STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

At a session of the Public Service Commission held in the City of Albany on June 12, 2025

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.

ORDER INSTITUTING PROCEEDING TO ESTABLISH CYBERSECURITY RULES FOR INFORMATION TECHNOLOGY

(Issued and Effective June 13, 2025)

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. One area of concern has been the increasing frequency and sophistication of threats targeting Information Technology (IT) containing sensitive electronic data, including Personally Identifiable Information (PII). Cybercriminals can cause significant financial losses for companies as well as for consumers whose private information may be revealed or stolen for illicit purposes. As it contains

critical infrastructure, the utility sector is a significant target of cybersecurity threats.

The ever-changing, ever-increasing threat environment has moved the Commission to require more stringent IT cybersecurity practices over time via issuance of occasional Orders. It has moved the State Legislature to memorialize 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 data.[1] And it moved Governor Hochul to call for State agencies -- including this one -- to strengthen cybersecurity regulation for water infrastructure in her 2025 State of the State message.[2]

In December 2024, the Commission adopted a report addressing the cybersecurity threat landscape for utility companies in New York State and recommending promulgation of a "specific set of mandatory, enforceable, minimum requirements for utility IT system cybersecurity programs, policies, and governance."[3] The time has come for comprehensive cybersecurity regulations for all regulated industries. This Order is a first step in that process.

---

[1] 2023 Sess. Law News of N.Y. Ch. 67 (A. 2896). See also Public Service Law §66(30).

[2] 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).

[3] Case 24-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.

BACKGROUND

New York has long recognized the necessity of cybersecurity for the protection of critical infrastructure. In the aftermath of the September 11, 2001 attacks, the Commission ordered utilities to retain consultants to evaluate both their physical and cybersecurity.[4] It also formed an office of utility security within the Department of Public Service, which was later renamed the Office of Resilience, Utility Security, Nuclear Affairs, and Emergency Preparedness.[5] In the years since 2001, the Commission has revisited cybersecurity in numerous orders, outlining rules for PII and general IT security, among

[4] Case 02-M-0953, Proceeding on Motion of the Commission as to Telephone and Energy Utility Arrangements for Safeguarding the Security of Their Physical Equipment and Cyber Systems, Order Instituting Proceeding and Establishing Procedures for Preparation of Security Evaluations (issued Aug. 2, 2002), p. 1.

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

other actions.[6] In 2022 and 2023, the Legislature passed and Governor Hochul signed into law two bills that became Public Service Law § 66(30),[7] underscoring the Commission's authority over cybersecurity for gas and electric companies.

Broadly, the sector's technologies can be categorized into two types: Information Technology (IT) and Operational Technology (OT). IT comprises "any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information,"[8] including

[6] See, e.g., Order Adopting Minimum Functional Requirements for Advanced Metering Infrastructure Systems and Initiating an Inquiry Into Benefit-Cost Methodologies (issued Feb. 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 09-M-0074, In the Matter of Advanced Metering Infrastructure, p.4; 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 Oct. 17 ,2019), pp. 50-64.; 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).

[7] 2022 Sess. Law News of N.Y. Ch. 743 (A. 3904-B); 2023 Sess. Law News of N.Y. Ch. 67 (A. 2896).

[8] 40 U.S.C. §11101.

systems 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 systems.[11]

The potential impacts of a cyberattack vary across IT and OT systems depending upon how the systems are designed, built, managed, and maintained. In the typical IT cyberattack, the goal is data theft or disabling of business systems.[12] A successful attack on utility IT systems could cause major disruptions for the utility, customers, and the financial sector.[13] An IT breach that results in the theft of PII can be particularly painful for individual customers: credit cards, social security numbers, bank routing numbers, and other

---

[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.

[11] Id.

[12] Robert M. Lee and Tim Conway, SANS Institute, The Five ICS Cybersecurity Critical Controls 6, https://sansorg.egnyte.com/dl/R0r9qGEhEe (last accessed October 19, 2024).

