NEW YORK STATE | Department of Public Service

KATHY HOCHUL
Governor

RORY M. CHRISTIAN
Chief Executive Officer

January 20, 2026

Honorable Kathy Hochul
Governor of New York State
New York State Capitol Building
Albany, NY 12224

Re: Case 25-M-0302 - In the Matter of the Rules and Regulations of the Public Service Commission, Contained in 16 NYCRR – Proposed Information Technology Cybersecurity Requirements.

Dear Governor Hochul:

Enclosed is a copy of the Notice of Revised Rulemaking concerning a proposal by the New York State Public Service Commission (Commission) to add a new Chapter XII, Subchapter A, Part 1200 (Information Technology Cybersecurity Requirements for Covered Entities) to Title 16 of the New York Code of Rules and Regulation. Also enclosed are the revised rule text, revised regulatory impact statement, revised regulatory flexibility analysis, revised rural area flexibility analysis, and revised job impact exemption.

These documents are transmitted to you in accordance with State Administrative Procedure Act §202(6-a) and Executive Law §101-a.

The statutory authority for the proposed regulations is Public Service Law Section §§ 65 (1), 66(1), (2), (5), 19(d), & (30), 89-b(1), 89-c(4) & (15), 79(1), 80(1), (2), & (4). A public hearing is not scheduled. Public comments will be received for a minimum of 45 days after publication of a summary of the proposed regulations in the State Register. The public may submit comments to the Hon. Michelle L. Phillips, Secretary to the Commission, at 3 Empire State Plaza, Albany, New York 12223-1350, to secretary@dps.ny.gov or to http://www.dps.ny.gov under Case 25-M-0302.

Very truly yours,

Assistant Counsel

Enc.

NEW YORK STATE | Department of Public Service

KATHY HOCHUL
Governor

RORY M. CHRISTIAN
Chief Executive Officer

January 20, 2026

The Honorable Andrea Stewart-Cousins
President Pro Tempore
New York State Senate
Legislative Office Building, Room 907
Albany, New York 12247

Re: Case 25-M-0302 - In the Matter of the Rules and Regulations of the Public Service Commission, Contained in 16 NYCRR – Proposed Information Technology Cybersecurity Requirements.

Dear Senator Stewart-Cousins:

Enclosed is a copy of the Notice of Revised Rulemaking concerning a proposal by the New York State Public Service Commission (Commission) to add a new Chapter XII, Subchapter A, Part 1200 (Information Technology Cybersecurity Requirements for Covered Entities) to Title 16 of the New York Code of Rules and Regulation. Also enclosed are the revised rule text, revised regulatory impact statement, revised regulatory flexibility analysis, revised rural area flexibility analysis, and revised job impact exemption.

These documents are transmitted to you in accordance with State Administrative Procedure Act §202(6-a) and Executive Law §101-a.

The statutory authority for the proposed regulations is Public Service Law Section §§ 65 (1), 66(1), (2), (5), 19(d), & (30), 89-b(1), 89-c(4) & (15), 79(1), 80(1), (2), & (4). A public hearing is not scheduled. Public comments will be received for a minimum of 45 days after publication of a summary of the proposed regulations in the State Register. The public may submit comments to the Hon. Michelle L. Phillips, Secretary to the Commission, at 3 Empire State Plaza, Albany, New York 12223-1350, to secretary@dps.ny.gov or to http://www.dps.ny.gov under Case 25-M-0302.

Very truly yours,

Assistant Counsel

Enc.

NEW YORK STATE | Department of Public Service

KATHY HOCHUL
Governor

RORY M. CHRISTIAN
Chief Executive Officer

January 20, 2026

The Honorable Carl E. Heastie
Speaker of the Assembly
Legislative Office Building, Room 932
Albany, New York 12248

Re: Case 25-M-0302 - In the Matter of the Rules and Regulations of the Public Service Commission, Contained in 16 NYCRR – Proposed Information Technology Cybersecurity Requirements.

