Mary Krayeske
Assistant General Counsel
Law Department

May 3, 2022

Hon. Michelle Phillips
Secretary
New York State Public
Service Commission
Three Empire State Plaza
Albany, NY 12223

Re: Cases 20-M-0082 and 18-M-0376

Joint Utility Petition to Modify Self Attestation

Dear Secretary Phillips:

The Joint Utilities[1] hereby file the attached document, Joint Utilities Petition to Modify the Data Security Agreement Self-Attestation Requirements and Implement a Governance Review Process for Regular Self Attestation Updates.

Please feel free to reach out if you have any questions.

Sincerely,

/s/ Mary Krayeske

Mary Krayeske

Attachment

[1] The Joint Utilities are Central Hudson Gas and Electric Corporation (Central Hudson), Consolidated Edison Company of New York, Inc., National Fuel Gas Distribution Corporation, New York State Electric & Gas Corporation, Niagara Mohawk Power Corporation d/b/a National Grid, KeySpan Gas East Corporation d/b/a National Grid and The Brooklyn Union Gas Company d/b/a National Grid NY, Orange and Rockland Utilities, Inc., and Rochester Gas and Electric Corporation.

Consolidated Edison Company of New York, Inc.
4 Irving Place 18th Floor New York NY 10003 212 460 1340 212 677 5850 fax krayeskem@coned.com

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

Proceeding on Motion of the Commission Regarding Strategic Use of Energy Related Data	))	Case 20-M-0082
Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place	)))	Case 18-M-0376

JOINT UTILITIES' PETITION TO MODIFY THE DATA SECURITY AGREEMENT SELF-ATTESTATION REQUIREMENTS AND IMPLEMENT A GOVERNANCE REVIEW PROCESS FOR REGULAR SELF-ATTESTATION UPDATES

To assure that energy service entities (ESEs)[1] seeking access to customer and system data continue to maintain updated cyber security protections, the Joint Utilities[2] petition the New York State Public Service Commission (Commission) for modifications to the Commission's October 17, 2019 *Order Establishing Minimum Cyber Security and Privacy Protections and Making Other Findings*[3] that will result in:

- Six updated and three new requirements in the current Self Attestation (SA) of the Commission-approved Data Security Agreement (DSA) that reflect evolving cybersecurity and privacy needs; and
- A governance process for regular SA review and to provide recommendations for further SA updates.

[1] Energy service entities (ESEs) refer to energy service companies (ESCOs), distributed energy resources (DERs) suppliers, direct customers, governmental agencies, and other entities as defined in the Data Security Agreement (DSA).

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

[3] Cases 18-M-0376 *et al*., *Proceeding on the Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place* (Cyber Security Proceeding), Order Establishing Minimum Cyber Security and Privacy Protections and Making Other Findings (issued October 17, 2019) (Minimum Protections Order).

The proposed modifications are the necessary next steps in the evolution of the Commission's data sharing and cybersecurity requirements. To provide adequate cybersecurity for ESEs and appropriate protection for customer and system data, the SA requirements, first established in 2019 in the *Minimum Protections Order*, must keep pace with best practices, technology, and industry requirements. This requires regular updates of the SA controls through a structured process with participation from the Joint Utilities, Department of Public Service Staff (Staff) and stakeholders. Keeping the SA up-to-date is especially important as the New York State Energy Research and Development Authority (NYSERDA) works toward implementing the Integrated Energy Data Resource (IEDR) platform and the Commission considers the Joint Utilities' Data Access Implementation Plan (DAIP), which includes a Data Ready Certification process.[4] Given these considerations, the Joint Utilities request that the Commission move expeditiously to address this petition no later than September 15, 2022.

