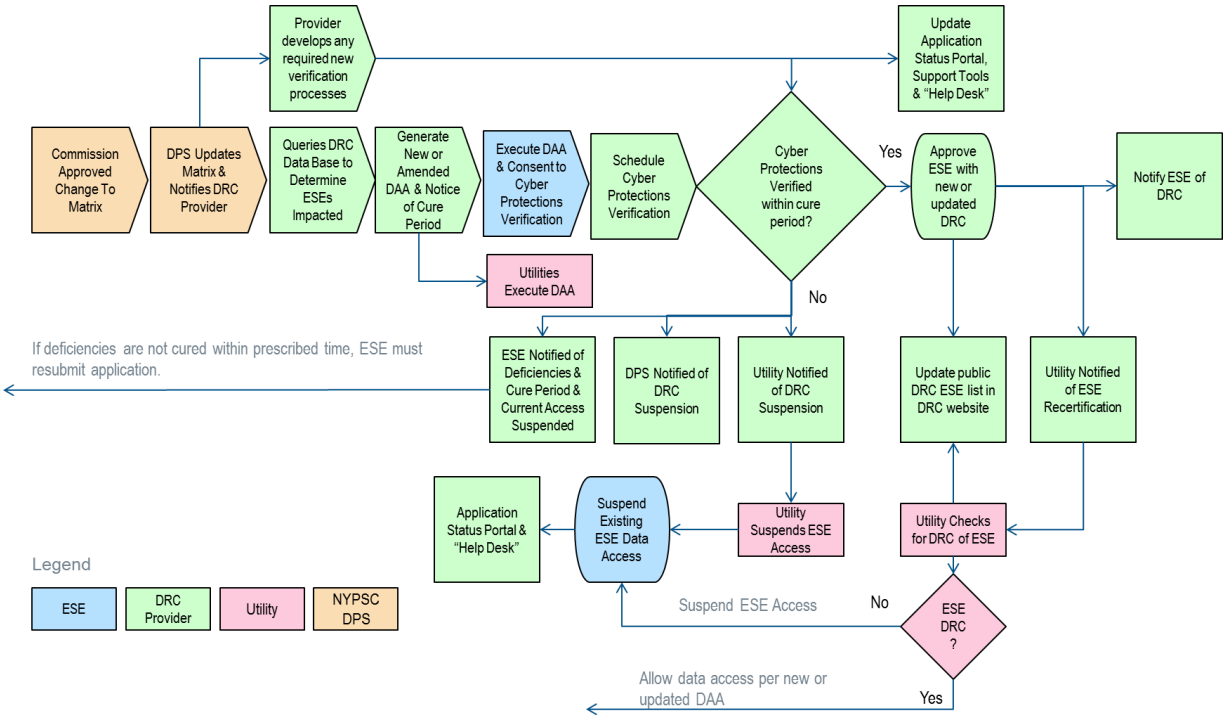

Figure 4 – DRC Provider Re-certification Process for Changes to the DAF Matrix

If the DAF Matrix requirements (*i.e.*, access mechanism, data set, applicability, or controls) change as determined by the Commission, the DRC Provider will be responsible for verifying any new cybersecurity or privacy requirements for all ESEs. The DRC Provider will send a re-certification notice to all currently certified ESEs to which the DAF Matrix change(s) apply. The DRC Provider will generate an amended DAA for the ESE and the utilities along with the re-certification notice, including a cure period for the ESE to comply by executing the revised DAA, and subsequently successfully verifying the updated cybersecurity and privacy requirements. If an ESE does not recertify before the compliance date, the DRC Provider must change the ESE certification status to suspended, update the public DRC listing, and notify the impacted utilities. The ESE will have a set number of days from suspension date to recertify before having to restart the DRC process anew, as described in the verification process description that follows.

4. DRC – Recertification Upon Data Incident

One ESE or many ESEs may experience a data incident or breach. If a data incident or breach is detected by or notification is given to the DRC Provider, the utility, or the ESE, each will be required to notify the other in conformance with the DRC contract or DAA. Depending on the incident, the utility or the DRC Provider or both can immediately suspend an ESE's data or other access. After being notified of an incident, the DRC Provider will evaluate the incident, determine which cybersecurity or privacy requirements have been impacted, and which ESE(s) should be suspended, if not done already. The DRC Provider will notify the affected utilities of the ESE DRC suspension and the utilities will take appropriate action to suspend access for that ESE or take other required actions following applicable utility-specific security processes, if not done already. The DRC Provider will also suspend the ESE DRC in the public DRC listing and will notify Staff of the suspension.

The DRC Provider, ESE, and applicable utilities must make any required notifications if there has been a cybersecurity incident. Figure 5 describes the steps in the DRC Provider recertification process upon a data incident or breach.

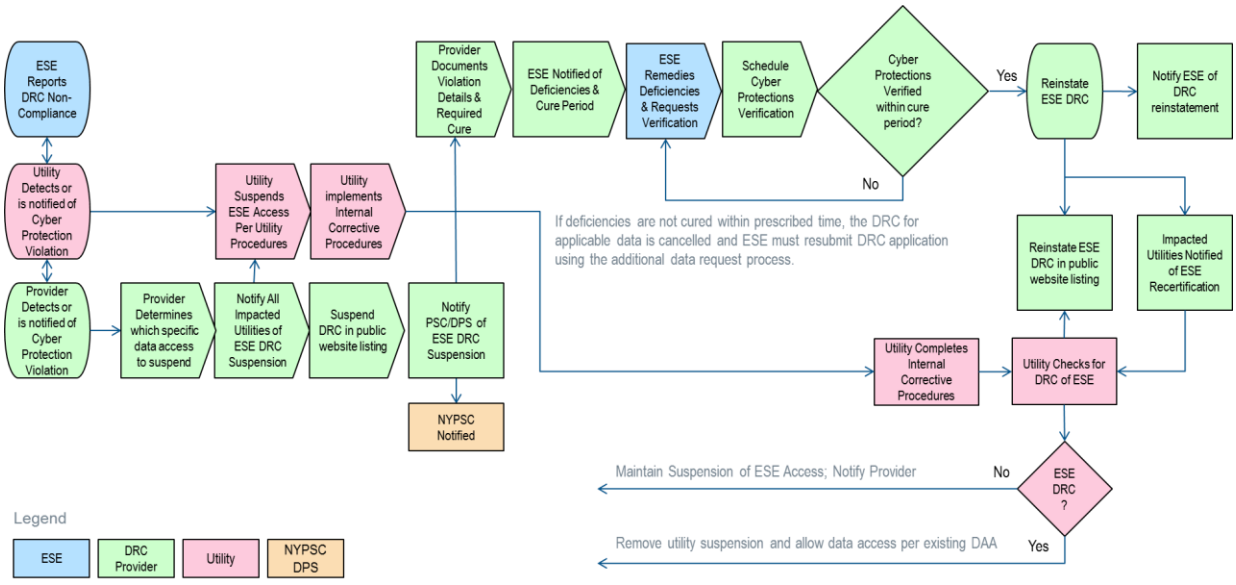

Figure 5 - DRC Provider Recertification Upon Data Incident

The DRC Provider will document the incident and determine what the required cure is for reinstatement of the DRC and notify the impacted ESE(s) of the deficiencies, the required remedy, and the cure period. The ESE shall remedy the deficiencies and request verification by the DRC Provider. If the ESE is successful in the verification process, the DRC Provider may reinstate the ESE(s) on the public DRC listing and notify the affected utilities of the reinstatement of the DRC. Restoring access to the utility data will also be governed by any additional utility-specific security requirements, technical testing, validation, and utility approval following utility-specific internal corrective actions and verification of ESE DRC reinstatement before restoring ESE access.

