STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

At a session of the Public Service Commission held in the City of Albany on April 16, 2026

COMMISSIONERS PRESENT:

Rory M. Christian, Chair
James S. Alesi
David J. Valesky
John B. Maggiore
Uchenna S. Bright
Denise M. Sheehan
Radina R. Valova

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.

MEMORANDUM AND RESOLUTION APPROVING ADOPTION OF INFORMATION TECHNOLOGY CYBERSECURITY REGULATIONS

(Issued and Effective April 17, 2026)

BY THE COMMISSION:

INTRODUCTION

For many years, the New York State Public Service Commission (the Commission) has monitored and regulated specific components of the cybersecurity of regulated utilities within the State of New York via its orders. But as the frequency and sophistication of threats targeting utilities has grown, it has become increasingly clear that comprehensive regulations are needed.

In June 2025, the Commission published a draft of mandatory, minimum, enforceable Information Technology (IT) regulations in the State Register and sought comments. In

January 2026 a revised draft responsive to those comments was published and additional comments were received. The Commission now adopts the revised regulations (Attachment A).

BACKGROUND

In the wake of the September 11, 2001 attacks, the Commission formed an office of utility security within the Department of Public Service (later renamed the Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness) and ordered utilities to review their cybersecurity frameworks.[1] In the years since, the Commission has revisited cybersecurity in numerous orders, outlining rules for Personally Identifiable Information (PII) and general IT security, among other actions.[2] Since the Commission's first

---

[1] Rebecca Slaytor, Performing Cybersecurity Expertise: Challenges for Public Utility Commissions, 35 Berkeley Tech. L.J. 757, 773 (2020).

[2] See, e.g., Case 09-M-0074, In the Matter of Advanced Metering Infrastructure, Order Adopting Minimum Functional Requirements for Advanced Metering Infrastructure Systems and Initiating an Inquiry Into Benefit-Cost Methodologies (issued February 13, 2009), p. 16; Case 13-M-0178, In the Matter of a Comprehensive Review of Security for the Protection of Personally Identifiable Customer Information, Order Directing the Creation of an Implementation Plan (issued August 19, 2013); Case 15-E-0050, Motion of the Commission as to the Rates, Charges, Rules and Regulations of Consolidated Edison Company of New York, Inc. for Electric Service, Order Approving Advanced Metering Infrastructure Business Plan Subject to Conditions (issued March 17, 2016), p. 44; 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), pp. 50-64; and Case 20-M-0082, In the Matter of the Strategic Use of Energy Related Data, Order Adopting a Data Access Framework and Establishing Further Process (issued April 15, 2021).

cybersecurity order over twenty-five years ago, cyberattacks against critical infrastructure have been characterized by every-increasing "frequency and sophistication." [3] Moreover, the threat landscape has evolved. Potential threat actors now range from small, financially motivated groups to state-sponsored Advanced Persistent Threats (APTs), strategically positioned to strike in the event of geopolitical or military conflict.[4]

In 2023, the State Legislature instructed the Commission to promulgate rules and regulations directing electric and gas corporations to "develop and implement tools to... monitor and protect customer privacy," including customer usage data.[5] In 2025, Governor Hochul called for the responsible state agencies to strengthen cybersecurity regulation for water

---

[3] Idaho National Laboratory, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector 2 (2016), https://nsarchive.gwu.edu/sites/default/files/documents/3705441/Idaho-National-Laboratory-Cyber-Threat-and.pdf (last accessed May 27, 2025).

[4] See CISA, Cybersecurity Alert: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a (last accessed May 27, 2025). See also U.S. Dep't of Energy, Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid 15-16, Oct. 2022, https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf (last accessed May 27, 2025); CISA, ICS Alert: Cyber-Attack Against Ukrainian Critical Infrastructure, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 (last accessed October 16, 2024).

[5] 2023 Sess. Law News of N.Y. Ch. 67 (A. 2896). See also Public Service Law §66(30).

infrastructure.[6] In December 2024, the Commission adopted a report recommending that it promulgate a "specific set of mandatory, enforceable, minimum requirements for utility IT system cybersecurity programs, policies, and governance."[7]

Broadly, the utility sector's technologies can be categorized into two types: Information Technology (IT) and Operational Technology (OT). IT comprises any "discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information."[8] Examples of IT systems includes those that handle PII.[9] OT encompasses a broad range of systems and devices that interact with the physical environment.[10] Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, and physical environment measurement

---

[6] Kathy Hochul, 2025 State of the State 67, available at https://www.governor.ny.gov/sites/default/files/2025-01/2025StateoftheStateBook.pdf (last accessed May 27, 2025).

[7] Case 25-M-0664, In the Matter of the Commission's Assessment of Utility Cybersecurity Programs, Protections, and Compliance with State Standards Pursuant to PSL Section 66(30), Order Authorizing the Release of a Report Pursuant to Public Service Law §66(30) (issued December 19, 2025), Attachment A at 3.

[8] Appendix A, §1200.1(g). This definition of IT is taken from the revised regulations. It, in turn, is based on 40 U.S.C. §11101, a definition commonly used to define the term. NIST, Special Publication 800-59, Guideline for Identifying an Information System as a National Security System, p. 15 (2003).

[9] NIST, Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), B-1 (2010), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

[10] NIST, Special Publication NIST SP 800-82r3, Guide to Operational Technology (OT) Security 8 (2023), https://doi.org/10.6028/NIST.SP.800-82r3.

systems.[11]

Although IT and OT systems are separate and distinct, they are often interconnected. Thus, one estimate is that three-quarters of cyberattacks impacting OT systems originated as IT attacks.[12] For this reason, the Commission determined to begin the promulgation of comprehensive cybersecurity regulations by addressing IT systems.

In June 2025, the Commission commenced this proceeding to consider draft regulations to address IT cybersecurity.[13] After an initial draft was published in the State Register comments were received and a second draft was published responsive to those comments.

