STATE OF NEW YORK

DEPARTMENT OF PUBLIC SERVICE

Case 20-M-0082 – Proceeding on Motion of the Commission Regarding Strategic Use of Energy Related Data

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

DEPARTMENT OF PUBLIC SERVICE STAFF

PRELIMNARY PROPOSAL FOR MODIFICATIONS TO THE DATA ACCESS FRAMEWORK

Dated September 4, 2026

Table of Contents

1. Introduction

On October 20, 2025, the Public Service Commission (Commission) issued its Modification Order, directing Department of Public Service Staff (Staff) to file a proposal recommending modifications to New York's Data Access Framework (DAF or the Framework).[1] The Commission found that several factors, including evolving market conditions, unimplemented processes, and changes in the cybersecurity landscape warranted a review of existing data access requirements. The Modification Order directed Staff to propose modifications that support customer choice, enable useful access to useful data, and appropriately address cybersecurity and privacy risks. The Commission further emphasized the need for statewide consistency, enforceability, and alignment with other frameworks, including the Uniform Business Practices (UBP).[2]

Pursuant to the Modification Order, Staff submits this Preliminary Proposal recommending modifications to the Framework. This Staff proposal responds to the Commission's directive in the Modification Order, and incorporates the information and concerns raised in filings to date, including various filings from the Joint Utilities,[3] such as the Data Access Implementation Plan, the Consent Process Assessment and Customer Consent Engagement Plan, and the May 4, 2022 Petition to Modify.[4] The recommendations presented in

---

1 Case 20-M-0082, Proceeding on the Motion of the Commission Regarding Strategic Use of Energy Related Data, Order Directing Staff Proposal to Modify Data Access Requirements (issued October 20, 2025) (Modification Order).

2 The UBP are posted on the Commission's website and updated as changes are made by the Commission. The current UBP can be found at: https://dps.ny.gov/uniform-business-practices.

3 The Joint Utilities include: Central Hudson Gas & Electric Corporation; Consolidated Edison Company of New York, Inc.; New York State Electric & Gas Corporation; Niagara Mohawk Power Corporation d/b/a National Grid; Orange and Rockland Utilities, Inc.; and Rochester Gas and Electric Corporation.

4 See Case 20-M-0082, supra, Joint Utilities Data Access Implementation Plan (filed September, 20, 2021) (DAIP); Joint Utilities Consent Process Assessment and Customer Consent Engagement Plan (filed September 20, 2021); and Joint Utilities Petition to Modify the Data Security Agreement Self-Attestation Requirements and Implement a Governance Review Process for Regular Self-Attestation Updates (filed May 4, 2022) (Petition to Modify).

this Preliminary Proposal are intended to establish high-level concepts for further consideration and stakeholder input.

2. Background

On April 15, 2021, the Commission adopted the Data Access Framework to serve as a single statewide source for data access requirements, outlining uniform rules, roles, and responsibilities, as well as protections around energy-related data access.[5] The Commission intended for the DAF to increase customers' familiarity with, and consent to, appropriate data sharing; improving access to customer energy-related data by Energy Service Entities (ESEs); link energy-related data with other sources of building data; and provide the mechanisms for appropriate access to energy-related data.[6]

As part of the DAF Order, the Commission ordered the creation of a Data Ready Certification (DRC) process to replace the existing Data Security Agreement (DSA) and Self-Attestation (SA) that were previously established within the Minimum Cybersecurity Protections Order.[7] To that end, in the DAF Order, the Commission directed Staff to file a Data Access Matrix (Matrix) that maps the existing Commission authorized cybersecurity and privacy requirements to the various combinations of access considerations such as purpose, access mechanism, and data type.[8] The Matrix was intended to be used by a third-party DRC Provider to determine what cybersecurity and privacy requirements the ESE would need to follow. Staff filed the Matrix on May 17, 2021.

---

5 Case 20-M-0082, supra, Order Adopting a Data Access Framework (issued April 15, 2021) (DAF Order).

6 DAF Order, pp. 2-3.

7 Case 18-M-0376, 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) (Minimum Cybersecurity Protections Order). The Minimum Cybersecurity Protections Order did not specifically adopt terms of the DSA (which were set through a collaborative business-to-business process), but instead adopted minimum cybersecurity and data privacy requirements for entities that receive customer data from, or exchange customer data with, the utilities on an electronic basis other than by email.

8 DAF Order, pp. 36-37.

Since the adoption of the DAF and the filing of the Matrix, implementation of the DRC has not progressed as originally intended. Although several required compliance filings were submitted by the Joint Utilities that will be discussed in detail within the next section, including the DAIP, the Consent Process Assessment and Customer Consent Engagement Plan, and the May 4, 2022 Petition to Modify, these filings remain pending before the Commission and have not yet been addressed. As a result, the DRC process has not been implemented and entities seeking customer-consented data continue to rely upon execution of utility-specific DSAs. Consequently, several of the statewide efficiencies and governance improvements anticipated by the Commission have not yet been realized. The Commission therefore determined that Staff should evaluate whether the original implementation approach remains appropriate or whether alternative mechanisms better achieve the underlying objectives of DAF.[9]

Based on these factors, the Commission determined that a comprehensive review and potential update of DAF is necessary to ensure continued alignment with market needs, customer expectations, evolving risks, and statutory requirements.