If the ESE fails to verify to the DRC Provider and the impacted utilities that required DRC and utility-specific technical access security remedies are in place within the cure period, the ESE's DRC will be terminated as described in the verification process that follows, and the ESE will be required to submit a new DRC request.

5. DRC – Cybersecurity and Privacy Requirements & Verification

Using the DAF Matrix, the DRC Provider will perform cybersecurity and privacy requirements verification. The DRC Provider will work with the ESE to gather the appropriate documentation, verify compliance, and then properly update and secure the compliance information provided by the ESE.

The DAF Matrix currently includes 15 cybersecurity protections that will be incorporated into the cybersecurity and privacy verification steps in the DRC process.[21] The verification process will be based on a risk sensitivity analysis of the data sets, data points and combinations thereof to adequately capture the potential impact to the Joint Utilities or their customers if the data is compromised. The DRC Provider will obtain the business rationale from the ESE DRC application as to why the data being requested is needed and the purposes of its use.

The verification process will use a methodology based on levels of data sensitivity according to the type of data requested in an ESE's application, for example:

a. **Level 1 – Low sensitivity-** Consists of data points or data types that cannot be traced to an individual or that do not provide information that may potentially damage a Joint Utility system. This data will be aggregated or anonymized to sufficiently protect individual customers.
b. **Level 2 – Moderate sensitivity -** Consists of data points or data types that are not considered personally identifiable information (PII) or critical energy infrastructure information (CEII).
c. **Level 3 – High sensitivity -** Consists of data points or data types that are required to be protected under state or federal law, or are considered PII or CEII.

[21] The Joint Utilities' comments on the DAF Matrix requested the addition of a data inventory requirement as well as a governance process intended to determine other necessary requirements given the constantly evolving state of cybersecurity and privacy. *See* IEDR Proceeding, Joint Utilities' Comments on Data Access Framework Matrix (filed August 20, 2021), pp. 4-6.

The verification process will be commensurate with the risk represented by the classification and sensitivity of the data to be shared with an ESE.

Table 1 shows the proposed verification requirements based on the sensitivity level of data classification.[22]

Data Sensitivity	Data Types	DAF Matrix Requirements[23]
Level 1 – Low Sensitivity	Aggregated Data, Anonymized Data	15 protections
Level 2 – Moderate Sensitivity	Customer Account Number, Billing Amount, Usage Information	15 protections
Level 3 – High Sensitivity	PII (name, address)	15 protections

Table 1 - Verification Requirements per Level of Sensitivity Classification

Once the DRC Provider has successfully completed the verification and certifies that the ESE meets the requirements based on the level of sensitivity, the appropriate DRC will be granted. If an ESE requests data that falls into a higher sensitivity level, the ESE will need to undergo another verification by the DRC Provider and be reissued a DRC commensurate with the appropriate level of sensitivity.

If the DRC Provider deems that the ESE does not meet the cybersecurity and privacy requirements, the ESE will have up to 6 months to remediate any failures before having to restart the DRC process anew but will not be certified to receive data until all requirements are met.

The Joint Utilities recognize that some ESEs may have a valid third-party cybersecurity audit certification. In such case, the DRC Provider may be able to leverage this audit in lieu of the DRC Provider's above stated verification requirements, if the ESE is able to demonstrate that the 15 cybersecurity protections were included within the third-party audit.

As described in the DAF Matrix comments submitted on August 20, 2021, the Joint Utilities recommend the creation of a DAF Matrix Governance and Maintenance Committee (MGMC) that will review and update the 15 cybersecurity and privacy requirements as well as a proposed new requirement that the ESE maintain a data inventory. If there are updates or new additions to the DAF Matrix, the DRC Provider will perform an assessment of the ESE's

[22] To develop Table 1, the Joint Utilities relied on industry best practices and standards to identify audit practices.

[23] Current minimum cybersecurity and privacy protections are established in the DSA and incorporated into the DAF Matrix.

compliance with the new or revised cybersecurity and privacy requirements as described in the DRC process shown in Figure 4.

The MGMC would assess the evolving cybersecurity and privacy threat landscape and determine if any additional requirements and controls are needed to mitigate and minimize risks. Any recommendations would also consider alignment with applicable state and federal regulations. Additionally, the MGMC will work with the DRC Provider to assure that verification requirements to access different types of data sets are defined and implemented as part of the DRC process.

The MGMC will conduct an annual review process to determine additional cybersecurity and/or privacy requirements based on the constantly evolving industry landscape. The MGMC would be comprised of representatives of Staff and the Joint Utilities. In addition, the Joint Utilities proposed the establishment or leverage of an existing advisory working group of stakeholders, including the DRC Provider, ESEs, and New York State Energy Research and Development Authority (NYSERDA), to provide suggestions and recommendations regarding DRC processes and requirements for the MGMC to consider.

6. DRC – Provider Data Performance Metrics and Reporting

The utilities will work with the DRC Provider to develop initial reporting metrics that correspond to the steps within the Data Ready Certification processes.[24] These metrics and Service Level Agreements (SLAs) will include, but are not limited to:

- number of ESEs registering for DRC;
- number of ESEs who have completed DRC;
- number of ESEs who are at each stage of the DRC process;
- number of ESEs who have discontinued the DRC process;
- average time to complete each step of the DRC process; and
- average time it takes an ESE to complete the DRC process from registration to certification.

The DRC Provider will prepare an evaluation report based on the data performance metrics defined during the DRC process development and file the report annually with the Commission

[24] IEDR Proceeding; DAF Order, p. 57.

prior to the Data Access Market Input Session.[25] The DRC Provider will be evaluated under these metrics annually.