LEGAL AUTHORITY

The IT regulations promulgated today govern the IT systems of "covered entities," which the regulations define as including all gas and electric utilities, water-works utilities, and steam utilities with certain exceptions. The Commission has ample authority to make and enforce such regulations.

As it relates to gas and electric corporations, the Commission has "general supervision" authority over "all gas corporations and electric corporations" in the State.[14] Those companies are required to provide safe and adequate service to

---

[11] Id.

[12] Australian Cyber Security Centre et al., Principles of Operational Technology Cyber Security 9-10, https://www.cyber.gov.au/sites/default/files/2024-10/principles of operational technology cyber security.pdf (last accessed October 18, 2024).

[13] Case 25-M-0302, Order Instituting Proceeding to Establish Cybersecurity Rules of Information Technology (issued June 13, 2025).

[14] Public Service Law §66(1).

their customers at just and reasonable rates.[15] The Commission is charged with keeping informed of the methods and practices of those companies and, when they are unsafe, inefficient, or inadequate, prescribing safe and adequate equipment and its use.[16] Given the multitude of cyber threats and the myriad consequences of a cyberattack, adequate cybersecurity is now an intrinsic part of safe and adequate service. The Commission also has the authority to order "reasonable improvements" to the manufacture, distribution, or supplying of gas or electric if those improvements are in the "public interest."[17] In addition to all these powers, the Commission may provide for both general audits of customer privacy and audits of cyber security practices.[18]

Given the potential financial impact of a successful cyberattack, adequate IT cybersecurity is crucial to ensure consumer protection, customer privacy, and just and reasonable rates, and it is plainly in the public interest. Moreover, in the case of gas and electric corporations, the Legislature has granted the Commission explicit authority to promulgate cybersecurity regulations. Specifically, the Public Service Law provides that the Commission "shall" promulgate both OT

[15] Public Service Law §65(1)-(2).

[16] Public Service Law §66(5).

[17] Public Service Law §66(2).

[18] Public Service Law §66(19)(a)&(d).

regulations and regulations to protect customer privacy.[19] As explained above, private customer data is routinely generated, manipulated, and stored on IT systems, and therefore this grant of authority necessarily involves regulating IT. Likewise, the IT-OT connection means that any grant of authority to regulate OT must touch upon IT as necessary to secure OT systems.

As it relates to water-works corporations, those companies must also provide "safe and adequate" service at "just and reasonable rates."[20] As with gas and electric companies, the Commission must keep informed of the practices of water-works corporations and when those practices are found to be "unsafe, inefficient or inadequate" it may prescribe safe, efficient, and adequate property and procedures for its use.[21] In addition to all these powers, the Commission has the power to provide for management and operation audits of water-works corporations with annual gross revenues in excess of ten million dollars.[22] Taken together, Article 89 of the Public Service Law has been recognized as "a comprehensive scheme for the regulation of water companies and for the fixing of rates."[23] For the same

---

[19] Public Service Law §66(30) reads, in part, that the Commission shall "[p]romulgate rules and regulations to direct electric or gas corporations to develop and implement tools to monitor (a) operational control networks giving the electric or gas corporation the ability to undertake the detection of unauthorized network behavior related to such corporation's industrial control systems, as defined in subdivision fifteen of section 1-103 of the energy law and (b) monitor and protect customer privacy, including but not limited to customer electric and gas consumption data from unauthorized disclosure.

[20] Public Service Law §89-b(1).

[21] Public Service Law §89-c(4).

[22] Public Service Law §89-c(15)

[23] City of New York v. Maltbie, 274 N.Y. 90, 96 (1937).

reasons that similar provisions justify IT regulations for gas and electric, they justify IT regulations for water.

Steam corporations are also obligated to provide "safe and adequate" service at "just and reasonable" rates.[24] As with gas and electric corporations, the Commission maintains "general supervision" over steam corporations.[25] The Commission has the power to "order such reasonable improvements" to the methods of manufacturing, distributing, or supplying steam "as will best promote the public interest."[26] It also has the power to regulate when equipment or property is found to be inadequate or inefficient, just as it does with gas, electric, and water corporations.[27] For the same reasons that similar provisions justify IT regulations for gas and electric, they also justify IT regulations for steam.

NOTICES OF PROPOSED RULEMAKING

Pursuant to the State Administrative Procedure Act (SAPA) §202(1), a Notice of Proposed Rulemaking (NOPR) was published in the State Register on July 9, 2025 [SAPA No. 25-M-0302SP1]. The time for submission of comments pursuant to that SAPA Notice expired on September 15, 2025. More than a dozen comments were received.

Thereafter, pursuant to SAPA §202(1), a revised NOPR was published in the State Register on February 4, 2026 [SAPA No. 25-M-0302SP1] that addressed the comments and described revisions to the initially proposed regulations. The time for

[24] Public Service Law §79(1).

[25] Public Service Law §80(1).

[26] Public Service Law §80(2).

[27] Public Service Law §80(4).

submission of comments pursuant to that SAPA Notice expired on March 23, 2026. Four comments were received by the expiration date, and two were received late.

EVALUATION OF COMMENTS

In an Order noticing the first draft of the IT cybersecurity regulations for comments, the Commission explained that the risk of a cyberattack can never be entirely eliminated.[28] Instead, the Commission's goal was "sound cybersecurity" practices, which it identified with the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) version 2.0.[29] The NIST framework identifies six "core" functions for sound cybersecurity: it requires periodic assessment of an organization's risk profile, affirmative steps to protect IT assets, proactive surveillance and detection of threats, pre-determined response strategies, effective recovery plans, and a strong governance structure to make these goals reality.[30] The Commission assesses the revised IT regulations against this framework.

As revised, the IT regulations obligate covered entities to adopt sound, risk-based cybersecurity practices to mitigate their risk-of and risk-from a cyberattack. They require each covered entity to assess its specific risk profile and to design a cybersecurity program that addresses those risks in a robust fashion. They require covered entities to protect their IT systems using generally accepted access controls and

[28] Case 25-M-0302, Order Instituting Proceeding, p. 12.