[13] IBM, Cost of a Data Breach Report 2024, available at https://www.ibm.com/reports/data-breach (last accessed May 27, 2025).

sensitive information taken by threat actors can result in devastating financial losses.[14]

Cybersecurity breaches of OT could result in disabling critical infrastructure itself: electric, gas, water, telecommunications, or the cable systems that deliver the modern internet. While IT systems and OT systems are distinct, IT cybersecurity is intertwined with OT cybersecurity in today's world. As OT systems have become more and more interconnected, "they have begun to resemble IT systems" in their system architecture and design.[15] This continuing convergence of IT and OT has had predictable results; one estimate is that three-quarters of cyberattacks impacting OT systems originated as IT attacks.[16] For this reason, a comprehensive OT cybersecurity plan must also address IT, and a comprehensive IT cybersecurity plan must also address the need to segment connections between IT and OT systems in the event of a cyberattack.

---

[14] According to the National Institute of Standards and Technology (NIST), "Breaches involving PII are hazardous to both individuals and organizations. Individual harms may include identity theft, embarrassment, or blackmail. Organizational harms may include a loss of public trust, legal liability, or remediation costs." NIST, Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), ES-1 (2010), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf (last accessed May 27, 2025).

[15] NIST, Guide to Operational Technology (OT) Security 1 (2023), https://doi.org/10.6028/NIST.SP.800-82r3 (last accessed May 27, 2025).

[16] 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).

Since the Commission's first orders touching upon cybersecurity over twenty years ago, cyberattacks against critical infrastructure have been characterized by every-increasing "frequency and sophistication."[17] Potential threat actors range from small, financially-motivated groups to state-sponsored Advanced Persistent Threats (APTs), strategically positioning themselves in the event of geopolitical or military conflict.[18] The Commission appreciates that many regulated utilities have proactively increased their cybersecurity programs with great success. However, given the increased and increasing threats to cybersecurity, mandatory, minimum, enforceable standards are warranted. Such standards must be strong enough to meet today's threats while remaining agile enough to adapt to new ones.

The draft regulations (Attachment A) proposed by this Order are a first step in accomplishing these goals. The Commission intends first to promulgate rules to regulate the IT systems of all regulated utilities as well as cable television

[17] 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).

[18] 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).

companies. Subsequent Orders will propose OT regulations for various utility sectors.

LEGAL AUTHORITY

The draft IT regulations are intended to govern the IT systems of "covered entities," which the draft defines as including all public utility companies as well as cable television companies, with certain exceptions based on size. 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.[19] Those companies are required to provide safe and adequate service to their customers at just and reasonable rates.[20] 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.[21] 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. Additionally, the Commission 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."[22] Given the potential financial impact of a successful cyberattack, adequate IT cybersecurity is crucial to ensure consumer protection and just and reasonable rates, and it is

[19] Public Service Law §66(1).
[20] Public Service Law §65(1)-(2).
[21] Public Service Law §66(5).
[22] Public Service Law §66(2).

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 regulations and regulations to protect customer privacy.[23] 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."[24] 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.[25] Taken together, Article 89 of the Public Service Law has been recognized as "a comprehensive scheme for the regulation of water companies and

---

[23] 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.

[24] Public Service Law §89-b(1).

[25] Public Service Law §89-b(4).

for the fixing of rates."[26] For the same 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.[27] As with gas and electric corporations, the Commission maintains "general supervision" over steam corporations.[28] 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."[29] 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.[30] For the same reasons that similar provisions justify IT regulations for gas and electric, they justify IT regulations for steam.

Similar to other public utilities, the Public Service Law mandates that telephone corporations provide "adequate" service to their customers at "just and reasonable" rates.[31] The Commission has general supervision of all telephone corporations in the State and is charged with keeping informed as to the safety of those companies' lines and property and how they are operated and managed.[32] When the Commission is of the opinion that the practices of a telephone company are "inadequate, inefficient, improper or insufficient" the Commission may

---

[26] City of New York v. Maltbie, 274 N.Y. 90, 96 (1937).
[27] Public Service Law §79(1).
[28] Public Service Law §80(1).
[29] Public Service Law §80(2).
[30] Public Service Law §80(4).
[31] Public Service Law §91(1)
[32] Public Service Law §94(2).

promulgate "proper regulations, practices, equipment and service… to be observed and used…."[33] For the same reasons similar provisions justify IT regulations for gas and electric, they justify IT regulations for telephone service.