The timeframe from when the ESE submits a DRC application to when that ESE receives a DRC is not controlled solely by the DRC Provider or the Joint Utilities, thus some of the performance metrics initially reported will be the actual time taken for each step in the DRC process and may be used as baseline data for developing performance standards in the future. Certain ESE actions in the DRC process may delay the overall DRC process. As shown earlier in Figure 2, the ESE will execute the DAA, consenting to the T&Cs, including the cybersecurity and privacy requirements, and the scheduling of the verification process with the DRC Provider. The DAF Order does not prescribe a maximum duration or timeframe for these steps. However, the Joint Utilities will create SLAs for process steps within the control of the DRC Provider as well as specific remedial actions to be taken if established SLA metrics and requirements are not met.

The Joint Utilities could refine the DRC process to include more prescriptive time parameters for each step of the process, but that is premature at this point. By setting up the process initially and operating for a defined test period, the Joint Utilities will better understand the critical process constraint points and set metrics that are best suited for all parties in the DRC process going forward.

[25] *See id*., p. 56, "*The Data Access Market Input Session….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."*

V. Data Ready Certification Plan

As part of this DAIP, the Joint Utilities have developed a Data Ready Certification Plan (DRC Plan) which presents a proposed set of tasks and estimated timelines to solicit and contract a DRC Provider and stand up the DRC processes and platform. The workstreams and key tasks of the DRC Plan are illustrated in Figure 6 and are described in more detail below.

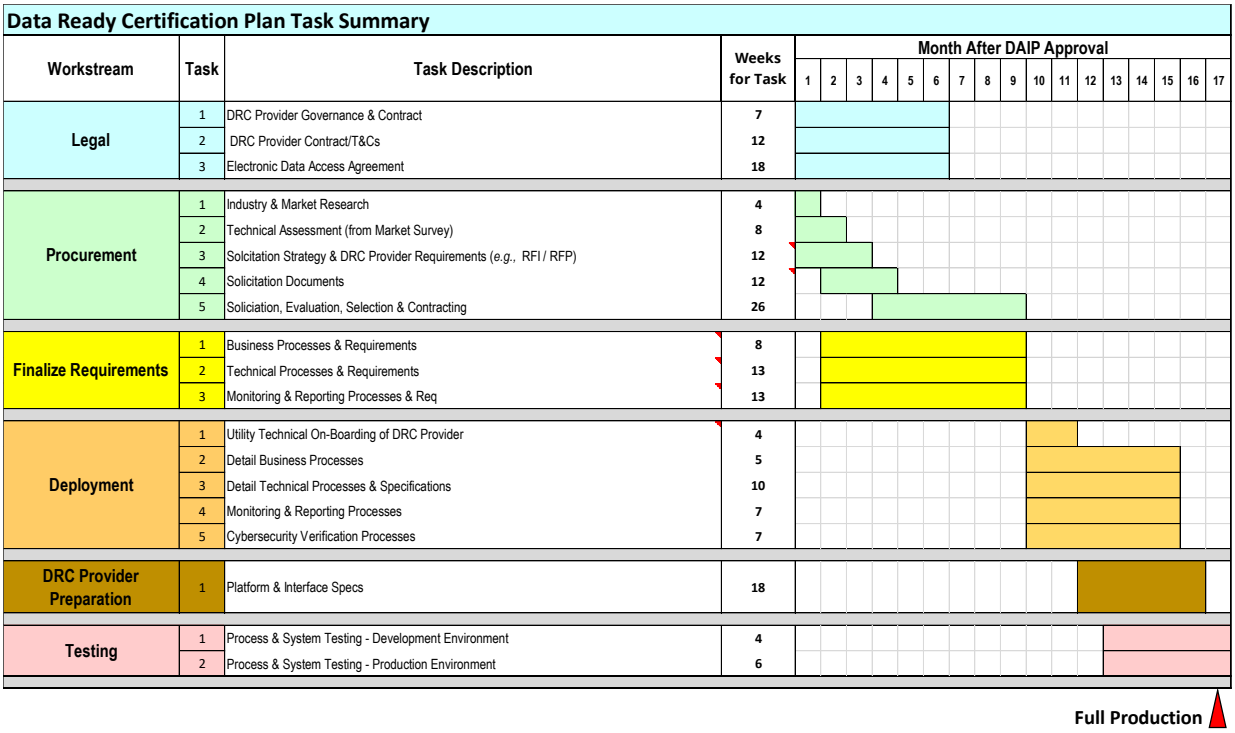

Figure 6 – DRC Plan Workstreams

This plan details a 17-month process for completion, in contrast to the Commission's prescribed 12 months in the DAF Order.[26] First, the Joint Utilities have worked to decrease the amount of time from initial estimates but believe this period is achievable. Second, to try to move the process along, the Joint Utilities will work with the DRC Provider to deploy the DRC Platform using an agile framework and providing releases in sprints. Each sprint will define the minimum viable product (MVP), a version of a product with just enough features to be usable

[26] *Id.*, App. B, p. 1. In contrast, the Joint Utilities believe that implementation cannot begin until after a Commission order is issued. *Supra*, note 6.

by early users who can then provide feedback for future product development. The Joint Utilities expect to have an MVP within 12 months after Commission approval of the DAIP.[27]

1. Legal Workstream - Development of Agreements

There are three key agreements to be developed to enable the development, implementation, and operation of the DRC process that are included within the legal workstream:

- Task 1 – DRC Provider Governance & Contract
- Task 2 – DRC Provider Contract/T&Cs
- Task 3 - Electronic Data Access Agreement (DAA)

The DRC Provider Governance and Contract process will be developed to facilitate the identification, qualification, selection, and contracting of the DRC Provider. Selecting and onboarding the DRC Provider is a critical milestone in the DRC Plan and essential for the final development of the many detailed business processes and technical requirements needed to successfully develop and implement the centralized DRC process envisioned by the DAF Order.

The task details, sequencing, and estimated durations to develop each of the Tasks in the Legal workstream are illustrated in Figure 7. "Weeks for Task" represents the estimated time to complete the Task, spread over the task duration. A detailed description of each Task is provided below.

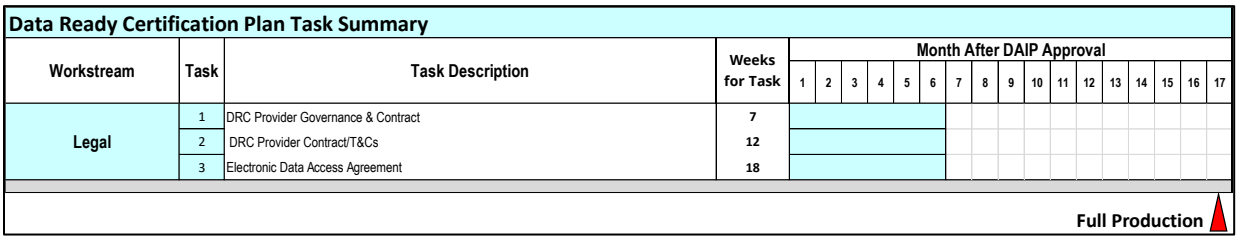

Figure 7 – Legal Workstream

Task 1 – DRC Provider Governance and Contract

Each utility will be a signatory to the DRC Provider Contract (Contract). The Contract will include a governance structure for the administration of the DRC Provider, establish payment responsibilities for each of the utilities for sharing the costs of the DRC Provider, and identify general and utility-specific T&Cs as required. The Joint Utilities anticipate that the Contract will be structured and have general provisions similar to other agreements the Joint Utilities have developed. Task 1 runs concurrent with Tasks 2 and 3 and will require an estimated of 7 weeks to complete, spread across the Legal workstream duration of approximately 26 weeks.