I. BACKGROUND

The Joint Utilities face an ever-increasing risk of cyber attack and have a continuing obligation to maintain and improve cyber defenses. Recent global events, including the ongoing war in the Ukraine, have heightened cybersecurity concerns and government warnings for the energy sector and other critical infrastructure across the United States. This, in turn, requires utilities to examine their security posture and asses potential cyber resilience risks. Utilities have particular concerns with third-party electronic interconnections where there is limited control over

[4] Case 20-M-0082, *Proceeding on Motion of the Commission Regarding Strategic Use of Energy Related Data* (IEDR Proceeding), Joint Utilities' Data Access Implementation Plan (filed September 20, 2021).

the third party's cyber security practices. Prior incidents with such entities prompted risk assessments and requests for controls on third party ESEs, including use of the DSA and SA.[5]

The Commission has long protected customer data and required that ESEs maintain adequate cyber security to protect customer data and secure business processes. In 2010, the Commission found that "[p]rotection of consumer information is a basic tenet of the Public Service Law and our policies."[6] The Commission approved a contract between Central Hudson and its vendor, OPower, in part, because the agreement included "privacy safeguards," which prohibited OPower from using customer information and usage data for any purpose other than to administer the program.[7] The Commission also noted with approval that the agreements included cyber security standards, specifically, voluntary standards issued by the United States Department of Commerce National Institute of Standards and Technology (NIST).[8]

In its REV Proceeding in 2015, the Commission re-emphasized the need for cyber security, finding that "[c]yber security is highly important for reasons of privacy, reliability, resiliency and market confidence."[9] The Commission also noted that technology is evolving and as a result, the area will require constant vigilance.[10] Similarly, in its *Order Adopting Distribution System*

[5] There are many recent examples of third parties causing cybersecurity issues for companies using their services. The practice of imposing requirements on third parties has been increasing and is being adopted by many entities, utility and other industry alike. Entities want to understand how third parties protect their systems and information in order to have some assurance that the third parties' actions are adequate. As this process matures, there is an ongoing effort toward industry-wide assessments.
[6] Cases 07-M-0548 *et al*., *Proceeding on Motion of the Commission Regarding and Energy Efficiency Portfolio Standards*, Order on Rehearing Granting Petition (issued December 3, 2010) (OPower Order), p. 17.
[7] *Id*., pp. 17-18.
[8] *Id*., p. 14.
[9] Case 14-M-0101, *Proceeding on Motion of the Commission in Regard to Reforming the Energy Vision* (REV Proceeding), Order Adopting Regulatory Policy Framework and Implementation Plan (issued February 26, 2015), p. 99 (citing Cyber Attacks Likely to Increase, Rainie, Lee; Anderson, Janna; and Connolly, Jennifer; Pew Research Internet Project, October 29, 2014).
[10] *Id*., p. 100.

Implementation Plan Guidance, the Commission stressed the importance of cyber security,[11] and regarding interconnections between utilities and DERs decided that "[a]long with identification of new system tools, rules must be put in place *incorporating cybersecurity and privacy protection*."[12]

In instituting its Cyber Security Proceeding in 2018,[13] the Commission recognized that cyber security threats are becoming more common and that industry must be vigilant in the wake of a cyber incident impacting a third-party vendor working for an ESCO in the retail access market. The third-party vendor's actions on behalf of ESCOs created a potential vulnerability and highlighted the need for more robust cyber security protections involving ESEs. The Commission stressed that "[i]t is essential to ensure that cyber security protections are being adequately addressed to mitigate the vulnerability of utility systems to cyber-attacks, and to ensure that confidential and sensitive customer information remains safeguarded from potential data breaches."[14]

Thus, in the *Minimum Protections Order* issued in the Cyber Security Proceeding, the Commission approved the DSA, including the controls in the SA, noting that "this current approach will provide a universal foundation of cyber security and data privacy requirements, while the Commission will continue to develop such requirements and may modify or expand upon them in the future, as appropriate."[15] In fact, the Commission identified its ongoing focus on current cyber security protections to strike an "appropriate balance" between "data privacy and

[11] REV Proceeding, Order Adopting Distributed System Implementation Plan Guidance (issued April 20, 2016), pp. 2-3.
[12] *Id*., p. 14 (emphasis added).
[13] Cyber Security Proceeding, Order Instituting Proceeding (issued June 14, 2018).
[14] *Id*., p. 3.
[15] Cyber Security Proceeding, Minimum Protections Order, p. 2

promoting consented data access."[16] The Commission expressly acknowledged the need to revisit and potentially modify or expand upon the minimum security standards at a later time.