2.1 Filings Made Following DAF

The Commission, as part of the DAF Order, directed the Joint Utilities to submit several implementation filings following the adoption of the Framework. While these filings remain pending, they provide insight into implementation challenges and inform several of the recommendations outlined in this Preliminary Proposal.

In September 2021, the Joint Utilities filed their DAIP, which outlined the utilities' approach to implementing DRC and selecting a third-party DRC provider. The proposed DRC process would replace the current method for ESEs to access certain energy-related data, which includes the execution of the DSA and SA with each individual utility, and implement new functions that would be managed by a DRC Provider and the Joint Utilities.[10] Under this proposed structure, the ESE would submit an application that includes all of its access considerations and would not be required to submit separate requests for each access

[9] Modification Order, p. 8.

[10] DAIP, p. 6.

consideration with each utility.[11] The DRC Provider would then verify the ESE's cybersecurity and privacy requirements against the Matrix and approve or deny the application.

The Joint Utilities' DAIP also outlined the scope and complexity of the DRC process. The DAIP proposed that ESEs submit a centralized application identifying their requested access considerations to be reviewed by a third-party DRC Provider that would verify the applicable cybersecurity and privacy requirements, which would be managed through a centralized DRC platform that contains the applications, documentation, certification status, Data Access Agreements, reporting, and other administrative functions.

The filed DAIP further contemplated the procurement of a DRC Provider, development of a DRC platform, development of legal agreements, refinement of technical requirements, cybersecurity and privacy verification processes, testing, deployment, monitoring, reporting, cost recovery, and transition of existing ESEs into the DRC process. The Joint Utilities also recognized that the proposed process represented a new and untested approach and that significant work by the utilities, Staff, and other market participants would be necessary before implementation.[12]

Because the DRC process has not been implemented to date, ESEs continue to rely on existing DSA and SA processes. Staff notes, however, that while the DRC process was envisioned to provide consistent requirements, the requirement for an ESE to execute the DSA and SA prior to obtaining access to data has continued to achieve the regulatory objective of establishing a consistent, statewide mechanism for evaluating cybersecurity and privacy requirements even without an operational DRC process. At the same time, the current DSA and SA process requires ESEs to execute agreements with individual utilities, creating administrative burdens. The DSA and SA established a foundation for cybersecurity and privacy protections; however, Staff also recognizes opportunities to revise the agreements and the process to improve consistency and reduce unnecessary burdens.

In addition to the DAIP, the Joint Utilities filed a Consent Process Assessment and Customer Consent Engagement Plan in September 2021, which proposed enhancements to

---

[11] DAIP, p. 7.

[12] DAIP, p. 1.

consent processes and customer engagement. The filing provides information on each of the utilities' current processes for customers to consent to sharing data with third parties, an assessment of nine Standardized Consent Requirements (SCRs) established in the DAF Order, and identification of where the utilities align and differ. The filing also provides information on the Joint Utilities' plan to communicate consent options to customers, noting the customer education and outreach campaigns can be adapted as needed when new data sharing mechanisms requiring utility customer consent are implemented.

On May 3, 2022, the Joint Utilities filed their Petition to Modify, proposing to, among other things, update the SA to reflect current minimum protections and best practices and propose a governance process for regular review of the SA terms. Specifically, the Joint Utilities proposed to modify and update six of the fifteen Commission established requirements within the existing SA, and establish three new requirements, discussed further below.

3. Scope of Staff's Preliminary Proposal

As directed by the Commission, this Staff Proposal reviews and identifies modifications to the Data Access Framework that simultaneously support customer choice, enable useful access to useful data by ensuring that data access processes are consistent, and appropriately address cybersecurity and privacy concerns. This Staff Proposal also evaluates how to achieve the intended outcomes of the Data Ready Certification process, consistent with the Commission's directive to explore how New York can achieve the intended risk-based approach for establishing cybersecurity and privacy requirements to ESEs, given that the DRC has not been realized.[13] Further, this Staff Proposal aligns DAF requirements with the Uniform Business Practices (UBPs) for Energy Service Companies (ESCOs) and Distributed Energy Resource (DER) Suppliers to ensure consistency with cybersecurity and privacy requirements, customer consent requirements, and data availability/data point definitions.[14]

In accordance with the Modification Order, this Preliminary Proposal also addresses additional considerations such as: (1) how customer understanding of data sharing is evolving; (2) the risks associated with data sharing; (3) customer expectations for providing

[13] Modification Order, p. 8.