[27] Pursuant to DAF Order Ordering Clause two (2) and Appendix B paragraph one (1) the Joint Utilities request an extension of the time for the Data Ready Certification program to be operational from twelve (12) months to seventeen (17) months.

Task 2 – DRC Provider Contract / T&Cs

1. Term

The Term of the Contract will include a Development Term which will cover the period from the Contract effective date to the DRC Process in-production date. The Operating Term will commence on the DRC Process in-production date and will remain in effect for three (3) years, with provisions for annual renewal thereafter.

The use of a Development Term provides the Joint Utilities with a mechanism to establish a project development timeline, milestones, and development performance requirements. Should the DRC Provider fail to perform in the Development Term, remedy or termination provisions can be triggered.

2. Statement of Work

Draft business and technical requirements will be developed in the Procurement workstream and be incorporated into the DRC Provider RFP to describe the project Statement of Work. A final Statement of Work will be produced as part of the RFP negotiations.

3. General Provisions

The general provisions to be included in the DRC Provider Contact may include but not be limited to:

- Performance Requirements
  - Service Level Agreements (SLAs)
  - Performance Metrics
  - Performance penalties/cures
- Cybersecurity insurance
- Warranty provisions
- Limitation of liability, indemnity, consequential damages, insurance (general business)
- Waivers
- General Covenants
- Assignment (general) / change in control
- Dispute Resolution
- Intellectual Property, Contract Deliverables and Use Rights
- Security and Privacy Protections, including right to audit
- Terms for the use of subcontractors
- Confidentiality Terms
- Termination Provisions

Task 2 runs concurrent with Tasks 1 and 3 and will require an estimated 12 weeks to complete, spread across the Legal workstream duration of approximately 26 weeks.

Task 3 – Electronic Data Access Agreement (DAA)

The DAA will include, at a minimum, the existing DSA provisions approved by the Commission. The Joint Utilities will develop a DAA template for the DRC Provider to include the appropriate provisions based on the ESE access considerations in the DRC application. The DAA will require ESEs to agree to abide by the terms of the DAA that reflects the cybersecurity and privacy requirements that must be maintained by the ESE to maintain an active DRC.[28]

After the DRC Provider verifies that the applicant ESE is registered and approved by DPS, the DRC Provider will provide the DAA to be executed by the ESE and the Joint Utilities electronically. The DAA will detail the cybersecurity and privacy requirements as prescribed by the DAF Matrix, including any liability, indemnity, or damage provisions, or other terms and conditions, based on the matrix and data sets to be shared with the ESE and the systems with which the ESEs will connect.

Starting with the existing DSA, the Joint Utilities will develop a DAA that meets the requirements of all the utilities and considers the different ESE levels and means of access, as described in the DAF Matrix. The DAA will include, but may not be limited to the following provisions:[29]

- ESE name, designated contact, phone number, and email;
- DRC Provider contact information;
- Scope of Agreement
- Term & Termination provisions
- Cybersecurity and privacy protections as prescribed by the DAF Matrix and the verification process and controls to be applied
- ESE compliance with all applicable Commission Uniform Business Practices[30]
- Notice of re-certification requirements and results of failure to comply
  - Changes in DAF Matrix (Commission Action)
  - Changes in ESE cybersecurity rating
- Notice of Suspension provisions
  - DAA contingent upon ESE maintaining applicable DRC
  - DAA can be suspended/cancelled in whole or in part if DRC is not maintained
- Dispute resolution requirements as prescribed in the DAF Order[31]
- Notice that as the data sets expand over time and the DAF Matrix is updated, the DAA will be updated to reflect these changes as needed and ESE will have to recertify accordingly

---

[28] IEDR Proceeding, DAF Order, p. 38.
[29] *Id*., p. 39.
[30] *See* Case 98-M-1343, *In the Matter of Retail Access Business Rules; see also* Case 15-M-0180, *In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products.*
[31] IEDR Proceeding, DAF Order, pp. 39-41.

- Disclosure if Legally Compelled
- Freedom of Information Law
- Return/Destruction of Information
- Utility Right to Audit
- Investigation
- Data Security Incidents
- Intellectual Property
- Additional Obligations
- Specific Performance
- Indemnification
- Notices (general)
- Consent to Jurisdiction
- Governing Law
- Survival
- Counterparts
- Amendments and/or Waivers
- Assignment
- Severability
- Entire Agreement
- Third-Party Beneficiaries
- Force Majeure
- Relationship of the Parties
- Construction and Binding
- Terms regarding the use of subcontractors
- Confidentiality terms

Task 3 runs concurrent with Task 1 and 2 and will require an estimated 18 weeks to complete, spread across the Legal workstream duration of approximately 26 weeks.

2. Procurement Workstream - DRC Provider Identification & Selection

The Joint Utilities will identify, evaluate, and secure the services of a qualified DRC Provider to develop and deliver the services described in Section IV.

There are 5 main tasks in the Procurement workstream

- Task 1: Industry and market research
- Task 2: Technical assessment
- Task 3: Solicitation strategy and DRC Provider requirements
- Task 4: Solicitation documents
- Task 5: Solicitation, evaluation, selection, and contracting

The task details, sequencing, and estimated durations to develop each of the Tasks in the Procurement workstream is illustrated in Figure 8. A description of each Task is provided below.