The Commission also further addressed the use of frameworks or standards in the *Minimum Protections Order*. Under "Data Protection Requirements," the Commission-approved DSA requires entities to comply with national, state and local laws and requirements, as well as "industry best practices or frameworks to secure information, computer systems, network, and devices using a defense-in-depth approach, such as and including, but not limited to NIST SP 800-53, ISO 27001/27002 … as best industry practices and frameworks evolve over time."[17] While declining to prescribe an explicit framework or standard, the Commission expressly reserved possible "adoption of a more prescriptive standard at a future date."[18] The Commission noted that "the flexibility afforded by the DSA will allow ESEs to observe cyber security standards that are most appropriate for their businesses. The *bare minimum* standards that must be followed are found in the Self Attestation … Otherwise, ESEs should adopt data protection requirements that go beyond those in the Self Attestation as appropriate."[19]

Next, in its *Data Access Framework Order*,[20] the Commission continued to address the need for cyber security and privacy requirements, and ordered that a single entity, a Data Ready Certification (DRC) Provider, manage the approval process for ESEs obtaining access to utility customer data. Moreover, once the Data Ready Certification process is implemented, the Commission will require that the ESE verify, via audit, that it has the mandated cyber controls in

[16] *Id.*, p. 3.
[17] Cyber Security Proceeding, Joint Utilities DSA Filing (filed January 8, 2020), DSA, p. 2.
[18] Cyber Security Proceeding, Minimum Protections Order, p. 49.
[19] *Id.*, p. 49 (emphasis added).
[20] IEDR Proceeding, Order Adopting a Data Access Framework and Establishing Further Process (Data Access Framework Order) (issued April 15, 2021).

place.[21] Finally, the Commission established a Staff-driven process to work with utilities (and stakeholders) to "ensure the proper data access requirements are in place."[22] The Commission directed Staff to "continuously review the appropriate application of existing requirements" and "propose developments to the application of the Framework for Commission consideration, as necessary."[23]

Thereafter, Staff issued its Cyber Matrix – a compilation of the existing Commission-mandated cyber security requirements for ESEs.[24] In their comments on the Cyber Matrix, the Joint Utilities recommended a governance process to update the matrix requirements as well as a data inventory requirement.[25]

In short, the Commission has repeatedly emphasized the importance of adequate cyber security protections and controls. This Petition seeks to update those controls first included in the Minimum Requirements Order to align with best practices.

II. DISCUSSION

The Commission has long recognized the importance of current and effective cybersecurity for utility customer and system data. In furtherance of the Joint Utilities' efforts to update and enhance cyber protections for ESEs with existing and future access to utility data, the Joint Utilities propose updating the SA to reflect current minimum protections and best practices. Additionally, to provide assurance that the SA remains current and up to date, the Joint Utilities propose a

[21] *Id*., p. 16. This requirement was upheld by the Commission on rehearing. *See* IEDR Proceeding, Order Denying Rehearing, Providing Clarification, and Confirming Tariff Modifications (issued November 18, 2021), pp. 8-10.
[22] IEDR Proceeding, Data Access Framework Order, p. 60.
[23] *Id*.
[24] The Commission required Staff to issue this Matrix. *See* IEDR Proceeding, Data Access Framework Order, pp. 36-38.
[25] *See* IEDR Proceeding, Joint Utilities' Comments on Data Access Framework Matrix (filed August 9, 2021), pp. 5-6. The Joint Utilities' Data Access Implementation Plan (DAIP) made similar recommendations. *See* IEDR Proceeding, Joint Utilities' Data Access Implementation Plan (filed September 20, 2021), pp. 13-14.