[29] Case 25-M-0302, Order Instituting Proceeding, p. 12. NIST, The NIST Cybersecurity Framework (CSF) 2.0 at 2, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (last accessed April 1, 2026).

[30] Id.

authentication practices, and they further require these entities to take proactive steps to detect network intrusions. Finally, the regulations require covered entities to plan both to respond to and recover from cyber incidents. These plans must be developed and implemented by a qualified Chief Information Security Officer employed for this purpose under the supervision of senior management. The regulations comply with all core functions of the NIST-CSF Framework, with appropriately specific refinements given criticality of the infrastructure involved.

Six comments were received pertaining to the revised IT regulations. One set of comments was received from the Independent Power Producers of New York, Inc. (IPPNY) and New York Transco, LLC (NYT). IPPNY and NYT represent "lightly regulated" electric corporations (which own electric generation facilities that produce and sell electricity on the wholesale marketplace) or merchant transmission developers (which build, own, and operate electric transmission lines delivering electricity in the wholesale market), respectively. At the onset, IPPNY is correct that these companies constitute electric corporations for the purposes of Public Service Law (PSL) §2(13) and public utility corporations for the purposes of PSL §2(23), making them presumptively subject to the revised regulations. However, section 1200.1(c)(2) of the revised regulations specifically exempts electric corporations maintaining fewer than 50,000 service lines. This has the effect of exempting wholesale electric producers and transmission line operations from the definition of "covered entities" because they maintain, by definition, zero service lines since they do not sell directly to the public.

To the extent that IPPNY seeks affirmation that their lightly regulated status means these are not subject to the

cybersecurity jurisdiction of the Commission, this goes too far. The regulation of electric corporations has been adapted over time to accommodate the development of competitive wholesale markets and lightened ratemaking policies. The Commission has determined that lightly regulated entities may be exempt from certain PSL provisions that pertain to retail service because they do not serve captive utility customers.[31] But lightened regulation does not preclude the Commission from any regulation in the public interest. The Commission retains authority to regulate the cybersecurity of lightly regulated companies to protect captive ratepayers.[32] Here, the Commission has stayed its hand for two reasons. First, wholesale electric producers and transmission line operators do not sell directly to captive ratepayers, and so the interest in their IT is lessened. Second, New York's interest in IT cybersecurity for wholesale generator and transmission companies is sufficiently vindicated by the North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC-CIP) regulations to which they are subject. Should the prudential reasons underlying this decision change in the future, the cybersecurity treatment of even lightly regulated entities may change, too.

The Commission also received comments in the form of a letter from Assemblymember Jonathan Rivera, the Chair of the NYS Assembly's Administrative Regulatory Review Commission.[33] Assemblymember Rivera notes that the initial draft of the IT

[31] See, e.g., Case 16-E-0409, Indeck Corinth Limited Partnership, Order Providing for Lightened Regulation (issued December 21, 2016), pp. 3-4.

[32] See Case 16-E-0409, supra, Order Providing for Lightened Regulation, pp. 4-5.

[33] Two late comments, duplicative of Assemblymember Rivera's comments, were also received after the expiration of the deadline to file comments.

regulations noticed for comment on July 9, 2025, included certain telecom companies within its ambit. Telecom companies were removed from the revised regulations, and Assemblymember Rivera comments they should be restored to the final regulations. In a slew of comments on the initial draft regulations, members of the telecom industry argued that the Commission lacks the authority to impose IT cybersecurity regulations on wireline telephone and cable providers. The Commission continues to review the existing statutory and regulatory framework concerning the obligation of telecom entities to implement cybersecurity defenses of their systems and products and to protect customers in the state.

The telecoms also argued that their market exposure, infrastructure, and cross-jurisdictional footprint render their cybersecurity posture distinct from that of the energy and water utilities The telecoms contend that the diversity of their systems contrast with New York's energy and water utilities, which are geographically bound by state lines, less differentiated in their IT infrastructures, more homogenous in their cybersecurity postures, and which have been subject to close regulation of their cybersecurity practices by the Commission for many years. Based on this, the telecoms argue generally for a more flexible, risk-based approach to cybersecurity regulations that takes account of each company's unique risk profile. The Department's ongoing review of the regulatory framework in the context of the asserted differences between the telecom industry and energy and water utilities counsel--at this time--for the omission of the telecom entities from this set of regulations. The Commission reserves the right

to promulgate regulations in the future to regulate telecom IT.[34]

Finally, the Commission received joint comments from a group of eleven regulated utilities, including electric, gas, steam, and one water utility (the Joint Utilities).[35] The Joint Utilities make two requests and, with those modifications, "support adoption of the rules by the Commission." First, the Joint Utilities comment that the Commission should limit third-party breach reporting requirements. Specifically, the Joint Utilities write that when their third-party vendors experience cybersecurity data breaches that fact should only be reported to the Commission if the information is made public by the vendor since reporting could place third-party vendors "in direct conflict with existing confidentiality agreements, data sharing agreements, and commercial contracts." The Commission disagrees with this analysis. Vendors often maintain important information, including PII, for utilities, and limiting reporting requirements would therefore undermine the entire thrust of the revised regulations. Moreover, even when breaches are made public this is often months later. Effective regulatory oversight of utilities' cybersecurity programs cannot be done with stale information.

Second, the Joint Utilities request that this Order

---

[34] Case 25-M-0302, Letters to Legislative Leaders Regarding Notice of Revised Proposed Rulemaking, pp. 42–43.