[14] Modification Order, pp. 8-9.

consent; (4) legislation related to cybersecurity, privacy, and customer consent; and (5) provisions in the UBPs related to data points available, cybersecurity and privacy requirements, and customer consent requirements.[15]

Staff expressly notes that several issues addressed in this proposal involve policy choices that would benefit from additional stakeholder participation before final Commission action. Accordingly, Staff recommends that this Preliminary Proposal serve as the foundation for focused stakeholder comments, and for a technical conference to be held to identify issues and further develop the process. The technical conference would provide utilities, ESEs, consumer advocates, cybersecurity professionals, and other interested stakeholders with an opportunity to discuss implementation challenges, identify operational considerations, and recommend refinements to the Framework. The record developed through that process would provide Staff with additional information to develop and issue, for Commission consideration, a final proposal to modify the Data Access Framework.

4. Considerations Informing Staff's Preliminary Proposal/Recommendations

4.1. Joint Utilities Petition to Modify

The Joint Utilities' Petition to Modify, along with party comments submitted in response thereto, provide a useful starting point for Staff's review. The Joint Utilities proposed six modifications to existing SA requirements, three new requirements, and a governance process intended to provide periodic review and modification to the SA. Among other things, the Joint Utilities proposed provisions addressing role-based access controls, encryption in transit and at rest, endpoint protection, employee background screening, and timely revocation of access when access to customer information is no longer required. The proposed new requirements would address data catalogs, network communications and segmentation, and physical access to information systems and operating environments. The Joint Utilities also proposed establishing a Governance Committee consisting of up to five Joint Utilities representatives and five Staff representatives, with an Advisory Working Group that would include ESEs and NYSERDA.

---

[15] Modification Order, p. 9.

The Governance Committee would review the SA on a recurring basis and recommend changes to the Commission.

In comments responding to the Petition to Modify, stakeholders raised concerns regarding both the proposed requirements and the proposed governance structure. Several parties supported a risk-based approach and questioned whether certain requirements should apply uniformly to all ESEs. Parties also raised questions regarding the applicability of particular National Institute of Standards and Technology (NIST) standards, the treatment of cloud-based infrastructure and serverless computing, encryption of email communications, the use of certification or third-party audit mechanisms in place of an SA, the appropriate role of ESEs in the governance process, and the assignment of responsibilities and liability following a cybersecurity incident. These comments show there is a general recognition of the need for appropriate cybersecurity protections, but significant questions remain regarding how those protections should be structured, how compliance should be demonstrated, and how requirements should be maintained over time.

4.2. Customer Understanding of Data Sharing

The Commission directed Staff to evaluate how customer understanding of energy-related data sharing has evolved since the adoption of the DAF. This consideration recognizes that customer participation is fundamental to achieving the objectives of the DAF, and customers cannot meaningfully exercise control over their energy-related data unless they understand what information may be shared, who may receive that information, the purpose for which it may be used, and the mechanisms available to authorize or revoke access. Customer understanding is essential to informed consent and effective participation in New York's energy marketplace.

As outlined in the Joint Utilities' Consent Process Assessment, the utilities have provided multiple mechanisms through which customers may authorize third-party access to energy-related data. These mechanisms include Green Button Connect, customer authorization forms processed directly by the utilities, Electronic Data Interchange processes supporting retail energy markets, retail access customer enrollment portals, demand response enrollment platforms, and pilot initiatives associated with the development of the Integrated Energy Data Resource. While these mechanisms collectively provide customers with numerous opportunities

to authorize data sharing, they differ significantly in presentation, terminology, customer interaction, and overall user experience.

In Staff's experience, customer familiarity with electronic authorization mechanisms has increased since the adoption of the DAF. The widespread use of online banking, digital healthcare portals, and customer-managed privacy settings across numerous industries has significantly changed customer expectations regarding access to, and control of, personal information. Customers increasingly expect online tools that clearly identify what information is being shared, for what purpose, with whom, and for how long. These evolving expectations support continued review of utility consent processes while maintaining accessibility for customers who prefer non-electronic communication methods.

Customer education has not been an ongoing component of the DAF, but rather only occurring during the initial authorization process. Consent forms focus on obtaining authorization for a specific data sharing transaction and are not designed to educate customers regarding broader data protections and privacy. Educational materials explaining the categories of energy-related data maintained by the utilities, and examples of how those data points may support innovative products and services, the cybersecurity protections in place for entities receiving customer information, and the customer's continuing ability to revoke previously granted consent, do not readily exist.

Staff also recognizes that customer understanding may vary depending upon the nature of the customer data requested. Requests involving aggregated or publicly available data have substantially different privacy considerations than requests involving customer-specific usage data, interval meter data, billing history, or personally identifiable information.