Dear Speaker Heastie:

Enclosed is a copy of the Notice of Revised Rulemaking concerning a proposal by the New York State Public Service Commission (Commission) to add a new Chapter XII, Subchapter A, Part 1200 (Information Technology Cybersecurity Requirements for Covered Entities) to Title 16 of the New York Code of Rules and Regulation. Also enclosed are the revised rule text, revised regulatory impact statement, revised regulatory flexibility analysis, revised rural area flexibility analysis, and revised job impact exemption.

These documents are transmitted to you in accordance with State Administrative Procedure Act §202(6-a) and Executive Law §101-a.

The statutory authority for the proposed regulations is Public Service Law Section §§ 65 (1), 66(1), (2), (5), 19(d), & (30), 89-b(1), 89-c(4) & (15), 79(1), 80(1), (2), & (4). A public hearing is not scheduled. Public comments will be received for a minimum of 45 days after publication of a summary of the proposed regulations in the State Register. The public may submit comments to the Hon. Michelle L. Phillips, Secretary to the Commission, at 3 Empire State Plaza, Albany, New York 12223-1350, to secretary@dps.ny.gov or to http://www.dps.ny.gov under Case 25-M-0302.

Very truly yours,

Assistant Counsel

Enc.

NEW YORK STATE | Department of Public Service

KATHY HOCHUL
Governor

RORY M. CHRISTIAN
Chief Executive Officer

January 20, 2026

The Honorable Sam Sutton
Chair, Administrative Regulations Review Commission
Legislative Office Building, Room 809
Albany, NY 12247

Re: Case 25-M-0302 - In the Matter of the Rules and Regulations of the Public Service Commission, Contained in 16 NYCRR – Proposed Information Technology Cybersecurity Requirements.

Dear Chairperson Sutton:

Enclosed is a copy of the Notice of Revised Rulemaking concerning a proposal by the New York State Public Service Commission (Commission) to add a new Chapter XII, Subchapter A, Part 1200 (Information Technology Cybersecurity Requirements for Covered Entities) to Title 16 of the New York Code of Rules and Regulation. Also enclosed are the revised rule text, revised regulatory impact statement, revised regulatory flexibility analysis, revised rural area flexibility analysis, and revised job impact exemption.

These documents are transmitted to you in accordance with State Administrative Procedure Act §202(6-a) and Executive Law §101-a.

The statutory authority for the proposed regulations is Public Service Law Section §§ 65 (1), 66(1), (2), (5), 19(d), & (30), 89-b(1), 89-c(4) & (15), 79(1), 80(1), (2), & (4). A public hearing is not scheduled. Public comments will be received for a minimum of 45 days after publication of a summary of the proposed regulations in the State Register. The public may submit comments to the Hon. Michelle L. Phillips, Secretary to the Commission, at 3 Empire State Plaza, Albany, New York 12223-1350, to secretary@dps.ny.gov or to http://www.dps.ny.gov under Case 25-M-0302.

Very truly yours,

Assistant Counsel

Enc.

NEW YORK STATE | Department of Public Service

KATHY HOCHUL
Governor

RORY M. CHRISTIAN
Chief Executive Officer

January 20, 2026

The Honorable Jonathan Rivera
Chair, Administrative Regulations Review Commission
Legislative Office Building, Room 540
Albany, NY 12247

Re: Case 25-M-0302 - In the Matter of the Rules and Regulations of the Public Service Commission, Contained in 16 NYCRR – Proposed Information Technology Cybersecurity Requirements.

Dear Chairperson Rivera:

Enclosed is a copy of the Notice of Revised Rulemaking concerning a proposal by the New York State Public Service Commission (Commission) to add a new Chapter XII, Subchapter A, Part 1200 (Information Technology Cybersecurity Requirements for Covered Entities) to Title 16 of the New York Code of Rules and Regulation. Also enclosed are the revised rule text, revised regulatory impact statement, revised regulatory flexibility analysis, revised rural area flexibility analysis, and revised job impact exemption.

These documents are transmitted to you in accordance with State Administrative Procedure Act §202(6-a) and Executive Law §101-a.