Governance Process[26] for regular review of the SA terms. In this Governance Process, the Joint Utilities urge the Commission to approve proposed updates in a timely fashion so that ESEs have appropriate controls when the DRC process is implemented. The proposed SA changes will update the existing requirements and provide a new minimum level of controls to assist utilities and ESEs.

Once updated, the Governance Process will establish a path forward for subsequent SA changes to ensure the SA remains current and adequately protective.[27]

a. Self-Attestation Changes

The existing SA has fifteen (15) requirements. The proposed updated SA, attached as Appendix A, would modify and update six (6) of the existing requirements and add three (3) new requirements.[28] Generally, these updates apply the longstanding, industry-accepted voluntary standard frameworks issued by NIST. The proposed updates reflect reasonable cyber hygiene practices and are considered minimum best practice requirements in 2022.[29] These universally accepted standards form the basis for several regulations, including, for example, the Transportation Security Agency's (TSA) recent Security Directives[30] and the Department of

[26] In addition to proposing updates to the SA, the Governance Committee would address revocation standards for addressing ESEs that have cyber incidents or choose not to meet the SA requirements as well as auditing the DRC provider. These items are needed to first address circumstances when ESEs should stop receiving information due to an event (something that would have been automatically addressed by utilities previously) and second, to ensure that the DRC provider is appropriately handling this information.

[27] The Data Access Framework Order notes that there would be a Staff driven process for updating controls after the DRC is implemented. Given that the timeline for this is unclear, having a process in place for the interim period will assist with changes. After the DRC is implemented, the Commission can reconsider if the then in place process is sufficient.

[28] This list does not contain the Commission-mandated audit requirement at this time as the DRC is not yet operational.

[29] As noted in the past, the Joint Utilities expect significantly more from their vendors. In fact, the utility industry is standardizing a vendor questionnaire, https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

[30] Available at: https://context-cdn.washingtonpost.com/notes/prod/default/documents/253b5b73-b5ce-4a8e-a9c2-a3e314ac65df/note/e8f64f8a-e82c-4850-b19c-d5cdf4d301d9

Defense (DoD) Cyber Maturity Model Certification (CMMC) process.[31] The NIST framework continues to mature as cyber security practices evolve. Using controls based on NIST frameworks allows entities to use varying methods for meeting the standards, while maintaining consistency in their requirements.

The proposed modifications, noted in Appendix A, follow (changes highlighted in bold):

- Item # 3 – Role-based access controls – Reflect an additional requirement that **Authentication and password controls align with NIST Special Publications 800-63B: Digital Identity Guidelines**.
  As an example, the TSA's recent Security Directive 2 requires this NIST control for gas operators.[32]
- Item # 6 – Anti-virus Software –Require **installation of Endpoint protection software on all servers and workstations and maintenance of same with up-to-date signatures**.
  This change reflects that Endpoint protection, which includes anti-virus software, is now the recommended technology for handling virus protection.
- Item # 7 – Encryption in Transit – Reflect expected encryption in transit requirements under NIST and **encrypt** all Confidential Customer and Non-Public Utility Information in transit using encryption methods **compliant with NIST cryptographic standards and guidelines**.
  This change removes the exemption for emails and moves from industry best practice to NIST.
- Item # 8 – Encryption at Rest –Reflect expected encryption at rest requirements under NIST and **encrypt** all Confidential Customer and Non-Public Utility Information at rest using encryption methods **compliant with NIST cryptographic standards and guidelines,** or is otherwise physically secured.
  This change moves allows entities to meet both current industry best practices and NIST.
- Item # 13 – Employee Background Screening –Include a criminal background check for employees with access to confidential information, employee background screening, **including criminal background checks**, occurs prior to the granting of access to Confidential Customer Utility Information.
  In line with applicable legal requirements, employees handling confidential information must clear a criminal background check given the sensitivity of this information
- Item # 15 – Revoking Access to Information – Include a 24 hour access revocation when access to this information is no longer required. Access to Confidential Customer Utility

[31] CMMC is a certification process that has been adopted by DoD and is expected to go into effect in 2025. Other federal agencies and departments are expected to use this model as well. CMMC requires certain controls to be in place depending on the level of classified information an entity possesses.