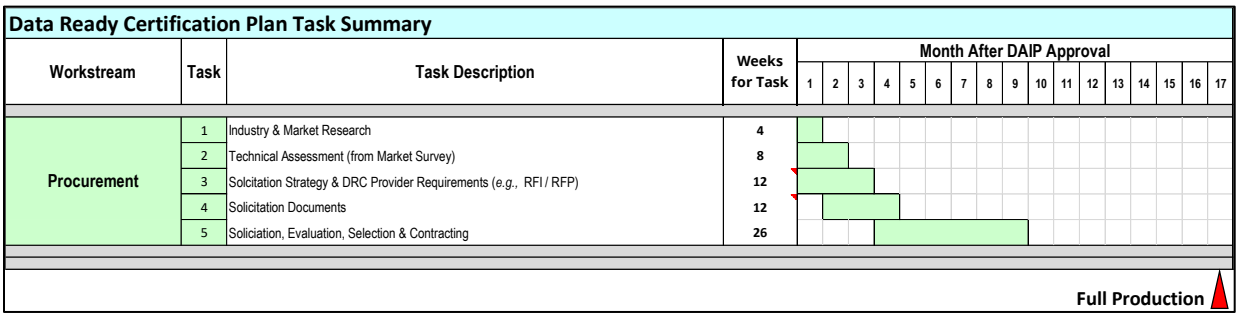

Figure 8 – Procurement Workstream

Task 1: Industry and Market Research

The DRC Provider functions and services are new to the utility industry. During the preparation of this DAIP, the Joint Utilities have surveyed the industry and market to identify where – if any – similar processes and services are in use, including what vendors, suppliers, platforms, and other tools are available. The Joint Utilities have examined the landscape for these types of services, identified business and technical best practices/lessons learned, explored processes and tools being employed for cybersecurity and privacy verification, and started to identify potential DRC Provider candidates that may be invited to participate in a solicitation process.

Task 1 runs concurrent with Tasks 2, 3, and 4. The market survey work began before the filing of this DAIP and may require an estimated 4 weeks after the DAIP is approved, in support of Tasks 2, 3, and 4.

Task 2: Technical Assessment

The industry and market survey have provided some insight on potential approaches to standing up the DRC Platform. Task 1 started before filing this DAIP and included the evaluation of potential "off the shelf" (OTS) or "customized off the shelf" (COTS) platforms versus building a customized service platform. At this point, an OTS product does not exist, and a customized platform needs to be developed. The market assessment will also inform the development of DRC Provider business and technical qualifications.

Task 2 runs concurrent with Tasks 1, 3, and 4. The platform and technical assessment work began before the filing of this DAIP and may continue for an estimated 8 weeks after the DAIP is approved, spread across the Procurement workstream duration in support of Tasks 3 and 4.

Task 3: Solicitation Strategy and DRC Provider Requirements

Findings from Tasks 1 and 2 will inform the DRC Provider solicitation strategy. This task will include the development of the draft business and technical requirements. The solicitation

strategy will be driven by the DRC Provider services needed and required qualifications compared to the known market offerings found in Tasks 1 and 2.

Draft requirements, qualifications, and expertise may include but not be limited to:

- Customer management experience
- Data governance and privacy management knowledge
- Application Development
  - Utility / application processing and management
  - Process development and engineering
  - Cloud and cloud security experience
  - Agile development methodologies
  - Application development managed services, including maintenance, Service Desk support, patches and upgrades
- Cybersecurity verification and compliance
  - Security standards and controls
  - Compliance programs oversight and processes

The Joint Utilities will issue an RFI prior to approval of this DAIP to better inform a future RFP. Task 3 runs concurrent with Tasks 1, 2 and 4. The draft business and technical requirements work began before the filing of this DAIP and may require 12 weeks to complete after the DAIP is approved in support of Task 4.

Task 4: Solicitation Documents

The Joint Utilities will draft solicitation documents based on outcomes of Tasks 1, 2 and 3 and incorporate the business, technical and commercial requirements, a draft Statement of Work (SOW), and draft DRC Provider contract with general and utility-specific T&Cs. A draft SOW for inclusion in the RFP may include, but not be limited to:

- Draft project development plan
- Draft development project organization
- DRC process description including
  - The steps in the DRC process (as described in Section IV)
  - Draft proposal for cybersecurity and privacy verification process which is intended to identify and evaluate what potential DRC Providers may recommend
  - Platform and website requirements including a user-friendly status dashboard providing a listing of certified ESEs, supports ESE application for DRC, and an "ESE help function" to assist applicants with the DRC process.
  - Description of an annual DRC Provider Performance Metrics Report (as described in Section IV)

Task 4 will run concurrently with Tasks 2 and 3 but the bulk of the work will be informed by outcomes from Tasks 1, 2 and 3 and thus are expected to be completed approximately 17

weeks after the DAIP is approved and require approximately 12 weeks of effort spread over that time frame to complete.

Task 5: Solicitation, Evaluation, Selection, and Contracting

The solicitation, evaluation, selection, and contracting process will take a minimum of 24 weeks, likely longer, and is largely subject to the factors that will not be known until Task 1 and Task 2 are completed. The timeline illustrated for Task 5 in Figure 8 is a representation and subject to substantial modification. The solicitation would be issued approximately 16 weeks after the DAIP is approved and solicitation, evaluation, selection, and contracting are estimated to take approximately 26 weeks.

3. Finalize Requirements and Design Workstream

During the DRC Provider solicitation, the Joint Utilities will update, refine, and finalize the draft DRC business and technical processes and specifications developed for and included in the DRC Provider solicitation, as well as further develop the DRC platform and interface requirements.

Figure 9 shows the Finalize Requirements workstream proposed tasks and timeline.

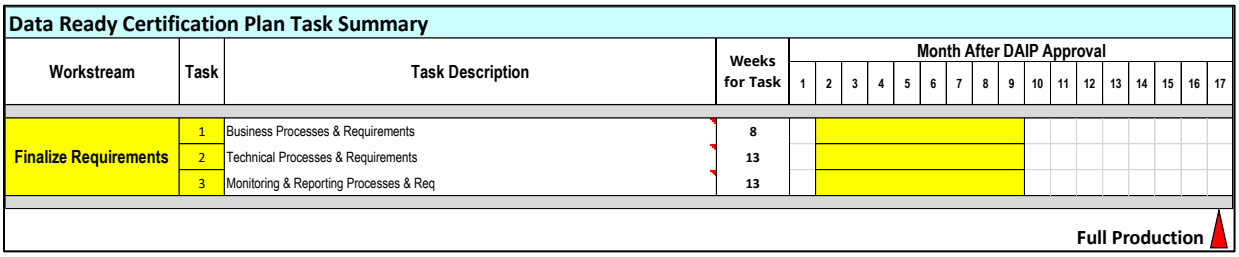

Figure 9 – Finalize Requirements and Design Workstream

Task 1: Draft Business Processes & Requirements

This task will involve finalizing DRC business use cases and supporting processes, including but not limited to, the process functionality of the platform, ESE interfaces, and automatic generation of the DAA and digital review/approval processes. This task will begin approximately 5 weeks after the DAIP is approved and require an estimated 8 weeks to complete, running concurrently with Tasks 2 and 3, spread across the approximate 34-week duration of the Finalize Requirements workstream.

Task 2: Draft Technical Processes and Requirements

This task will involve finalizing the DRC technical processes and requirements, including but not limited to, the cybersecurity and privacy protections verification methodology and process, and DRC platform and website interface requirements. This task will begin approximately 5 weeks after the DAIP is approved and require an estimated 13 weeks to complete, running concurrently with Tasks 1 and 3, spread across the approximate 34-week duration of the Finalize Requirements workstream.