[35] The eleven companies making up the Joint Utilities are Central Hudson Gas & Electric Corporation, Consolidated Edison Company of New York, Inc., National Grid (The Brooklyn Union Gas Company d/b/a National Grid NY; KeySpan Gas East Corporation d/b/a National Grid; Niagara Mohawk Power Corporation d/b/a National Grid), New York State Electric & Gas Corporation, Orange and Rockland Utilities, Inc., Rochester Gas and Electric Corporation, National Fuel Gas Distribution Corporation, Liberty Utilities (New York Water) Corp., and Liberty Utilities (St. Lawrence Gas) Corp.

provide special cost recovery mechanisms for "incurred, incremental costs associated with implementing compliance obligations that exceed existing cybersecurity practices." The Joint Utilities point to special cost recover mechanisms the Commission previously fashioned when adopting the Integrated Energy Data Resource order[36] and the Comprehensive Energy Efficiency Initiative.[37] The Commission rejects these analogues since those programs were newly minted and required significant initial cost outlays to bring online. In contrast, all Joint Utilities maintain cybersecurity programs at high levels of maturity, which require only incremental investments to comply with the revised rules. Accordingly, the appropriate cost recovery mechanism here is cost deferral.

Operations and maintenance expenses incurred by a utility to comply with the cyber security directives in this Order may be deferred on its books and records subject to future review in the utility's next rate proceeding. Similarly, for capital expenditures incurred to comply with this Order, the utility may defer the carrying costs associated with these capital expenditures after the related plant is placed into service, until such time the plant is reflected in base rates. The carrying costs shall reflect the return of investment (i.e., depreciation expense) and return on investment. The applicable rate to be used to calculate the return on investment shall be the utility's Commission-authorized, pre-tax rate of return.

[36] Case 20-M-0082, Proceeding on Motion of the Commission Regarding Strategic Use of Energy Related Data, Order Implementing an Integrated Energy Data Resource (issued February 11, 2021), p. 21.

[37] Case 18-M-0084, In the Matter of a Comprehensive Energy Efficiency Initiative, Order Adopting Accelerated Energy Efficiency Targets (issued December 13, 2018), p. 67.

All deferred costs shall be reasonably and incrementally incurred to comply with this Order, to the extent such compliance requires activities or investments that go beyond the utility's existing cybersecurity practices. For labor-related operations and maintenance, expenses will be considered incremental and eligible for deferral only to the extent that total actual labor expenses for the relevant year exceed the labor expenses included in rates. Further, the utility must demonstrate the incremental labor expenses were directly related to complying with the cyber security directives of this Order.

The net plant in service associated with capital expenditures incurred to comply with this Order shall be excluded from each utility's total actual net plant in service for purposes of the net plant reconciliation calculation until such time as the incremental incurred plant is allowed to be reflected in base rates.

The utility shall maintain documentation to support the nature and amount of all deferred costs. All deferred costs shall be subject to audit and review by Department of Public Service staff and shall be subject to Commission determination in the utility's next rate proceeding.

This cost recovery mechanism strikes the appropriate balance between assuring cost recovery and ensuring appropriate oversight by Department staff.

CONCLUSION

The regulations adopted today represent a significant step in meeting the Commission's long-term goal to strengthen the cybersecurity of regulated entities within the Commission's jurisdiction, in line with the broader New York State Cybersecurity Strategy announced by Governor Hochul in August

2023.[38] It fulfils the Governor's State of the State call to address the cybersecurity needs of water infrastructure. And it fulfils the statutory directive to promulgate regulations to protect customer privacy contained in gas or electric company information technology. The Commission will continue the hard work of strengthening cybersecurity in the coming months and years.

By the Commission,

(SIGNED) MICHELLE L. PHILLIPS
Secretary

[38] Kathy Hochul, New York State Cybersecurity Strategy 5 (2023), https://www.governor.ny.gov/sites/default/files/2023-08/2023-NewYork-CybersecurityStrategy.pdf.

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

At a session of the Public Service Commission held in the City of Albany on April 16, 2026

COMMISSIONERS PRESENT:

Rory M. Christian, Chair
James S. Alesi
David J. Valesky
John B. Maggiore
Uchenna S. Bright
Denise M. Sheehan
Radina R. Valova

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.

RESOLUTION OF THE COMMISSION

(Issued and Effective April 17, 2026)

STATUTORY AUTHORITY

Public Service Law §§65(1)-(2), 66(1), 66(2), 66(5), 66(19)(a), 66(19)(d), 66(30), 79(1), 80(1), 80(2), 80(4), 89-b(1), 89-c(4), 89-c(15)

RESOLVED:

1. The provisions of §202(1) of the State Administrative Procedure Act and §101-a(2) of the Executive Law have been complied with.

2. The adoption of 16 NYCRR Part 1200 is approved.

By the Commission,

(SIGNED) MICHELLE L. PHILLIPS
Secretary

APPENDIX A

Chapter XII. Regulated Entity Security

Subchapter A. Information Technology

Part 1200. INFORMATION TECHNOLOGY CYBERSECURITY REQUIREMENTS FOR COVERED ENTITIES

Section 1200.0 Finding of Necessity and Purpose.

For many years, the New York State Public Service Commission has monitored and regulated specific components of cybersecurity for utilities within its jurisdiction. One area of concern has been the increasing frequency and sophistication of threats targeting the information technology of companies supplying critical infrastructure. This includes systems handling sensitive electronic data, like personal identifiable information, as well as business records. Cybercriminals can cause significant financial losses for regulated entities and for New York consumers whose private information may be revealed or stolen for illicit purposes. The utility sector is a significant target of cybersecurity threats, and the danger continues to increase.

Given the increasing threats to cybersecurity, minimum, enforceable standards are warranted. The purpose of these regulations is to establish such minimum standards for information technology systems of large companies within the commission's jurisdiction. These regulations seek to protect both customer privacy as well as the broader integrity of information technology. Adoption of a cybersecurity program as outlined in these regulations is a priority for the commission and for the State of New York. For the companies covered by these regulations, existing commission orders in conflict with it will be abrogated as the regulations are phased in. For smaller companies not covered by these regulations, existing commission orders or regulations will still apply. For all regulated entities, it is critical that those that have not yet done so move swiftly and urgently to adopt a cybersecurity program compliant with these regulations or governing orders.

Section 1200.1 Definitions.