The Public Service Law's treatment of cable television companies is unique; they are not treated as public utilities.[34] Nevertheless, these companies are still required to provide safe, adequate, and reliable service to customers.[35] The Commission is charged with prescribing standards that promote "safe, adequate and reliable [cable] service to subscribers" and the operation of systems "consistent with the most advanced state of the art."[36] In order to do this, the Commission may "establish minimum specifications for equipment, service and safety of cable television systems for use by municipalities."[37] Finally, as it relates specifically to IT and PII, the Commission may adopt rules "providing consumer protections to customers of cable television companies, as the commission deems necessary and proper."[38] The Commission may promulgate rules and regulations as it finds necessary to carry out its purposes.[39] For the same reasons similar provisions justify IT regulations for gas and electric, they justify IT regulations for cable television corporations. In addition, the need to protect consumer privacy, including PII, further justifies and provides authority for regulations of cable television corporations' IT systems.

---

[33] Public Service Law §97(2).
[34] Public Service Law §2(23).
[35] Public Service Law §224(1).
[36] Public Service Law §215(2)(d)(i)-(ii).
[37] Public Service Law §215(2)(4).
[38] Public Service Law §224-a(8).
[39] Public Service Law §216(1).

NOTICE OF PROPOSED RULEMAKING

In accordance with section 202(1) of the State Administrative Procedure Act, the Commission is required to submit a Notice of Proposed Rulemaking to the Secretary of State for publication in the State Register and to provide an opportunity for public comment of no less than sixty days prior to final adoption of regulations.

DISCUSSION AND CONCLUSION

While the risk of a cyberattack cannot be entirely eliminated, sound cybersecurity begins by identifying an organization's cybersecurity risk profile -- the assets it holds, the threats it faces, its organizational priorities, etc.[40] Proactive analysis allows an organization to protect its assets by effectively addressing identified risks to prevent or lower the likelihood of an adverse impact from a cyberattack.[41] It may do this using strategies like access control, data encryption, and organization-specific cybersecurity training.[42] But it is not enough to simply train for threats. Robust cybersecurity requires constant vigilance to timely detect threats and attacks so that they may be responded to quickly.[43] This type of surveillance is core to modern cybersecurity. Once a cyberattack is detected, an organization must be ready to respond swiftly to contain any deleterious effects by, for

[40] NIST, The NIST Cybersecurity Framework (CSF) 2.0 at 2, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (last accessed May 27, 2025).
[41] Id.
[42] Id.
[43] Id. at 3.

example, segmenting IT and OT systems.[44] Finally, critical infrastructure organizations must plan to recover from a cyberattack by restoring normal operations in a safe, timely, and efficient manner to minimize any disruptions.[45] The thread woven through this entire framework is governance; an organization whose governance structure takes cybersecurity threats seriously and empowers qualified staff will achieve the best results.[46]

The draft regulations obligate covered entities to adopt sound, risk-based cybersecurity practices to mitigate their risk-of and risk-from a cyberattack. The draft requires each covered entity to assess its specific risk profile and to design a cybersecurity program that addresses those risks in a robust fashion. The draft requires covered entities to protect their IT systems using generally accepted access controls and authentication practices, and it further requires these entities to take affirmative steps to detect network intrusions. Finally, the draft regulations require covered entities to plan both to respond to and recover from cyber incidents. These plans are to be developed and implemented by a qualified Chief Information Security Officer employed for this purpose.

Senior management must take this issue seriously, assume responsibility for the organization's cybersecurity program, and file an annual certification confirming compliance with the draft regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers' private information.