The statutory authority for the proposed regulations is Public Service Law Section §§ 65 (1), 66(1), (2), (5), 19(d), & (30), 89-b(1), 89-c(4) & (15), 79(1), 80(1), (2), & (4). A public hearing is not scheduled. Public comments will be received for a minimum of 45 days after publication of a summary of the proposed regulations in the State Register. The public may submit comments to the Hon. Michelle L. Phillips, Secretary to the Commission, at 3 Empire State Plaza, Albany, New York 12223-1350, to secretary@dps.ny.gov or to http://www.dps.ny.gov under Case 25-M-0302.

Very truly yours,

Assistant Counsel

Enc.

VERIFIED Validate

For Department of State use only.

Notice of Revised Rule Making

Public Service Commission
(SUBMITTING AGENCY)

[x] Approval has been granted by Executive Chamber to propose this rule making.
[ ] This rule making does not require Executive Chamber approval.

NOTE: Typing and submission instructions are at the end of this form. Please be sure to COMPLETE ALL ITEMS. Incomplete forms will be cause for rejection of this notice.

1. Proposed action:

Addition of Chapter XII, Subpart A, Part 1200 Title 16 NYCRR

_____ _____ Title_____ NYCRR

_____ _____ Title_____ NYCRR

_____ _____ Title_____ NYCRR

_____ _____ Title_____ NYCRR

_____ _____ Title_____ NYCRR

2. Statutory authority under which the rule is proposed:

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

3. Subject of the rule:

Institution of mandatory, minimum, enforceable cybersecurity rules for information technology.

4. Purpose of the rule:

To protect private customer data, minimize financial risks of cyber attacks, and fulfill statutory mandates.

5. Terms of rule (SELECT ONE):

[ ] The full text of the rule is attached because it does not exceed 2,000 words.

[x] A summary of the rule is attached because the full text of the rule exceeds 2,000 words.

[x] Full text is posted on the following State website. [Pursuant to SAPA §202(7)(d), provide sufficient information to enable the public to access the full text without extensive searching. For example, provide a URL or a title to either a webpage or a specific section of the website where the full text is posted]:

https://documents.dps.ny.gov/public/MatterManagement/CaseMaster.aspx?MatterCaseNo=25-m-0302&CaseSearch=Search

6. *Public hearings* (check box and complete as applicable):

[x] NO public hearing is scheduled. (*SKIP TO ITEM 9*)

[ ] A public hearing is required by law and is scheduled as indicated below. (***Note***: first hearing date must be at least 60 days **after** publication of this notice unless a different time is specified in statute.)

[ ] A public hearing is not required by law, but is scheduled as indicated below.

Time:	*Date:*	*Location:*

7. Interpreter services (check only if a public hearing is scheduled):

[ ] Interpreter services will be made available to hearing impaired persons, at no charge, upon written request to the agency contact designated in this notice.

8. Accessibility (check appropriate box only if a public hearing is scheduled):

[ ] All public hearings have been scheduled at places reasonably accessible to persons with a mobility impairment.

[ ] Attached is a list of public hearing locations that are **not** reasonably accessible to persons with a mobility impairment. An explanation is submitted regarding diligent efforts made to provide accessible hearing sites.

9. Revised rule compared to proposed rule (identify **only** those changes made since the **last** published rule):

A. The original notice of **proposed** rule making was published in the *State Register* on 07/09/2025 , I.D. No. PSC-27-25-00021 - P

B. List the date and I.D. No. of any previously published notice(s) of **revised** rule making:

, I.D. No. -

, I.D. No. -

C. Substantial revisions were made in [Parts, sections, subdivisions or paragraphs]:

1200.1, 1200.3	1200.5, 1200.6	1200.8, 1200.9	1200.11, 1200.
1200.18	1200.20	1200.24	