For purposes of this Part only, the following definitions apply:

(a) *Affiliate* means any person that controls, is controlled by or is under common control with another person. For purposes of this subdivision, control means direct or indirect authority to direct or cause the direction of the management and policies of a person, whether through the ownership of stock of such person or otherwise.

(b) *Authorized User* means any employee, contractor, agent or other person that participates in the operations of a covered entity and is authorized to access and use any information technology or data of the covered entity.

(c) *Covered Entity* means any public utility company as defined in subdivision 23 of section 2 of the Public Service Law except:

(1) a water-works corporation, as defined in subdivision 26 of section 2 of the Public Service Law serving fewer than 50,001 service connections, as defined in subdivision (c) of section 501.1 of this Title;

(2) an electric corporation, as defined in subdivision 13 of section 2 of the Public Service Law, maintaining fewer than 50,000 service lines, as defined in subdivision (b) of section 98.1 of this Title;

(3) a gas corporation, as defined in subdivision 11 of section 2 of the Public Service Law, that constitutes a small business as defined in subdivision 8 of section 102 of State Administrative Procedure Law;

(4) a telephone corporation, as defined in subdivision 17 of section 2 of the Public Service Law;

(5) any person operating solely as a telegraph corporation, as defined in subdivision 19 of section 2 of the Public Service Law;

(6) a municipal corporation as defined in section 119-n of the General Municipal Law;

(7) an employee, agent, representative or designee of a covered entity, who is itself a covered entity, provided that such employee, agent, representative or designee is covered by the cybersecurity program of the covered entity.

(d) *Cybersecurity Event* means

(1) any successful or unsuccessful attempt to gain unauthorized access to, disrupt or misuse information technology owned or controlled by a covered entity or information stored on such information technology; or

(2) the unauthorized dissemination, intentionally or unintentionally, of nonpublic information stored on information technology owned or controlled by a covered entity.

(e) *Cybersecurity Incident* means a cybersecurity event that

(1) has a reasonable likelihood of harming any part of the normal operations of the covered entity; or

(2) actually or imminently jeopardizes the confidentiality, integrity or availability of the covered entity's information technology or the continuing functionality of any aspect of the covered entity's business or operations; or

(3) results in loss of operational data of the covered entity; or

(4) includes a demand for payment of a ransom to restore access to the covered entity's information technology system; or

(5) results in the dissemination of nonpublic information stored on information technology owned or controlled by a covered entity; or

(6) otherwise triggers a notice requirement to any government body, regulatory agency or any other supervisory body by law, order, or regulation.

(f) *Electronic Masking* means a security technique that obfuscates or anonymizes sensitive data elements such that the original information is not visible or accessible to unauthorized individuals or systems.

(g) *Information Technology* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, provided that information technology does not include operational technology.

(h) *Least Privilege* means the principle that a system should restrict the access privileges of authorized users (or processes acting on behalf of authorized users) to the minimum necessary to accomplish assigned tasks.

(i) *Multi-Factor Authentication* means authentication through verification of at least two of the following types of authentication factors:

(1) something the user knows; or

(2) something the user has; or

(3) something the user is.

(j) *Nonpublic Information* means all electronic information that is not publicly available information and is:

(1) business-related information of a covered entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a materially adverse impact to the business, operations or security of the covered entity; or

(2) any information concerning an individual that, because of name, number, personal mark, or other identifier, can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) driver's license number or non-driver identification card number, (iii) bank account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; or

(3) any (i) financial records, including billing records, of any individual or (ii) security code, access code or password that would permit access to an individual's financial accounts; or

(4) any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual; or

(5) identifiable customer consumption or use data.

(k) *Penetration Testing* means a test methodology during which assessors attempt to circumvent or defeat the security features of an information technology system by attempting penetration of the system from outside or inside the covered entity's Information technology environment.

(l) *Person* means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, company, association or joint-stock association.

(m) *Publicly Available Information* means any information that a covered entity has a reasonable basis to believe is lawfully made available to the general public from Federal, State or local government records; widely distributed media; or disclosures to the general public that are required to be made by Federal, State or local law.

(1) For the purposes of this subdivision, a covered entity has a reasonable basis to believe that information is lawfully made available to the general public if the covered entity has taken steps to determine:

(i) that the information is of the type that is available to the general public; and

(ii) whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(n) *Risk Assessment* means the risk assessment that each covered entity is required to conduct under section 1200.9 of this Part.

(o) *Risk-Based Authentication* means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a user and requires additional verification of the user's identity when such deviations or changes are detected, such as through the use of challenge questions.

(p) *Senior Officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information technology, compliance and/or risk of a covered entity.

(q) *Third Party Service Provider(s)* means a person that (1) is not an affiliate of a covered entity, (2) provides services to a covered entity, and (3) maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to a covered entity.

(r) *Operational Technology* means a discrete electronic system, including hardware or software components, as well as combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment, manage devices that interact with the physical environment or monitor and control devices, processes, and infrastructure in an industrial setting, including industrial control systems, supervisory control and data acquisition systems, physical access control systems, distributed control systems, safety instrumented systems, programmable logic controllers, human machine interfaces, remote terminal units, and other similar control systems often found in industrial and critical infrastructure sectors.

Section 1200.2 Cybersecurity Program.

(a) *Cybersecurity Program*. Each covered entity must maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information technology.

(b) The cybersecurity program must be based on the covered entity's risk assessment and must, at a minimum, contain a plan to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of nonpublic information stored on the covered entity's information technology;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the covered entity's information technology systems, and nonpublic information stored on those systems, from unauthorized access, use or other malicious acts;

(3) detect cybersecurity events;

(4) respond to identified or detected cybersecurity events to mitigate any negative effects;

(5) recover from cybersecurity events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) A covered entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the covered entity.

(d) All documentation and information relevant to the covered entity's cybersecurity program must be made available to the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee, within 10 calendar days of a request.

Section 1200.3 Cybersecurity Policy.