4.3. Risks Associated with Data Sharing

The Commission also directed Staff to evaluate the risks associated with customer energy-related data sharing. Although expanded access to energy-related data offers benefits to customers, utilities, and market participants, those benefits must be balanced against the risks associated with unauthorized disclosure, inappropriate use, cybersecurity incidents, and lack of customer confidence in the management of their data.

Since the adoption of the DAF, the cybersecurity landscape has continued to evolve. Public and private organizations have experienced increasingly sophisticated attacks,

supply chain threats, and other cybersecurity incidents targeting sensitive information. These threats reinforce the Commission's recognition that cybersecurity and privacy requirements must evolve. The Joint Utilities also recognized these changing risks in their petition to update the existing SA requirements and establish an ongoing governance process.

The current DSA/SA approach does not treat cybersecurity as a continuous risk management process but rather a one-time compliance obligation. The existing DSA/SA process relies upon entities requesting customer information to execute an agreement and attest to certain standardized requirements with each utility company from whom they are seeking customer data. While these requirements established an important baseline of requirements, actual implementation challenges demonstrate that the DSA and SA alone cannot ensure continued compliance with evolving cybersecurity expectations. Staff further recognizes that the risks associated with data sharing are not uniform across all types of energy-related data. The nature and sensitivity of the data, as well as the potential consequences of unauthorized access or disclosure, should therefore inform the applicable cybersecurity and privacy protections.

4.4. Customer Expectations Regarding Consent

The Commission has expressly recognized that customer energy-related data belongs to the customer and not the utility, and that customers have a right to direct or consent to the use of that data.[16] Informed customer consent has been and continues to be an essential principle of the Commission's data policy.

The DAF established nine SCRs designed to create a consistent statewide authorization process. These SCRs address, among other things, the availability of both web-based and non-web-based consent options, standardized consent language, provide customer revocation options, and authorization for additional purposes.[17] These SCRs continue to provide a baseline framework for obtaining customer consent. Nevertheless, implementation experience and developments in customer privacy law suggest that customer expectations have evolved, and that customers expect continued visibility into how their information is being used after initial consent has been provided.

---

[16] Minimum Cybersecurity Protections Order, p. 13.

[17] DAF Order, pp. 65-67.

Numerous industries, including banking and finance, social media, and healthcare, provide customers with routine notifications regarding account activity, access to personal information, changes in privacy settings, and opportunities to review or withdraw data sharing permissions. Customers expect to understand which organizations currently have access to their energy-related data, along with understanding the purposes for which the data is being used and how long that entity will have authorized access to their energy-related data.

4.5. Legislative and Regulatory Developments

Since the adoption of the Framework, legislative and regulatory actions regarding cybersecurity and consumer privacy have expanded at both the State and national levels. While many of these statutes and regulations apply to different industries or entities, they collectively provide broader policies that Staff finds relevant in evaluating energy-related data access. However, Staff does recognize that the applicability of these policies should be considered in the context of the specific types of data requested and the associated risks, rather than applied uniformly across all energy-related data points.

4.5.1. NIST

The NIST, an agency within the U.S. Department of Commerce, develops technical standards, guidelines, and frameworks addressing cybersecurity, privacy, and information security. NIST publications are frequently used as reference points for cybersecurity programs across public and private sectors because they provide structured standards for identifying and addressing cybersecurity risks. NIST guidance is commonly used within the utility and energy sectors as a source of cybersecurity best practices and technical controls. One NIST publication relevant to this discussion is the NIST Special Publication 800-63B.[18] The Joint Utilities proposed incorporating NIST 800-63B into the cybersecurity requirements applicable to ESEs, specifically in connection with role-based access controls, encryption, and authentication and password controls. However, NIST 800-63B has since been superseded by

[18] NIST, Special Publication 800-63B – Digital Identity Guidelines: Authentication and Lifecycle Management (June 2017), available at nist.gov.

NIST 800-63B-4.[19] The current NIST guidance should be considered when evaluating if any standard should be required and incorporated into DAF.

4.5.2. New York State Privacy and Cybersecurity Framework

New York has established a statutory framework governing data security and privacy that is directly relevant to utility customer data. The Stop Hacks and Improve Electronic Data Security (SHIELD) Act of 2019 requires entities that own or license private information of New York residents to implement reasonable safeguards to protect such data.[20] The SHIELD Act reflects New York's policy that entities collecting consumer data must be accountable for preventing unauthorized access, misuse, and disclosure. The SHIELD Act adopts a flexible, risk-based approach that recognizes cybersecurity obligations should reflect the size and complexity of the organization, the nature of its activities, and the sensitivity of the information.

Similarly, the New York State Department of Financial Services' cybersecurity regulations,[21] while applicable to covered financial institutions, establishes widely recognized best practices for governance, risk assessment, incident response, and accountability that Staff finds instructive for entities accessing utility customer data. These include documented cybersecurity programs, periodic risk assessments, written policies and procedures, and incident response planning. Staff believes these concepts provide useful guidance when considering modifications to DAF's requirements.