10. The revised text of the rule and any required statements and analyses may be obtained from:

Agency contact Beth Faranda

Agency name New York State Department of Public Service

Office address 3 Empire State Plaza
Albany, New York 12223

Telephone (518) 474-5306 *E-mail* Beth.Faranda@dps.ny.gov

11. Submit data, views or arguments to (complete only if different than previously named agency contact):

Agency contact Hon. Michelle Phillips, Secretary to the Commission

Agency name Public Service Commission

Office address 3 Empire State Plaza
Albany, NY 12223-1350

Telephone (518) 474-6530 *E-mail* secretary@dps.ny.gov

12. Public comment will be received until:

[x] 45 days after publication of this notice [MINIMUM public comment period, SAPA §202(4-a)(a)]

[ ] 5 days after the last scheduled public hearing required by statute (MINIMUM, with required hearing).

[ ] Other: (*specify*)

13. Additional matter required by statute:

[ ] YES (include below material required by statute).

[x] NO additional material required by statute.

14. ***Revised Regulatory Impact Statement (RIS)***

(SELECT AND COMPLETE ONE; ALL ATTACHMENTS MUST BE 2,000 WORDS OR LESS, EXCLUDING SUMMARIES OF STUDIES, REPORTS OR ANALYSES [Needs and Benefits])

A. The attached Revised RIS contains:

[x] The full text of the Revised RIS.

[ ] A summary of the Revised RIS.

Full text is posted on the following State website. [Pursuant to SAPA §202(7)(d), provide sufficient information to enable the public to access the full text without extensive searching. For example, provide a URL or a title to either a webpage or a specific section of the website where the full text is posted]:

B. A **statement is attached** explaining why a Revised RIS is not required (check one box):

[ ] Changes made to the last published rule do not necessitate revision to the previously published RIS.

[ ] This is a technical amendment exempt from SAPA §202-a.

15. ***Revised Regulatory Flexibility Analysis (RFA) for small businesses and local governments***

(SELECT AND COMPLETE ONE; ALL ATTACHMENTS MUST BE 2,000 WORDS OR LESS)

A. The attached Revised RFA contains:

[x] The full text of the Revised RFA.

[ ] A summary of the Revised RFA.

Full text is posted on the following State website. [Pursuant to SAPA §202(7)(d), provide sufficient information to enable the public to access the full text without extensive searching. For example, provide a URL or a title to either a webpage or a specific section of the website where the full text is posted]:

B. A **statement is attached** explaining why a Revised RFA is not required (check one box):

[ ] Changes made to the last published rule do not necessitate revision to the previously published RFA.

[ ] The changes will not impose any adverse economic impact or reporting, recordkeeping or other compliance requirements on small businesses or local governments. The attached statement sets forth this agency's findings and the reason(s) upon which the findings were made, including what measures were used to determine those findings.

16. ***Revised Rural Area Flexibility Analysis (RAFA)***

(SELECT AND COMPLETE ONE; ALL ATTACHMENTS MUST BE 2,000 WORDS OR LESS)

A. The attached Revised RAFA contains:

[x] The full text of the Revised RAFA.

[ ] A summary of the Revised RAFA.

Full text is posted on the following State website. [Pursuant to SAPA §202(7)(d), provide sufficient information to enable the public to access the full text without extensive searching. For example, provide a URL or a title to either a webpage or a specific section of the website where the full text is posted]:

B. A **statement is attached** explaining why a revised RAFA is not required (check one box):

[ ] Changes made to the last published rule do not necessitate revision to the previously published RAFA.

[ ] The changes will not impose any adverse impact or reporting, recordkeeping or other compliance requirements on public or private entities in rural areas. The attached statement sets forth this agency's findings and the reason(s) upon which the findings were made, including what measures were used to determine those findings.

17. ***Revised Job Impact Statement (JIS)***

(SELECT AND COMPLETE ONE; ALL ATTACHMENTS MUST BE 2,000 WORDS OR LESS)

A. The attached Revised JIS contains:

[×] The full text of the Revised JIS.

[ ] A summary of the Revised JIS.