(a) Each covered entity must implement and maintain a written cybersecurity policy or policies, approved by a senior officer, the covered entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the covered entity's policies and procedures for the protection of its information technology and nonpublic information. The cybersecurity policy must be based on the covered entity's risk assessment and must address the following areas to the extent applicable to the covered entity's operations:

(1) information security;

(2) data governance and classification;

(3) asset inventory and device management;

(4) access controls and identity management;

(5) business continuity and incident recovery planning and resources;

(6) systems operations and availability concerns;

(7) systems and network security;

(8) systems and network monitoring;

(9) systems and application development and quality assurance;

(10) physical security and environmental controls;

(11) a cybersecurity surveillance program;

(12) customer data privacy;

(13) the sufficiency of segregation of customer data from other business systems;

(14) vendor and third party service provider management;

(15) risk assessment;

(16) incident response; and

(17) implementation of controls to allow segmentation of its information technology from its operational technology in the event of a cybersecurity incident.

(b) All documentation and information relevant to the covered entity's cybersecurity policy must be made available to the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee, within 10 calendar days of a request.

Section 1200.4 Chief Information Security Officer.

(a) Chief Information Security Officer. Each covered entity must designate a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, "Chief Information Security Officer" or "CISO"). The CISO may be employed by the covered entity, one of its affiliates or a third party service provider. To the extent this requirement is met using a third party service provider or an affiliate, the covered entity must:

(1) retain responsibility for compliance with this Part;

(2) designate a senior member of the covered entity's personnel responsible for direction and oversight of the third party service provider; and

(3) require the third party service provider to maintain a cybersecurity program that protects the covered entity in accordance with the requirements of this Part.

(b) Report. At least yearly, the CISO of each covered entity must report in writing to the covered entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report must be timely presented to the senior officer of the covered entity responsible for the covered entity's cybersecurity program. The CISO must report on the covered entity's cybersecurity program and material cybersecurity risks. The CISO must consider to the extent applicable:

(1) the confidentiality of nonpublic information and the integrity and security of the covered entity's information technology;

(2) the covered entity's cybersecurity policies and procedures;

(3) material cybersecurity risks to the covered entity;

(4) the overall effectiveness of the covered entity's cybersecurity program; and

(5) cybersecurity incidents involving the covered entity during the time period addressed by the report.

Section 1200.5 Continuous Monitoring, Penetration Testing and Vulnerability Assessments.

(a) The cybersecurity program for each covered entity must include monitoring and testing, developed in accordance with the covered entity's risk assessment, designed to assess the effectiveness of the covered entity's cybersecurity program. The monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in information technology that may create or indicate vulnerabilities, covered entities must conduct:

(1) penetration testing of the covered entity's information technology based on relevant identified risks in accordance with the risk assessment at least every 12 months; and

(2) vulnerability assessments, including any systematic scans or reviews of information technology reasonably designed to identify publicly known cybersecurity vulnerabilities in the covered entity's information Technology based on the Risk Assessment at least every six months.

(b) All documentation and information pertaining to a Covered Entity's monitoring, testing, Penetration Testing, and vulnerability assessments must be made available to the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee, within 10 calendar days of a request.

Section 1200.6 Audit Trail.

(a) Each covered entity must securely maintain systems that:

(1) are designed to reconstruct material changes to information technology sufficient to reconstruct and restore normal operations of the covered entity at the time of a cybersecurity incident disrupting service; and

(2) include audit trails designed to detect and respond to cybersecurity incidents that have a reasonable likelihood of harming any part of the normal operations of the covered entity.

(b) Each covered entity must maintain audit trail records required by subdivision (a) of this section for not fewer than three years.

Section 1200.7 Access Privileges.

(a) As part of its cybersecurity program, each covered entity must limit user access privileges to information technology that provides access to nonpublic information and must review such access privileges yearly based on the covered entity's risk assessment.

(b) In assigning access privileges, user access privileges must be assigned according to the principle of least

privilege.

(c) Each covered entity must create a written policy to employ electronic masking of sensitive information, determining what information is masked for which authorized users according to the principle of least privilege.

Section 1200.8 Application Security.

(a) Each covered entity's cybersecurity program must include written procedures, guidelines or standards designed to ensure the use of secure development practices for in-house developed applications utilized by the covered entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the covered entity within the context of the covered entity's technology environment.

(b) All such procedures, guidelines or standards must be reviewed, assessed, and updated at least once every two years by the CISO (or a designee) of the covered entity.

Section 1200.9 Risk Assessment.

(a) At least once every two years, each covered entity must conduct a risk assessment of the covered entity's information technology sufficient to inform the design of the cybersecurity program required by section 1200.2 of this Part. Such risk assessment should be updated as reasonably necessary to address changes to the covered entity's information technology, nonpublic information or business operations. The covered entity's risk assessment should allow for revision of controls to respond to technological developments and evolving threats and should consider the particular risks of the covered entity's business operations related to cybersecurity, nonpublic information collected or stored, information technology utilized and the availability and effectiveness of controls to protect nonpublic information and information technology.

(b) The risk assessment must be carried out in accordance with written policies and procedures and must be documented. Such policies and procedures must, at a minimum, include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the covered entity;

(2) criteria for the assessment of the confidentiality, integrity, security, and availability of the covered entity's information technology and nonpublic information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks.

(c) All documentation and information relevant to the covered entity's risk assessment must be made available to the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee, within 10 calendar days of a request.

Section 1200.10 Cybersecurity Personnel and Intelligence.

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 1200.4(a) of this Part, each covered entity must:

(1) utilize qualified cybersecurity personnel of the covered entity, an affiliate or a third party service provider sufficient to manage the covered entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 1200.2(b)(1)-(6) of this Part;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A covered entity may choose to utilize a qualified third party service provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 1200.11 of this Part.

Section 1200.11 Third Party and Affiliate Service Provider Security Policy.