4.5.3. PSC Cybersecurity Proceeding

The Commission's cybersecurity requirements have also evolved since the adoption of the DAF. In 2025, the Commission instituted a proceeding to establish comprehensive cybersecurity requirements applicable to information technology systems of

---

[19] NIST, SP 800-63B-4 - Digital Identity Guidelines: Authentication and Authenticator Management (July 2025), available at nist.gov.

[20] See L. 2019, ch. 117.

[21] 23 NYCRR Part 500.

regulated utilities.[22] The Cyber Proceeding reflects the Commission's recognition that cybersecurity threats, technologies, and the systems used to maintain and exchange information continue to evolve. This proceeding is relevant to the modification of the DAF because utilities' information technology systems and cybersecurity obligations are directly related to the systems through which customer utility data is held and transmitted. The DAF should establish the cybersecurity and privacy requirements applicable to entities receiving customer utility data, while utility obligations established through the Commission's broader cybersecurity rules should continue to govern the utility's own systems.

4.5.4. Other Jurisdictions

In addition to developments in New York, Staff also considered comprehensive privacy regulations adopted in other jurisdictions, including the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA),[23] and the European Union's General Data Protection Regulation (GDPR).[24]

Although utilities in New York are not each directly subjects to these laws, they provide relevant standards for consumer data governance that Staff propose to incorporate into New York's modified Framework. Common principles across these regulations include purpose limitations, which limits data access to specific, disclosed purposes; data minimization, designed to narrow the data available to only what is necessary to fulfill the authorized purpose; transparency and consumer control, which requires consumers to have visibility into who is accessing their data and the ability to withdraw consent; accountability; and security safeguards. These principles provide useful context for the DAF.

4.6. Alignment with UBP Requirements

The Commission directed Staff to evaluate whether modifications to the UBPs are necessary to improve consistency between them and the DAF. The Framework established

---

[22] Case 25-M-0302, Proceeding on Motion of the Commission of the Rules and Regulations of the Public Service Commission, Contained in 16 NYCRR-Proposed Information Technology Cybersecurity Requirements (Cyber Proceeding).

[23] Information related to the CCPA and CPRA is available at https://oag.ca.gov/privacy/ccpa.

[24] Information related to the GDPR is available at https://gdpr-info.eu/.

statewide policies governing customer consent, cybersecurity, privacy, and access to customer utility data. However, certain related requirements continue to exist within the ESCO and DER Supplier UBPs, creating the potential for overlapping requirements, such as data point availability and requirements where the UBPs point to NIST standards, customer consent requirements, and annual notice requirements regarding privacy.

Statewide consistency is central to an effective Framework. Utilities, ESCOs, DERs, ESEs, and customers should be able to rely upon a single framework regarding access to customer utility data. Accordingly, as discussed in more detail below, Staff recommends that the DAF serve as the Commission's primary policy framework regarding access to customer utility data. Where the UBPs address customer data consent, access requirements, and annual privacy notices, Staff recommends revising those provisions to reference the DAF directly. This approach would maintain consistency between the DAF and the UBPs, while ensuring future modifications to the DAF automatically remain applicable across multiple Commission documents.

5. Preliminary Proposal

As discussed above, the Commission directed Staff to evaluate whether modifications to the Framework are necessary to ensure that New York State's data access requirements continue to support customer choice, facilitate useful access to energy-related data, and appropriately address cybersecurity and privacy risks. Staff's recommendations seek to maintain the central objectives of the DAF while strengthening protections and removing unnecessary administrative barriers to legitimate, customer-authorized data access. Based on the Commission's directives, filings submitted by the Joint Utilities, and Staff's experience administering the Framework, the recommendations below reflect Staff's preliminary assessment of potential revisions to the DSA and SA and are intended to provide a starting point for further stakeholder discussions. Through the initial stakeholder feedback and technical conference process, Staff will seek input from utilities, ESEs, consumer representatives, cybersecurity experts, and other interested parties regarding the effectiveness, practicality, and potential impacts of these preliminary recommendations. The process will also provide an opportunity for parties to identify implementation concerns, propose alternative language or approaches, and provide information regarding the cost, benefits, and feasibility of specific revisions.

Staff will consider the information and perspectives developed through the technical conference in preparing a more comprehensive Staff proposal. The comprehensive Staff Proposal will be issued for public comment before final Commission action. That proposal will further evaluate the issues discussed below and set forth more specific recommendations for revisions to the DSA and SA, including proposed requirements, implementation procedures, and timelines for Commission consideration.

5.1. Cyber Security and Privacy

The Commission's Minimum Protections Order, the SHIELD Act, and other regulatory frameworks such as the New York Department of Financial Services Cybersecurity Regulation and the GDPR, support cybersecurity protections that are risk-based and promote accountability and ongoing review.