[32] Available at: https://context-cdn.washingtonpost.com/notes/prod/default/documents/253b5b73-b5ce-4a8e-a9c2-a3e314ac65df/note/e8f64f8a-e82c-4850-b19c-d5cdf4d301d9

Information is revoked **within 24 hours** when no longer required, or if employees separate from the ESE or Third Party Representative.
This requirement aligns with North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)[33] standards.

Each of the Joint Utilities currently meet these updated SA requirements. ESEs should also meet these requirements.

A description of the proposed additions, also noted in Appendix A, follows (highlighted in bold):

- Item # 16 – **Inventory – Developing and maintaining a data inventory that an ESE can use to catalog its data and location.**
  Entities must have an adequate understanding of the data they possess to ensure that it is appropriately protected. A data inventory will assist entities in understanding where their sensitive data is located and is foundational to the cybersecurity life cycle management process.[34]
- Item # 17 – **Communications – Organization communications (*i.e.*, information transmitted or received by organizational systems) are monitored, controlled and protected at the external boundaries and key internal boundaries of the information systems. Sub-networks for publicly accessible system components are physically or logically separated from internal networks. Management of devices use encrypted sessions.**
  These are part of NIST and other standards, including those required by the International Organization for Standardization (ISO), and represent minimum standards in 2022. The Joint Utilities meet these requirements.
- Item # 18 – **Physical Access – Physical access to organizational information systems, equipment, and the respective operating environments is limited to authorized individuals. Physical security controls include the following:**
  - **Visitors are escorted and their activity is monitored**
  - **Audit logs of physical access are maintained**
  - **Physical access devices are controlled and managed**

  Entities having access to confidential information should maintain appropriate physical security measures. The Joint Utilities have such controls.

[33] CIP Standards (nerc.com)
[34] The Joint Utilities requested this addition in the Cyber Matrix comments and the DAIP. This item is a work in progress for the Joint Utilities, as it is for many entities. *See supra* note 25.

The Joint Utilities urge the Commission to approve these SA updates and additions so that ESEs obtaining utility data meet appropriate industry standards and best practices. These items will also incentivize ESEs to continue to improve cyber protections.

b. Governance Committee

The Joint Utilities propose that the Commission establish a Governance Committee. A process and Governance Committee would provide a forum for regular reviews and updates of the SA. The Governance Committee could also be empowered to address other issues related to the DRC process. The charter for the proposed Governance Committee is included as Attachment B.

Among other things, the Governance Committee would:

- Consist of up to five Joint Utilities members and up to five Staff members, all of whom are cyber security subject matter experts
- Meet at least quarterly
- Establish an Advisory Working group, including, at a minimum, ESEs and NYSERDA, who would provide the Governance Committee with suggestions and recommendations as well as provide feedback on proposed recommendations for further updates to the SA
- Consider the current threat landscape, existing regulatory and legislative framework, and identify risks and potential gaps in the current protections
- Recommend changes to the SA to the Commission, as needed
- Participate and engage with stakeholder forums

As noted earlier, based on the Data Access Framework Order, this Governance Committee would remain in place until the DRC is in place, at which point Staff is expected to take over this process. At this time, the Joint Utilities recommend that consideration be given to continuing the involvement of the Governance Committee to support Staff and stakeholders as appropriate.