The Commission recognizes that it could be difficult

[44] Id.
[45] Id.
[46] Id. at 2.

for small service providers to comply with these requirements. For this reason, the draft regulations generally exempt small utilities and cable television companies. At some future time, the Commission anticipates promulgating cybersecurity regulations for smaller providers.

The draft regulations represent a significant step in meeting the Commission's long-term goal to strengthen the cybersecurity of all entities within the Commission's jurisdiction, in line with the broader New York State Cybersecurity Strategy announced by Governor Hochul in August 2023.[47] 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 orders:

1. A proceeding is initiated to establish cybersecurity rules for information technology for public utilities and cable television companies.

2. Interested stakeholders must file comments no later than September 15, 2025.

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

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

4. This proceeding is continued.

By the Commission,

(SIGNED) MICHELLE L. PHILLIPS
Secretary

ATTACHMENT A

Chapter XII. Regulated Entity Security

Subpart 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 twenty-three of section two of the Public Service Law or any cable television company as defined in subdivision one of section two-hundred and twenty-one of the Public Service Law, except:

(1) A water-works corporation, as defined in subdivision twenty-six of section two of the Public Service Law serving fewer than fifty-thousand service connections, as defined in subdivision c of section five hundred and one point one of this Title;

(2) A cable television company, as defined in subdivision one of section two-hundred and twenty-one of the Public Service Law, with fewer than fifty-thousand subscribers;

(3) An electric corporation, as defined in subdivision thirteen of section two of the Public Service Law, maintaining fewer than fifty-thousand service lines, as defined in subdivision b of section ninety-eight point one of this Title;

(4) A gas corporation, as defined in subdivision eleven of section two of the Public Service Law, that constitutes a small business as defined in subdivision eight of section one-hundred and two of State Administrative Procedure Law;

(5) A telephone corporation, as defined in subdivision seventeen of section two of the Public Service Law, servicing fewer than fifty-thousand access customers;

(6) Any person operating solely as a telegraph corporation, as defined in subdivision nineteen of section two of the Public Service Law;

(7) A municipal corporation as defined in section one hundred nineteen-n of the General Municipal Law;

(8) 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) 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 (i) federal, state or local government records; (ii) widely distributed media; or (iii) 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 (i) is not an Affiliate of a Covered Entity, (ii) provides services to a Covered Entity, and (iii) 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 seven 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 seven 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 annually, 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 at least every eighteen months based on relevant identified risks in accordance with the Risk Assessment; and

(2) bi-annual 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.

(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 seven 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 paragraph (a) of this section for not fewer than five 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 yearly and assessed and updated as necessary by the CISO (or a designee) of the Covered Entity.

Section 1200.9 Risk Assessment.

(a) At least yearly, 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 seven 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 yearly 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 regular 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 (a) above, the feasibility of encryption and effectiveness of the compensating controls must be reviewed by the CISO at least annually.

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 biannually, 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 seven 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 biannually at the direction of the Director of the Office of Resilience, Utility Security, Nuclear Affairs and Emergency Preparedness, or designee.

(c) Staff of the Department of Public Service are to be granted physical and digital access to all assets of Covered Entities to prepare their audits upon request within seven 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 an annual 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 annual third-party audit must be filed with the Commission no later than September 15 of each year.

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

Section 1200.19 Third Party Forensic Investigation

(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 Covered Entity must 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 seven 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 one of section eight hundred and ninety-nine 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 two of section eight hundred and ninety-nine 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 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 Non-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 (a), 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 (a), for a period of no fewer than five calendar years. All documentation and information relevant to the Covered Entity's Cybersecurity Event 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 seven calendar days of a request

(c) Annually, 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 seven 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, 1200.6, 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 January 1, 2026. Covered Entities will be required to annually 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) 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, 1200.12, 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.

(3) Two years from the effective date of this Part to comply with the requirements of section 1200.11 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 § 1200.23(a)(1), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for partial exemption under 16 NYCRR § 1200.23(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]