The SHIELD Act requires covered entities to implement reasonable safeguards, including risk assessments, workforce training, incident response planning, and vendor oversight, as appropriate to the size and complexity of the entity and the nature of the data. Similarly, the New York Department of Financial Services Cybersecurity Regulation requires covered entities to maintain a cybersecurity program, adopt written policies, conduct periodic risk assessments, and implement incident response and reporting mechanisms. These provisions provide a useful pathway for risk-based cybersecurity governance that, if applied to the DAF, could better define expectations, improve implementation, clarify responsibilities, and facilitate consistent administration of customer-authorized data sharing.

Throughout the administration of the DAF, Staff has observed implementation challenges associated with the DSA process. Utilities, ESEs, and Staff have gained practical experience and identified areas where additional clarity or modification may improve implementation. For example, utilities have identified challenges associated with evaluating whether prospective or existing ESEs maintain compliance with cybersecurity standards and adequately protect customer utility information. Although the DSA establishes contractual obligations between data custodians (which includes the utilities) and ESEs, utilities have indicated that assessing compliance can be difficult in practice. Similarly, utilities have identified issues regarding the appropriate roles and responsibilities following a cybersecurity incident that

affects customer information, including which entity should be responsible for the cost and implementation of incident reporting and coordination.

Considering those concerns, Staff recommends retaining the DSA/SA process, with revisions. As a general matter, the DSA should continue to be utilized as the primary agreement that establishes the responsibilities of the data custodian and the ESE. Similarly, Staff recommends that the SA continue to be used to identify the cybersecurity and privacy protections ESEs must have in place in order to access customer data. This approach maintains a familiar process that is already being used, while allowing the Commission to make it clearer and more consistent.

Staff recommends modifying the individual requirements in the SA relating to access controls and authentication, endpoint protection, encryption, personnel screening, data inventory, network safeguards, and physical access, as follows.

- SA Item 3 should be revised to require user identification and periodic review of access rights.
- SA Item 4's requirement for multi-factor authentication for remote administrative access should be retained and extended to systems that store or process Confidential Customer Utility Information. The SA should identify the particular Commission-approved authentication baseline that applies, rather than requiring an ESE to determine generally what it means to align with NIST 800-63B.
- Staff recommends retaining the existing patching requirement within Item 5, including prompt treatment of critical vulnerabilities, but allowing an ESE to document an equivalent control when immediate installation would create an operational or security risk. Staff recommends adopting the Joint Utilities' proposal to replace the narrower antivirus requirement within SA Item 6 with endpoint protection on servers and workstations that store, process, or access Confidential Customer Utility Information. The control should require protection to be actively maintained and updated.
- Regarding SA Item 7, Staff recommends that SA require Confidential Customer Utility Information to be encrypted in transit and at rest, and to remove the exemption for email communications. An email containing

Confidential Customer Utility Information should be encrypted or replaced by a secure portal or other protected delivery method. Staff does not recommend revising this SA item to include a general reference to NIST cryptographic standards and guidelines, as proposed by the Joint Utilities, but instead recommend the revised SA should specify the minimum standards required for encryption.

- Staff recommends modifying SA Item 13 to require role-appropriate background screenings before a person receives access to Confidential Customer Utility Information, rather than mandating the same criminal history check for every employee as proposed by the Joint Utilities.
- The revised SA should adopt the Joint Utilities' proposed 24-hour limit in SA Item 15 for revoking access when access is no longer required or employment ends, while requiring immediate revocation when a termination or other circumstances presents a known security risk.

Staff further recommends modifying various sections in the statewide DSA relating to utility discretion regarding ESE compliance, statewide acceptance with utility-specific technical testing, third-party responsibility, security incidents, and responsibility and indemnification, as follows.

- Staff recommends revising the DSA to limit individual utility discretion within Section 13(c) related to the acceptance of an ESE's attestation, and instead measure an ESE's compliance against Commission-approved requirements.
- Section 5 of the DSA should be modified to require the execution of the Commission-approved SA, and remove language allowing each utility to impose "such other risk assessment forms" or determine, in its sole discretion, whether an ESE's general security program is acceptable. That notwithstanding, a utility should retain authority to request information reasonably necessary to investigate a specific incident, identified deficiency, or risk to its system.
- Staff submits that an executed DSA and completed SA should satisfy the general cybersecurity review statewide, and should not have to be re-approved

by every utility. Each utility may still perform the technical onboarding and connection testing that is necessary, but Staff recommends that a utility-specific test cannot add a new cybersecurity control outside of Commission-approved requirements.