III. CONCLUSION

As explained herein, the Commission has recognized the importance of protecting utility systems. The Commission has also acknowledged the obligation of ESEs to protect their

systems, and the role this plays in protecting utility systems. The Joint Utilities' proposed SA updates will bring the legacy SA in line with current standards and the proposed governance process will provide a means for future updates to the SA as necessary to respond to emerging trends, technology, and cyber threats. Given the expected approval for the Data Access Implementation Plan, the Joint Utilities respectfully request that the Commission act on this petition no later than the September 15, 2022 Open Session, either in conjunction with an order on the DAIP or before an order on the DAIP is issued. Approving the proposed modifications in this petition will provide assurance that up-to-date controls are in place prior to implementation of the DRC process.

Dated: May 3, 2022

Respectfully submitted,

CENTRAL HUDSON GAS AND ELECTRIC CORPORATION

By: */s/ Paul A. Colbert*

Paul A. Colbert
Associate General Counsel – Regulatory Affairs
Central Hudson Gas and Electric Corporation
284 South Avenue
Poughkeepsie, NY 12601
Tel: (845) 486-5831
Email: pcolbert@cenhud.com

CONSOLIDATED EDISON COMPANY OF NEW YORK, INC. and ORANGE AND ROCKLAND UTILITIES, INC.

By: */s/ Mary Krayeske*

Mary Krayeske
Assistant General Counsel
Consolidated Edison Company of New York, Inc.
4 Irving Place
New York, New York 10003
Tel.: (212) 460-1340
Email: krayeskem@coned.com

NIAGARA MOHAWK POWER CORPORATION d/b/a NATIONAL GRID, KEYSPAN GAS EAST CORPORATION d/b/a NATIONAL GRID, and THE BROOKLYN UNION GAS COMPANY d/b/a NATIONAL GRID NY

By: */s/ Jeremy J. Euto*

Jeremy J. Euto
Assistant General Counsel
National Grid
300 Erie Boulevard
West Syracuse, New York 13202
Tel: (315) 428-3310
Email: Jeremy.euto@nationalgrid.com

NEW YORK STATE ELECTRIC & GAS CORPORATION and ROCHESTER GAS AND ELECTRIC CORPORATION

By: */s/ Amy A. Davis*

Amy A. Davis
Senior Regulatory Counsel
89 East Avenue
Rochester, NY 14649
Tel.: (585) 771-4234
Email: amy.davis@avangrid.com

NATIONAL FUEL GAS DISTRIBUTION CORPORATION

By: */s/ Jeffrey B. Same*

Jeffrey B. Same
Senior Attorney
6363 Main Street
Williamsville, NY 14221
Tel.: (716) 857-7507
Email: samej@natfuel.com

APPENDIX A

Enhanced Cybersecurity Protections

Cybersecurity experts for the Joint Utilities propose to enhance and modernize the existing minimum protections established in the 2018 Data Security Agreement (DSA) and Self Attestation (SA). The Joint Utilities believe this proposal is particularly timely given the Commission's expectation to begin implementation of the Data Access Framework (DAF) and Data Ready Certification (DRC) process in 2022. The following table includes an updated list of 18 cybersecurity protections: nine from the existing DSA/SA; six with proposed modifications; and three new protections, one from the Joint Utilities' DAF Matrix comments and two from the attached petition.

Cyber Protection	Original Language (DSA/SA)	Propose Addition/Change
1	An Information Security Policy is implemented across the ESE's corporation which includes officer level approval.	None
2	An Incident Response Procedure is implemented that includes notification within 48 hours of knowledge of a potential incident alerting utility when Confidential Customer Utility Information is potentially exposed, or of any other potential security breach.	None
3	Role-based access controls are used to restrict system access to authorized users and limited on a need-to-know basis.	Role-based access controls are used to restrict system access to authorized users and limited on a need-to-know basis. Authentication and password controls align with NIST 800-63B: Digital Identity Guidelines.
4	Multi-Factor Authentication is used for all remote administrative access, including, but not limited to, access to production environments.	None
5	All production systems are properly maintained and updated to include security patches on a periodic basis. Where a critical alert is raised, time is of the essence, and patches will be applied as soon as practicable.	None
6	Antivirus software is installed on all servers and workstations and is maintained with up-to-date signatures.	Require installation of endpoint protection software on all servers and workstations and maintenance of same with up-to-date signatures.
7	All Confidential Customer Utility Information is encrypted in transit utilizing industry best practice encryption methods, except that Confidential Information does not need to be encrypted during email communications.	Encrypt all Confidential Customer and Non-Public Utility Information in transit using encryption methods compliant with NIST cryptographic standards and guidelines
8	All Confidential Customer Utility Information is secured or encrypted at rest utilizing	Encrypt all Confidential Customer and Non-Public Utility Information at rest using