(a) Each covered entity must implement written policies and procedures designed to ensure the security of information technology and nonpublic information that are accessible to, or held by, third party service providers or affiliates. Such policies and procedures should be based on the risk assessment of the covered entity and must address to the extent applicable:

(1) the identification and risk assessment of third party service providers and affiliates;

(2) minimum cybersecurity practices required to be met by such third party service providers or affiliates in order for them to access the information technology or nonpublic information of a covered entity; and

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such third party service providers or affiliates.

(b) Such policies and procedures must be reassessed every two years based on the risk such third party service providers or affiliates present and the continued adequacy of their cybersecurity practices.

(c) Such policies and procedures must include relevant guidelines for due diligence and/or contractual protections relating to third party service providers or affiliates including, to the extent applicable, guidelines addressing:

(1) the third party service provider or affiliate's policies and procedures for access controls, including its use of multi-factor authentication as required by section 1200.12 of this Part, to limit access to relevant information technology and nonpublic information;

(2) the third party service provider or affiliate's policies and procedures for use of encryption as required by section 1200.15 of this Part to protect nonpublic information in transit and at rest;

(3) notice to be provided to the covered entity in the event of a cybersecurity incident directly impacting

the covered entity's information technology or the covered entity's nonpublic information being held by the third party service provider or affiliate; and

(4) representations and warranties addressing the third party service provider or affiliate's cybersecurity policies and procedures that relate to the security of the covered entity's information technology or nonpublic information.

(d) Limited Exception. An agent, employee, representative or designee of a covered entity who is itself a covered entity need not develop its own third party information security policy pursuant to this section if the agent, employee, representative or designee follows the policy of the covered entity that is required to comply with this Part.

Section 1200.12 Access Controls

(a) Multi-Factor Authentication. Based on its risk assessment, each covered entity must select access controls, which may include multi-factor authentication and/or risk-based authentication, to protect against unauthorized access to nonpublic information or information technology.

(b) Multi-factor authentication must be utilized for any authorized user accessing the covered entity's internal networks from an external network, such as that from a virtual private network, remote access, or remote desktop, unless the covered entity's CISO (or designee) has approved in writing the use of reasonably equivalent or more secure access controls.

Section 1200.13 Limitations on Data Retention.

As part of its cybersecurity program, each covered entity must include policies and procedures for the secure disposal on a periodic basis not exceeding once every three years of any nonpublic information identified in section 1200.1(i)(2)-(4) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the covered entity, except where such information is otherwise required to be retained by law, order or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Section 1200.14 Training and Monitoring.

As part of its cybersecurity program, each covered entity must:

(a) implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access, use of or tampering with nonpublic information by such authorized users; and

(b) provide annual cybersecurity awareness training for all personnel that is updated to reflect risks identified by the covered entity in its risk assessment.

Section 1200.15 Encryption of Nonpublic Information.

(a) As part of its cybersecurity program, based on its risk assessment, each covered entity must implement

controls, including encryption, to protect nonpublic information held or transmitted by the covered entity both in transit over external networks and at rest.

(1) To the extent a covered entity determines that encryption of nonpublic information in transit over external networks is not feasible, the covered entity may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the covered entity's CISO.

(2) To the extent a covered entity determines that encryption of nonpublic information at rest is not feasible, the covered entity may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the covered entity's CISO.

(b) To the extent that a Covered Entity is utilizing compensating controls under subdivision (a) of this section, the feasibility of encryption and effectiveness of the compensating controls must be reviewed by the CISO at least yearly.

Section 1200.16 Incident Response Plan.

(a) As part of its cybersecurity program, each covered entity must establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity incident.

(b) Such incident response plan must, at a minimum, address the following areas:

(1) the goals of the incident response plan;

(2) the definition of clear roles, responsibilities and levels of decision-making authority;

(3) the internal processes for responding to a cybersecurity incident;

(4) the internal processes for recovering from a cybersecurity incident;

(5) external and internal communications and information sharing;

(6) use of a qualified third-party forensic investigator as required by section 1200.19 of this Part.

(7) planning to recover information technology to normal operations in a way that minimizes disruption to customers;

(8) identification of requirements for the remediation of any identified weaknesses in information technology and associated controls;

(9) documentation and reporting regarding cybersecurity incidents and related incident response activities;

(10) segmentation of information technology from operational technology during a cybersecurity incident; and

(11) the evaluation and revision, as necessary, of the incident response plan following a cybersecurity incident.

(c) At least yearly, each covered entity must conduct a test of the cybersecurity incident response plan through, at minimum, a tabletop or other exercise simulating a network breach and compromise of nonpublic information and update the plan based on the results within 90 days of said testing.

(d) All documentation and information relevant to the covered entity's incident response plan must be made available to the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee, within 10 calendar days of a request.

Section 1200.17 Audits by Department Staff

(a) Not more than yearly, covered entities are required to submit to cybersecurity audits by staff of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness upon request.

(b) Audits will be conducted according to rubrics updated at least once every two years at the direction of the Director of the Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee.

(c) Covered entities must make available for inspection by Staff of the Department of Public Service all physical and digital assets necessary to prepare their audits upon request within 10 calendar days of a request.

(d) Covered entities should make best efforts to correct any deficiencies noted in a departmental audit.

Section 1200.18 Third Party Audits

(a) On a yearly basis, covered entities must cause to be conducted a third-party audit of the cybersecurity of their information technology and nonpublic information. Such third-party audits must, at a minimum, assess:

(1) the level of executive level leadership and support for customer privacy related to cybersecurity;

(2) policies and procedures related to protection of nonpublic information and customer privacy;

(3) the quality of data network security (including intrusion detection and intrusion protection, network access controls, and data loss prevention tools);

(4) the sufficiency of segregation of customer data from other business systems;

(5) training and employee threat awareness education regarding cyber threats to the security of customer data;

(6) the adequacy of limitations on access to customer data by vendors and consultants;

(7) physical security for the protection of data systems;

(8) post-incident response and recovery protocols and drills for a suspected or known cybersecurity incident;

(9) supply chain risk and third party risk;

(10) the covered entity's ability to effectively segment its information technology from its operational technology during a cybersecurity incident; and

(11) compliance with the requirements of this Part.