Task 3: Draft Monitoring and Reporting Processes

This task will involve finalizing the DRC process monitoring and reporting requirements, including the development of performance metrics, reporting inventory, and reporting mechanisms such as a DRC dashboard, report generator, etc. This task will begin approximately 5 weeks after the DAIP is approved and require an estimated 13 weeks to complete, running concurrently with Tasks 1 and 2, spread across the approximate 34-week duration of the Finalize Requirements workstream.

4. Deployment Workstream

The Deployment workstream tasks are specifically associated with the DRC Provider. The Joint Utilities will work with the DRC Provider to refine the business and technical processes developed in the Finalize Requirements and Design workstream, obtain final process design approval and prepare for the DRC Provider to implement in the DRC platform. This workstream is shown in Figure 10 and consists of the following proposed tasks:

Data Ready Certification Plan Task Summary

Workstream	Task	Task Description	Weeks for Task	Month After DAIP Approval
				1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
Deployment	1	Utility Technical On-Boarding of DRC Provider	4	
	2	Detail Business Processes	5	
	3	Detail Technical Processes & Specifications	10	
	4	Monitoring & Reporting Processes	7	
	5	Cybersecurity Verification Processes	7	

Full Production

Figure 10 – Deployment Workstream

Task 1: Technical Onboarding of the DRC Provider

This task will involve the Joint Utilities working with the DRC Provider to update, revise and finalize the DRC project plan, tasks, and milestones used in the solicitation process and confirm deliverables including DRC Provider build milestones. This task will begin upon the DRC Provider contract execution and have an approximate duration of 4-5 weeks.

Task 2: Detail Business Processes

This task will begin concurrent with Task 1 and will involve the Joint Utilities working with the DRC Provider to update, revise and finalize the DRC business processes used in the solicitation process such as the ESE request, receipt, verify and accept/reject process, the automatic generation, and digital review/signing of the DAA, etc. This task will run concurrent with Tasks 3, 4, and 5 and have an estimated duration of 5 weeks spread over the Deployment workstream duration of approximately 26 weeks.

Task 3: Detail Technical Processes and Specifications

This task will begin concurrent with Task 1 and will involve the Joint Utilities working with the DRC Provider to update, revise and finalize the DRC detailed technical processes and specifications used in the solicitation process such as the DRC platform and web interface requirements. This task will run concurrent with Tasks 2, 4, and 5 and have an estimated duration of 10 weeks spread over the Deployment workstream duration of approximately 26 weeks.

Task 4: Develop Monitoring and Reporting Processes and Specifications

This task will involve the Joint Utilities working with the DRC Provider to update, revise, and finalize the DRC detailed monitoring reporting processes and specifications used in the solicitation process, such as the DRC reporting inventory and the reporting mechanisms. This task will run concurrent with Tasks 2, 3 and 5 and have an estimated duration of 7 weeks spread over the Deployment workstream duration of approximately 26 weeks.

Task 5: Develop Cybersecurity Processes and Specifications

This task will involve the Joint Utilities working with the DRC Provider to update, revise, and finalize the DRC detailed cybersecurity processes used in the solicitation process including cybersecurity and privacy protection verification methodology. This task will run concurrent with Tasks 2, 3 and 4 and have an estimated duration of 7 weeks spread over the Deployment workstream duration of approximately 26 weeks.

5. DRC Provider Preparation Workstream

This workstream involves the DRC Provider's preparation to develop and stand up the DRC Platform with the user interface specifications in both development and production environments. The DRC Provider will develop the DRC Platform test plan and scripts to be approved by the Joint Utilities. This workstream is shown in Figure 11 and will begin approximately 13 weeks after the DRC Provider contract is executed and will have an estimated duration of 22 weeks.

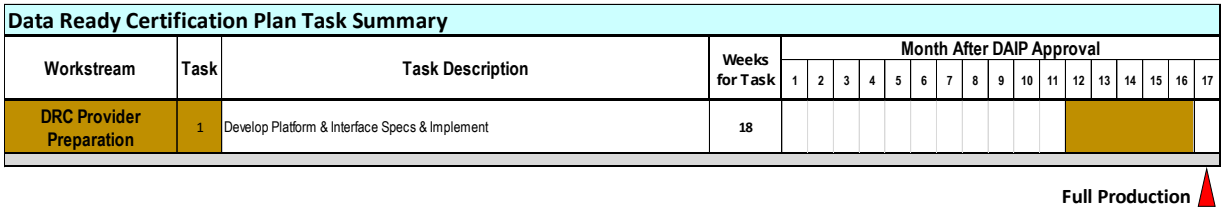

Figure 11 – DRC Provider Preparation Workstream

6. Testing Workstream

This workstream includes tasks to test specific business processes and technical functionality, integration testing, full end-to-end process tests, and a technical functionality test. The testing will occur first in a development environment and then moved to the production environment for commissioning and release for production. The final SOW and Project Development Plan will drive the detailed tasks and durations in this workstream.

The workstream tasks are detailed in Figure 12. The workstream will start approximately 17 weeks after the DRC Provider contract signing and have an estimated duration of 22 weeks.

Data Ready Certification Plan Task Summary

Workstream	Task	Task Description	Weeks for Task	Month After DAIP Approval																
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Testing	1	Process & System Testing - Development Environment	4																	
	2	Process & System Testing - Production Environment	6																	

Full Production

Figure 12 – Testing Workstream

VI. DRC Cost Savings

Many of the processes identified in the DAIP are new and incremental to existing or planned processes for the Joint Utilities. Currently, the Joint Utilities' resources involved in ESE certification for access to non-public data encompass two key activities, business onboarding / certification (including application management and cybersecurity and privacy verification) and technical onboarding. The proposed centralized DRC process in the DAIP will replace the current utility / business onboarding process only, as technical onboarding will continue for existing programs, such as Green Button Connect (GBC) and EDI for ESCOs, and will require additional support as these programs grow.

The current business onboarding / certification process includes the utilities providing a DSA and SA to interested ESEs upon request. Once an ESE returns an executed DSA and completed SA, the Joint Utilities review the DSA/SA for completeness, accuracy, and a signature and file the DSA/SA in their records. These actions (essentially sending and receiving an email) are not time or labor-intensive tasks. As a result, for those utilities that currently receive ESE applications to access non-public customer or system data and utility systems, the resources and employees involved in the ESE business onboarding / certification process only use a small fraction of their time to support such activities. Further, because almost all ESEs provide a completed DSA and SA, the number of ESEs that require audits or further investigation to ensure compliance is minimal and consists of two situations: 1) conduct random audits of a small number of ESEs on an annual basis to ensure compliance and, 2) conduct compliance investigations where an ESE has not provided a complete DSA and SA. These audit processes have not consumed a material amount of time and labor costs.