	industry best practice encryption methods, or is otherwise physically secured.	encryption methods compliant with NIST cryptographic standards and guidelines, or is otherwise physically secured.
9	It is prohibited to store Confidential Customer Utility Information on any mobile forms of storage media, including, but not limited to, laptop PCs, mobile phones, portable backup storage media, and external hard drives, unless the storage media or data is encrypted.	None
10	All Confidential Customer Utility Information is stored in the United States or Canada only, including, but not limited to, cloud storage environments and data management services (Inconsistent with "zero trust architecture")	None
11	ESE monitors and alerts their network for anomalous cyber activity on a 24/7 basis.	None
12	Security awareness training is provided to all personnel with access to Confidential Customer Utility Information.	None
13	Employee background screening occurs prior to the granting of access to Confidential Customer Utility Information.	Employee background screening, including criminal background checks, occurs prior to the granting of access to Confidential Customer Utility Information
14	Replication of Confidential Customer Utility Information to non-company assets, systems, or locations is prohibited.	None
15	Access to Confidential Customer Utility Information is revoked when no longer required, or if employees separate from the ESE or Third Party Representative.	Access to Confidential Customer Utility Information is revoked within 24 hours when no longer required, or if employees separate from the ESE or Third Party Representative
16	N/A	Developing and maintaining a data inventory that an ESE can use to catalog its data and location (source: Joint Utilities' DAF Matrix comments)
17	N/A	Organizational communications (i.e., information transmitted or received by organizational information systems) are monitored, controlled, and protected at the external boundaries and key internal boundaries of the information systems. Subnetworks for publicly accessible system components are physically or logically separated from internal networks. Management of network devices use encrypted sessions.
18	N/A	Physical access to organizational information systems, equipment, and the respective operating environments is limited to authorized individuals. Physical security controls include the following: -- Visitors are escorted and their activity is monitored -- Audit logs of physical access are maintained -- Physical access devices are controlled and managed

APPENDIX B

Cybersecurity & Privacy Governance Committee Charter

BACKGROUND

Up-to-date cybersecurity and data privacy protections and processes must be in place for third-party access to non-public customer and system data from the Joint Utilities of New York. Data access initiatives such as the Data Access Framework (DAF) and Data Ready Certification (DRC) require oversight by the Joint Utilities to ensure necessary protections are in place and up-to-date.

PURPOSE

The Cybersecurity & Privacy Governance Committee (Committee) will provide oversight of New York energy data access initiatives involving cyber security and data privacy risk to ensure necessary protections for entities with access to confidential customer and utility information. These entities include the DRC Provider,[1] energy service entities (ESEs),[2] and other third parties.

KEY ACTIVITIES

The Governance Committee will:

- Regularly review and update the Self Attestation by considering the current cybersecurity and privacy threat landscape and applicable state/federal legislation, both pending and enacted.
- Address identified gaps in Staff's DAF Cybersecurity Matrix[3] that require the creation or modification of cybersecurity and privacy protections and processes by reviewing proposals with stakeholders/DPS Staff for feedback and filing proposed updates with the PSC.
- Review proposals with stakeholders and DPS Staff for feedback.
- File and coordinate proposed updates to SA or DAF Matrix with the Public Service Commission.
- Post Data Ready Certification provider process implementation:

[1] The DRC Provider is a third party that will be contracted by NYSERDA to manage ESE and other access to utility information.