(b) The third-party audit must be conducted by a qualified auditor.

(c) The yearly third-party audit must be made available to the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee no later than September 15 of each year.

(d) Covered entities should make best efforts to correct any deficiencies noted in the yearly third-party audit.

Section 1200.19 Forensic Investigations

(a) Each covered entity must establish a contractual relationship with a qualified third-party vendor to conduct forensic investigations into a cybersecurity incident or a suspected cybersecurity incident.

(b) In the event of a suspected cybersecurity incident, the covered entity must conduct a forensic investigation. As part of this investigation, the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness may require the covered entity to include its third-party vendor.

(c) At the completion of a forensic investigation the covered entity must cause a report to be prepared. Said report must be made available to the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee, within 10 calendar days of a request.

(d) Covered entities should make best efforts to correct any deficiencies noted in the report.

Section 1200.20 Credit Monitoring

(a) Each covered entity must establish a contractual relationship with a credit monitoring service for use in the event of a possible compromise of private information, as defined in paragraph b of subdivision 1 of section 899-aa of General Business Law. Such credit monitoring service must, at a minimum, have the ability to:

(1) track changes to a customer's credit files at all major credit reporting bureaus;

(2) alert the customer to new accounts, inquiries, delinquencies, or other suspicious activities;

(3) alert the customer to the use of the social security number associated with said customer;

(4) monitor the dark web for compromised data and alert the customer to it.

(b) Whenever a covered entity is required to make notice to any person of a breach in the security of its system as required by subdivision 2 of section 899-aa of General Business Law it must also notify said person of

the availability of credit monitoring pursuant to this Part.

(c) Said credit monitoring will be paid for by the covered entity, its insurance carrier, a third-party vendor, or other responsible party, as applicable, for no less than one year from the date of offer.

Section 1200.21 Notices

(a) Notice of Cybersecurity Incident. Each covered entity must notify the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee, as promptly as possible but in no event later than 72 hours after the covered entity reasonably believes a cybersecurity incident affecting the information technology or on public information of the covered entity or those of an affiliate, or those of a third party provider has occurred or is occurring.

(b) Notwithstanding the provisions of subdivision (a) of this section, each covered entity is required to maintain a log of all cybersecurity events and cybersecurity incidents, regardless of whether the events are subject to the notice requirements of subdivision (a), for a period of no fewer than three calendar years. All documentation and information relevant to the covered entity's cybersecurity events or cyber incidents log must be made available to the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee, within 10 calendar days of a request.

(c) Yearly, each covered entity must submit to the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee, a written statement covering the prior calendar year. This statement must be submitted by June 30, in such form set forth as Appendix 18 of this Title, certifying that the covered entity is in compliance with the requirements set forth in this Part. Each covered entity must maintain for examination by the department all records, schedules and data supporting this certificate for a period of five years. To the extent a covered entity has identified areas, systems or processes that require material improvement, updating or redesign, the covered entity must document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be made available for inspection by the director, or designee, within 10 calendar days of a request.

Section 1200.22 Confidentiality.

Information provided by a covered entity pursuant to this Part is subject to exemptions from disclosure under the Public Service Law, Public Officers Law or any other applicable State or Federal law.

Section 1200.23 Exemptions.

(a) Notwithstanding any other Part of these regulations, a covered entity that does not directly or indirectly operate, maintain, utilize or control any information technology, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess nonpublic information is exempt from the requirements of sections 1200.2, 1200.3, 1200.4, 1200.5, 1200.7, 1200.8, 1200.10, 1200.12, 1200.14, 1200.15, 1200.16, and 1200.18 of this Part.

(1) A covered entity that qualifies for the above exemption pursuant to this section will file a Notice of Exemption in the form set forth as Appendix 19 of this Title within 30 days of the determination that the covered entity is exempt.

(2) In the event that a covered entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such covered entity will have 180 days from such fiscal year end to comply with all applicable requirements of this Part.

Section 1200.24 Effective Date.

This Part will be effective June 1, 2026. Covered Entities will be required to yearly prepare and submit to the Director of the Department of Public Service's Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee, a Certification of Compliance under section 1200.21(c) of this Part commencing June 30, 2027.

Section 1200.25 Transitional Periods.

(a) Transitional Period. Covered entities have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.

(b) There is no transitional period to comply with the requirements of section 1200.21 of this Part.

(c) The following provisions include additional transitional periods. Covered entities will have:

(1) One year from the effective date of this Part to comply with the requirements of sections 1200.4(b), 1200.5, 1200.9, 1200.11, 1200.12, and 1200.14(b) of this Part.

(2) Eighteen months from the effective date of this Part to comply with the requirements of sections 1200.6, 1200.8, 1200.13, 1200.14 (a) and 1200.15 of this Part.

Section 1200.26 Severability.

If any provision of this Part or the application thereof to any person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment will not affect or impair the validity of the other provisions of this Part or the application thereof to other persons or circumstances.

APPENDIX 18 (Part 1200)

(Covered Entity Name)

June 30, 20_____

Certification of Compliance with New York State Public Service Commission Information Technology Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended (year for which Board Resolution or Compliance Finding is provided) complies with Part 1200 of Title 16 of the New York Code of Rules and Regulations.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)_____ Date:_____

[DMM Portal Filing Instructions]

APPENDIX 19 (Part 1200)

(Covered Entity Name) (Date)

Notice of Exemption

In accordance with 16 NYCRR § 1200.21(a), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for partial exemption under 16 NYCRR § 1200.21(a):

If you have any question or concerns regarding this notice, please contact:

(Insert name, title, and full contact information)

(Name) Date:

(Title)

(Covered Entity Name)

[DMM Portal Filing Instructions]