Each utility assessed its existing ESE data access mechanisms and processes, ESE application volumes, and associated processing costs. Given the current volume of ESE applications and limited time spent on the business onboarding / certification process vs. technical onboarding, the Joint Utilities identified no material cost savings to be captured by no longer having to use its resources for the ESE business onboarding / certification process. As such, the Joint Utilities did not identify any funding sources to be allocated towards covering the DRC process costs.

VII. DRC Cost Recovery

The Joint Utilities' proposal regarding the recovery of DRC costs consists of two components: 1) cost-sharing among the Joint Utilities and 2) cost recovery of each utility's resulting share of costs. For the sharing of DRC costs, the Joint Utilities propose that such costs be allocated to the Joint Utilities, as well as to Liberty Utilities and Long Island Power Authority (LIPA). The cost allocations are based on the utilities' total MWh sales of electricity and Dth sales of gas[32] to all customers, as reported in their Annual Reports to the Commission for the Year Ended December 31, 2019.[33] LIPA deliveries are based on data provided by LIPA for the respective period. The MWh and Dth sales used do not include sales for resale and gas sales for electric power generation (firm gas sales for electric generation for Central Hudson and RG&E are included). Allocation of DRC costs across electric and gas deliveries for all utilities will ensure equitable treatment of single service utilities (electric only and gas only) where service territories for different utilities overlap. Table 2 provides the results of the DRC Provider cost allocation, on a percentage basis.[34]

Company	MWh	Dth	MWh Equivalent*	Total	Allocation
	(1)	(2)	(3) = (2) * CF	(4) = (1) + (3)	(5) = (4) / Sum (4)
Central Hudson	4,928,035	16,838,792	4,933,783	9,861,818	3%
Consolidated Edison	55,292,620	194,795,198	57,075,188	112,367,808	29%
NYSEG	15,514,709	56,350,721	16,510,818	32,025,527	8%
National Grid	33,980,642	391,016,610	114,568,258	148,548,900	38%
O&R	3,952,524	25,663,233	7,519,353	11,471,877	3%
RG&E	7,070,604	61,182,049	17,926,402	24,997,006	6%
National Fuel Gas	-	102,486,735	30,028,716	30,028,716	8%
Liberty Utilities	-	7,506,579	2,199,435	2,199,435	1%
LIPA	18,801,000	-	-	18,801,000	5%
Total	139,540,134	855,839,917	250,761,952	390,302,086	100%
* MWh/Dth Conversion Factor (CF)=	0.293001				

Table 2 - DRC Provider Cost Allocation Mechanism

The Joint Utilities propose that each utility's allocation of DRC costs, which will include implementation, or start-up, and ongoing operation and maintenance costs, be deferred as a regulatory asset with carrying charges applied on the net of tax balance at each utility's pretax overall cost of capital until fully recovered.

---

[32] gas deliveries converted to an MWh equivalent.

[33] The PSC Annual Filings may be found at: https://www3.dps.ny.gov/W/PSCWeb.nsf/ArticlesByTitle/A97C16D00017FB1F852578E0005454E8

[34] The Joint Utilities recognize that this may not reflect all of NYPA sales, however, for simplicity, NYPA deliveries are included as part of each utility's deliveries from NYPA programs and recovered in a similar manner as costs are handled currently.

Further, the Joint Utilities propose that the way these costs, net of identified savings opportunities, if any, are to be recovered be dependent on the magnitude of the balance subject to recovery. As mentioned in prior sections, the Joint Utilities are in the process of preparing an RFI to identify a rough order of magnitude regarding the potential cost of the DRC Provider.

The Joint Utilities propose that the costs, and associated carrying charges, continue to be deferred for future recovery as determined by the Commission.

To the extent costs exceed initial expectations, the Joint Utilities propose that DRC cost recovery be modified to be recovered through the use of an existing surcharge mechanism at each utility for bill presentment purposes. While the surcharge mechanisms may differ among utilities, the underlying structure of recovery would be consistent across utilities reflecting surcharge factor determination on an annual basis, electric and/or gas rates set volumetrically, rates set subsequent to the initial determination to include a reconciliation component, and all rates filed on a statement in advance of the proposed effective date.[35]

VIII. DRC Transition Plan

The Joint Utilities will coordinate with their Retail Access departments and any other groups currently interfacing with ESEs to consistently explain the DRC process to new or existing ESEs.

1. Existing Energy Service Entity

The Joint Utilities propose the following steps to notify existing ESEs of the new DRC process:

- **Step 1** - Once Staff publishes the centralized listing including all registered ESEs and the Data Access Framework Application Guide,[36] the Joint Utilities will send a notification e-mail to their existing ESEs to describe the new DRC process and provide estimated dates to launch the DRC platform. The DSP Staff Data Access Framework Guide[37] will clearly explain the components of the DAF and DRC process that will be developed with the DRC Provider.
- **Step 2 -** The Joint Utilities will send a second e-mail notification to the existing ESEs once the DRC Provider has been contracted and set up, providing more details regarding the new DRC process and associated cybersecurity and privacy requirements.
- **Step 3** - The Joint Utilities will send a third e-mail notification to existing ESEs once the DAA has been approved by the Commission and the DRC process is active for online

[35] As this process continues, the Joint Utilities will continue to identify potential costs and which entity, including potentially the ESEs or other entities, should bear responsibility for such costs.
[36] IEDR Proceeding, DAF Order, p. 61, 69-70. Also referred to in the DAF Order as the "Data Access Guide."
[37] *Id.*, p. 61.

application through the DRC website. At such time, the existing ESEs must submit a certification of their cybersecurity and privacy requirements. The existing ESEs will be required to submit a DRC application through the DRC website within 4 months of receipt of the first e-mail notification requesting to submit a DRC application. The Joint Utilities will send two more monthly e-mails as reminders to the existing ESEs to submit a DRC application. If the existing ESEs fail to submit a DRC application after 4 months of the first e-mail request, the ESEs may have their data access. The DRC website will have a Frequently Asked Questions (FAQ) section and the DRC Provider contact information so facilitate the process for ESEs. The ESE DRC will be valid for all certified data types requested with all the Joint Utilities.

2. New Energy Service Entity

The Joint Utilities will publish information about the new DRC process before it becomes live to begin educating customers and ESEs on the upcoming changes. The information, including links to Staff's Data Access Framework Application Guide, will be shared on the individual utility websites, the Joint Utilities website, and the Joint Utilities DSP Enablement quarterly newsletter.

The Joint Utilities will schedule a public stakeholder webinar to share information with ESEs and other interested stakeholders about the new DRC process at least three months before it becomes operational. Once the DRC process becomes operational, the Joint Utilities will update existing utility data access request processes and websites to redirect requests to the dedicated DRC website.