- Staff further recommends that the DSA retain rules assigning responsibility to an ESE for third-party representatives that store, transmit, or process customer information on the ESE's behalf. A third-party representative without a direct utility connection should not be required to execute a separate DSA with every utility, but the ESE must remain accountable for the third party's actions.
- Regarding Data Security Incidents under Section 11, Staff recommends retaining the 48-hour limit for notice of a potential security incident. Section 11 of the DSA should allow for immediate temporary suspension of data transfers when the data custodian has a reasonable basis to believe that continued access presents an ongoing material risk to customer data and information. Where such a temporary suspension is warranted, the utility should promptly provide written notice to the ESE stating the reasons for the suspension and the conditions for reinstatement and should restore access when the ESE demonstrates compliance with those security requirements. Disputes should be subject to the applicable UBP or UBP-DERS process, with expedited Staff review available after the immediate risk has been contained.

This preliminary recommended approach acknowledges the Joint Utilities' position that the controls should be updated, while addressing parties' concerns regarding vague standards, utility discretion, cost, due process, and the absence of ESE participation. It does not replace the DSA/SA, but instead it establishes clear minimum controls for ESEs, allows equivalent methods of compliance where appropriate, and requires additional process only when the data, access method, or circumstances present a higher risk.

Staff welcomes stakeholder feedback on the proposed revisions to the DSA/SA process, as well as feedback on potential changes to substance of the DSA and SA themselves.

5.2. Data Ready Certification and the Data Access Matrix

As discussed above, the Commission established the Data Ready Certification process as a means of facilitating standardized customer-authorized access to customer utility information while ensuring ESEs satisfied the requirements established under the DAF. The DRC process was intended to replace existing DSA/SA processes and provide a consistent mechanism for evaluating eligibility for access to customer utility information.

The Joint Utilities' DAIP outlined the size and complexity of the process that was envisioned. The filing proposed a third-party provider, a centralized application and website, new legal agreements, procurement and contracting, cybersecurity verification, recertification, monitoring, reporting, incident management, and the transition of existing ESEs. The Joint Utilities estimated that full implementation would take approximately 17 months after approval of the DAIP.[25] The filing also explained that the existing utility process for receiving and reviewing the DSA and SA requires limited utility resources and identified no cost savings that could be used to support the new DRC process. Instead, the Joint Utilities proposed allocating the new costs among utilities and recovering those costs through existing rate mechanisms.[26]

Staff recommends that the Commission eliminate the Data Ready Certification process and the Data Access Matrix from the DAF. Staff does not find meaningful reasons at this time why creating a process with a third-party certification provider and centralized platform is necessary to achieve the Commission's objectives. The revised DSA and SA process should remain in place, with revisions, and should be used to establish requirements and confirm that an ESE meets them. Instead, Staff recommends improving the lower-cost process that is already in place rather than create an additional certification system and platform. A single statewide DSA and SA process can provide consistent requirements, account for different levels of risk, and reduce repeated reviews for ESEs seeking data from more than one utility.

The Matrix was intended to help the DRC Provider determine which requirements applied to the request. If DRC is eliminated, a separate Matrix is not needed. The revised DSA and SA, and its instructions, can identify the protections that apply to all ESEs, explain when

---

[25] DAIP, p. 16.

[26] DAIP, p. 27.

additional protections apply, and provide examples. Keeping this information in the DSA and SA will make the process easier to understand and reduce the risk of conflicting requirements.

The technical conference process should focus on how the revised DSA and SA process will work statewide, including how an accepted agreement will be recognized, what utility-specific technical review may still be necessary, how often an ESE must renew or update its agreement, and how the transition should occur.

5.3. Ongoing Review and Data Point Availability

Staff preliminarily recommends establishing a DAF Committee, supported by a Data Access Advisory Working Group, similarly to what was proposed by the Joint Utilities in their Petition to Modify. Specifically, the Joint Utilities proposed a committee made up of utility and Staff representatives, with ESEs and other stakeholders participating through the separate Advisory Working Group. Comments on that proposal raised reasonable concerns regarding ESE representation and the ability of some parties to participate meaningfully in the development of requirements that would apply to them.

Staff recommends ESEs and other stakeholders have input regarding any requirements through representative participation in an Advisory Working Group. This Advisory Working Group would bring recommendations to the DAF Committee of Staff and the utilities, who would then create proposals for modifications or enhancements to DAF for Commission consideration. Those proposals would be publicly filed for consideration following a standard public notice and comment period.

The main role of the DAF Committee, which Staff recommends being composed of utility and Staff members with relevant cybersecurity or privacy experience, should be to identify emerging issues, review experience under DAF, and develop, for Commission consideration, recommendations based on feedback from the Advisory Group. Conversely, the DAF Committee should not have the authority to modify any requirements, suspend an ESE's access, or otherwise establish new requirements without Commission approval.

Staff recommends that the Advisory Working Group initially prioritize a review of data point availability. The Advisory Working Group could create a statewide data dictionary and a set of commonly recognized use cases for DAF Committee review and Commission

consideration. The data dictionary should provide consistent definitions and identify meaningful differences in utility availability.