[2] Per the DAF Order, an ESE is defined as "Any entity (including, but not limited to, ESCOs, DERs, and CCA Administrators) seeking access to energy related data from the data custodian, for the purposes defined under the access requirements. This does not include entities, such as utility contractors, who are performing a service for the utilities." (Appendix A, p. 6)

[3] Staff issued its Cybersecurity Matrix on May 17, 2021, which is a matrix of the current requirements associated with obtaining information from utilities.

1. Develop and maintain process to revoke access in the event an ESE has an issue (cyber or privacy incident) or is non-compliant with DSA/SA requirements.
2. Audit the DRC process regularly.

- Engage Stakeholders through presentations, whitepapers, forums, workshops, or working groups, as applicable.

MEMBER ROLES AND RESPONSIBILITIES

Joint Utilities	• Attend schedule meetings,[4] understand the current threat landscape and risks, and are familiar with the SA and DRC requirements and processes. • Manage administrative functions (e.g., onboarding of committee members, recordkeeping, meeting preparation, training, presentation, etc.). • Perform an annual review of the Governance Committee Charter for appropriate changes. • Coordinate an Advisory Working Group to consider stakeholder inputs.
DPS Staff	• Attend schedule meetings, understand the current threat landscape and risks, and are familiar with the SA and DRC requirements and processes. • Representation will come from Office of Markets and Innovation as well as from Office of Resiliency and Emergency Preparedness
DRC Provider	• Assess compliance of third parties to issue DRC. • Verify on an ongoing basis compliance of third parties at a frequency set by the Committee to allow third parties to maintain DRC.
Third Parties	• Comply with all processes established by the DRC Provider and Committee and ensure appropriate protections.

COMMITTEE MEMBERSHIP

Each Joint Utility is represented by **a designated person with cybersecurity expertise** (e.g., Chief Information Security Officer (CISO), Chief Information Officer (CIO)) with 7+ years of utility cybersecurity and/or privacy experience **and one delegate**. The Committee shall be composed of at least five Joint Utilities members and up to five DPS Staff member(s). The Committee will be chaired by one member from the Joint Utilities selected by a majority vote (51 percent) of the Committee and the Chair term will not exceed two years. Prior Chairs can serve future additional terms as a Chair upon the discretion of the Committee. This is a standing

[4] For all members, will make every attempt to attend all meetings, to be on-time, and to review all documents disseminated prior to the meeting. If a representative or their alternate cannot attend a meeting, the representative should let the Chair's know prior to the meeting (by telephone or e-mail).

Committee with no term limits for the members other than the Chair. Committee members may be dismissed at the discretion of the Committee Chair. Each member shall have an alternate to serve as a back-up.

If needed, specific utility and industry technical experts can be brought in support for specific topic discussions in the group.

The Chair may designate subcommittees on specific topics. These subcommittees will be charged with bringing suggestions, ideas, and perhaps draft products back to the Committee for discussion as well as to the Advisory Working Group as needed.

The Chair and designated utility/staff members will hold an agenda setting meeting prior to each meeting. The topics to be discussed at each meeting will be agreed to in the agenda setting meeting.

MEETINGS

The Committee will meet at least quarterly and hold additional meetings as needed to fulfill its responsibilities as described in this Committee Charter and as called by the Committee Chair.

ADVISORY WORKING GROUP

The Committee will establish, or leverage an existing, advisory working group of stakeholders (e.g., Utility Coordination Group), including the DRC Provider, ESEs, and NYSERDA, to:

- provide suggestions, feedback and recommendations for the Committee.

  The Advisory Working Group can explain their positions to the Committee but the Committee itself remains the deciding group for issuing recommendations. If they have issues with the recommendations provided to the Commission, the Commission will provide a period for Notice and Comment on the recommendations.

REPORTING

Annually, the Committee will submit a report to the Commission, summarizing the findings and proposing recommendations for cybersecurity and privacy protections and processes. The Commission will act on the report withing 4 months of the recommendations being issued.