IX. Data Performance Metrics Reporting

The Joint Utilities will submit a Data Performance Metrics report semi-annually as applicable for each of their non-public data access use cases and applications. The semi-annual reports will be submitted approximately 30 days after the end of the last reporting month under the DAF Order. For example, for the period January to June, the report will be submitted by July 31.

The Joint Utilities will track the Data Performance Metrics provided in the DAF Order[38] to assess ESE data access effectiveness, including the following as applicable by each data access use case and their associated User Agreement:[39]

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 (in 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; and
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.

The specific Data Performance Metrics for each data access use case will ultimately be based on the Data Quality and Integrity Standards contained in the User Agreements developed by Joint Utilities and accepted by ESEs when accessing the specific data access use mechanism.

---

[38] *Id*., pp. 54–55.

[39] *Id*., p. 48, where the Commission defines the User Agreement as: "*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."* User Agreements are specific to each utility: "*The Commission will require use-case specific User Agreements 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."*

X. APPENDIX - DEFINITIONS

1 Access Role: The access role is determined through the Data Ready Certification (DRC) process and details the exact data sets and transmittal/access methods through which the Energy Services Entity (ESE) is approved to access energy-related data.

2 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.

3 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.

4 Confidential Customer Utility Information: Information that Utility is: (A) required by the UBP at Section 4: Customer information(C)(2), (3) or UBP DERS at Section 2C: Customer Data, to provide to ESCO, Direct Customer, DERS, GBC Provider or Governmental Unit or (B) any other information provided to ESE by Utility and marked confidential by the Utility at the time of disclosure, but excludes (i) information which is or becomes generally available to the public other than as a result of a disclosure by Receiving Party or its Representatives; (ii) information which was already known to Receiving Party on a non-confidential basis prior to being furnished to Receiving Party by Disclosing Party; (iii) information which becomes available to Receiving Party on a non-confidential basis from a source other than Disclosing Party or a representative of Disclosing Party if such source was not subject to any prohibition against transmitting the information to Receiving Party and was not bound by a confidentiality agreement with Disclosing Party; (iv) information which was independently developed by the Receiving Party or its Representatives without reference to, or consideration of, the Confidential Information; or (v) information provided by the customer with customer consent where the customer expressly agrees that the information is public.

5 Confidential ESE Information: Information that ESE is: (A) required by the Uniform Business Practices ("UBP"), DERS UBP ("UBP DERS") or Commission order or rule to receive from the end use customer and provide to Utility to enroll the customer or (B) any other information provided by ESE to Utility and marked confidential by the ESE, but excludes (i) information which is or becomes generally available to the public other than as a result of a disclosure by Receiving Party or its Representatives; (ii) information which was already known to Receiving Party on a non-confidential basis prior to being furnished to Receiving Party by Disclosing Party; (iii) information which becomes available to Receiving Party on a non-confidential basis from a source other than Disclosing Party or a representative of Disclosing Party if such source was not subject to any prohibition against transmitting the information to Receiving Party and was not

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

6 Confidential Information: Collectively, Confidential Customer Utility Information or Confidential ESE Information.

7 Critical Energy/Electric Infrastructure Information (CEII): Information related to or proposed to critical electric infrastructure, generated by or provided to the Federal Energy Regulatory Commission (FERC) or other Federal agency, other than classified national security information, that is designated as critical electric infrastructure information by FERC or the Secretary of the Department of Energy pursuant to section 215A(d) of the Federal Power Act.

8 Cybersecurity Protections: Risk mitigation controls implemented to address the risk to IT systems and the data they house.

9 Data Access Agreement (DAA): By the condition of seeking access to energy-related data, the DRC Provider will require ESEs to agree to abide by the terms of a Data Access Agreement that includes the requirements established in the DAF Order.

10 Data Access Framework Matrix (DAF Matrix): The DAF Matrix maps the existing Commission authorized cybersecurity and privacy requirements to the various combinations of purpose, access mechanism, and data type. The DAF Matrix includes the components of all the existing Data Security Agreements and the Self-Attestation, as well as the other existing data access requirements. Each requirement is listed with a name, description, where it originated from, indicators for access mechanism and/or data sets, and the use case applicability.[40]

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

12 Data Performance Metrics: As defined in Section IX of this DAIP.

13 Data Ready Certification Platform (DRC Platform or Platform): The software developed and managed by the DRC Provider to meet the processes described in the DAF Order, including but not limited to the workflows to manage the DRC processes, dashboards, metrics, content management, and ESE-related information.

14 Data Ready Certification Process: As defined in Section IV of this DAIP.

[40] *See* IEDR Proceeding, Data Access Framework Matrix (filed May 17, 2021).

15 Data Security Agreement and Self Attestation (DSA and SA): As defined and established in Case 18-M-0376, and filed on December 16, 2019.

16 Data Security Incident (Incident): Data Security Incident means a situation when Utility or ESE reasonably believes that there has been: (A) the loss or misuse (by any means) of Confidential Information; (B) the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Confidential Information, or Private Information as defined by GBL § 899-aa, computer systems, network and devices used by a business; (C) any other act or omission that compromises the security, confidentiality, or integrity of Confidential Information, or (D) any material breach of any Data Protection Requirements in relation to the Processing of Confidential Information, including by any current or former Representatives.

17 Energy Service Entity (ESE): Any entity (including, but not limited to, ESCOs, DERS, and Community Choice Aggregation (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.

18 ESCO: Has the meaning set forth in the Uniform Business Practices (UBP) approved by the Commission in Case 98-M-1343 and as it may be amended from time to time, which is "an entity eligible to sell electricity and/or natural gas to end-use customers using the transmission or distribution system of a utility."

19 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.

20 Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (*e.g.*, name in combination with any one or more of the following data elements: address, social security number or other identifying number or code, residential and/or mobile telephone number, email addresses, driver's license number or other driver identification data, financial account information, credit-related information, including any information related to credit checks or background checks, credit or debit card numbers, and personal identification numbers such as access codes, security codes, or passwords that would permit access to financial accounts, medical insurance numbers, and medical or health information, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements (*i.e.*, indirect identification).

21 Privacy Protections: Risk mitigation controls that are implemented to address the privacy risks of the data.

22 Service Level Agreement (SLA): An agreement that defines the level of service expected by the utility from the DRC Provider, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-on service levels not be achieved.

23 Software as a Service (SaaS): A method of software delivery and licensing in which software is accessed online via a subscription, rather than bought and installed on individual computers.

24 Statement of Work (SOW): A document within a contract that describes the work requirements for a specific project along with its performance and design expectations. The main purpose of the SOW is to define the liabilities, responsibilities, and work agreements between two parties, usually clients and service providers.

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

26 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.