In addition, Staff recommends a limited governmental entity exemption similar to the approach proposed by the City of New York in its comments on the DAF Matrix.[27] Specifically, a State or local governmental entity requesting data to carry out a statutory, regulatory, planning, benchmarking, energy-management, research, or other public functions should not be required to satisfy all DAF requirements. For the avoidance of doubt, the exemption should not remove the obligation to protect customer-specific data. Governmental entities should remain subject to appropriate cybersecurity, privacy, confidentiality, use, retention, and incident-reporting requirements, but should be permitted to demonstrate compliance through applicable governmental policies or standards.

Through the technical conference process, Staff seeks stakeholder input on the DAF Committee and Advisory Working Group's membership and procedures, the information that should be included in the statewide data dictionary, the initial use cases that should be prioritized, the treatment of aggregated and anonymized data, and the scope of the governmental entity exemption.

5.4. Customer Consent and Education

As discussed above, customer authorization serves as the foundation of the Framework. The Commission has consistently recognized that customer information should be shared only with appropriate authorization from the customer, and for legitimate customer-directed purposes. The Commission has reiterated that customer trust is foundational to effective data access. Since adoption of DAF, however, consumer expectations regarding data sharing, privacy, transparency, and control over their information have evolved. Recent changes to New York law further emphasize transparency and accountability in data handling practices. The SHIELD Act requires entities to safeguard private information and recognizes that consumer authorization must be supported by appropriate controls. Similarly, privacy regulations adopted in other jurisdictions reinforce the principles that are directly relevant to utility customer data.

---

[27] Case 20-M-0082, supra, City of New York Comments on Data Access Matrix (filed August 20, 2021) p. 3.

The CPRA requires that, in California, personal information be collected and used only for specified, explicit purposes disclosed to the consumer. The CPRA further limits use of personal information to purposes consistent with consumer expectations and grants consumers the right to withdraw consent for certain data uses. The European Union's GDPR similarly recognizes that consent should be freely given, specific, informed, and revocable, and personal data should be processed only for specific purposes.

The Joint Utilities' Consent Process Assessment outlines that consent is currently obtained through several different systems and processes. The Consent Process Assessment also identifies differences in the information presented, the methods available to customers, and the extent to which utilities can evaluate consent obtained directly by third parties.

Staff recommends that the Commission require common consent information across data custodians and across access methods. At a minimum, every consent process should clearly identify the categories of data being shared, the purpose of the request, the duration and frequency of access, whether the data may be provided to another party, and the method for revoking consent. Customers should receive confirmation of their authorization and be provided an easy way to review and revoke ongoing access. Staff also recommends retaining the requirement that customers be provided an annual notice that serves as a reminder to customers which entities have access to their data, the purpose and types of data involved, and how to revoke permission. Staff further recommends that data custodians provide customers with a clear view of active authorizations through their existing customer account tools where practicable, while continuing to offer non-electronic options.

The Joint Utilities' Consent Process Assessment and Customer Consent Engagement Plan proposed recurring outreach through email, newsletters, bill messages, and social media. Staff recommends common statewide outreach and education explaining the types of energy data that may be shared, examples of how that data may be used, the protections that apply, how customers can determine whether an entity is authorized, and how customers can review or revoke access.

The technical conference should be used to develop common consent language and process and develop a statewide customer consent Outreach and Education Plan.

6. Stakeholder Engagement

Staff's recommendations in this Preliminary Proposal are intended to establish the policy direction for modifications to the DAF. Staff recognizes, however, that several recommendations require additional technical and operational details before the Commission issues final Framework modifications. Staff therefore will convene a technical conference following the filing of comments to this Preliminary Proposal to gather technical and operational information before proposing additional, specific revisions to DAF requirements. The purpose of the technical conference should be to develop the record concerning implementation of the recommendations proposed by Staff, identify technical or operational issues that may affect implementation, evaluate potential unintended consequences, and identify appropriate refinements to proposed requirements.

Staff recommends that parties be prepared to provide specific information, including existing practices, technical limitations, implementation costs, potential alternatives, and examples demonstrating how proposed requirements would affect access to customer utility data.

7. Conclusion

The Commission established the Data Access Framework to facilitate secure, customer-authorized access to utility customer information while protecting customer privacy and supporting the development of renewable energy products and services, competitive energy markets, and innovation within the utility sector. Since the Framework was adopted, advancements in technology, changes in customer understanding and expectations, evolving cybersecurity risks, and experience gained through implementation have demonstrated opportunities to improve certain provisions. The updates proposed and future modifications that will be determined through the proposed and technical conference, which will be followed by a more comprehensive Staff Proposal to be issued for formal public comment, will help the Commission in strengthening consumer protections over their own utility data, enhance customer control over their data use, and ensure consistent statewide treatment.