[ ] Full text is posted on the following State website. [Pursuant to SAPA §202(7)(d), provide sufficient information to enable the public to access the full text without extensive searching. For example, provide a URL or a title to either a webpage or a specific section of the website where the full text is posted]:

B. A **statement is attached** explaining why a revised JIS is not required (check one box):

[ ] Changes made to the last published rule do not necessitate revision to the previously published JIS.

[ ] The changes will not impose a substantial impact on jobs and employment opportunities. The attached statement sets forth this agency's findings that the rule will have a positive impact or no impact on jobs and employment opportunities; except when it is evident from the subject matter of the rule that it could only have a positive impact or no impact on jobs and employment opportunities, the statement shall include a summary of the information and methodology underlying that determination.

C. [ ] A revised JIS is **not** attached because this rule was proposed by the State Comptroller or Attorney General.

18. ***Assessment of Public Comment*** *(including legislative comment)* (CHECK ONE):

[×] Attached is an assessment of public comment.

No particular form is required, and it need **only** include comments not addressed in any previously published assessment of public comment for this rule. However, the assessment must be based on any written comments received by the agency and any comments presented at any public hearing held by the agency about this proposal. It must contain a summary and an analysis of the issues raised and significant alternatives suggested, a statement of the reason(s) why any significant alternatives were not incorporated, and a description of any changes made as a result of such comments. If the assessment exceeds 2,000 words, submit a summary.

[ ] An assessment is not attached because no comments were received.

AGENCY CERTIFICATION (To be completed by the person who PREPARED the notice)

I have reviewed this form and the information submitted with it. The information contained in this notice is correct to the best of my knowledge.

I have reviewed Article 2 of SAPA and Parts 260 through 263 of 19 NYCRR, and I hereby certify that this notice complies with all applicable provisions.

Name	Vincent Stark	*Signature*	
Address	3 Empire State Plaza, Albany, NY 12223		
Telephone	(518) 473-5234	*E-Mail*	vincent.stark@dps.ny.gov
Date	01/20/2026		

Please read before submitting this notice: Reset Form

- **SPECIAL NOTE: Actions proposed as a Consensus Rule Making cannot be revised.**

1. Except for this form itself, all text must be typed in the prescribed format as described in the Department of State's *Register* procedures manual, *Rule Making in New York.*

2. Rule making notices, with any necessary attachments (in MS Word), should be e-filed via the Department of State website.

DRAFT

Chapter XII. Regulated Entity Security

~~Subpart~~ 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 i~~I~~nformation t~~T~~echnology of companies supplying critical infrastructure. This includes systems handling sensitive electronic data, like p~~P~~ersonal i~~I~~dentifiable i~~I~~nformation, 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 ~~I~~information ~~T~~technology systems of large companies within the ~~C~~commission's jurisdiction. These regulations seek to protect both customer privacy as well as the broader integrity of i~~I~~nformation t~~T~~echnology. Adoption of a cybersecurity program as outlined in these regulations is a priority for the c~~C~~ommission and for the State of New York. For the companies covered by these regulations, existing c~~C~~ommission orders in conflict with it will be abrogated as the regulations are phased in. For smaller companies not covered by these regulations, existing c~~C~~ommission 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 p~~P~~erson that controls, is controlled by or is under common control with another p~~P~~erson. For purposes of this subdivision, control means direct or indirect authority to direct or cause the direction of the management and policies of a p~~P~~erson, whether through the ownership of stock of such p~~P~~erson or otherwise.

(b) *Authorized User* means any employee, contractor, agent or other p~~P~~erson that participates in the operations of a c~~C~~overed ~~E~~entity and is authorized to access and use any i~~I~~nformation t~~T~~echnology or data of the c~~C~~overed e~~E~~ntity.

(c) *Covered Entity* means any public utility company as defined in subdivision ~~twenty-three~~23 of section ~~two~~-2 of the Public Service Law~~ or any cable television company as defined in subdivision one-1 of section two-hundred and twenty-one221 of the Public Service Law,~~ except:

(1) aA water-works corporation, as defined in subdivision twenty-six26 of section two-2 of the Public Service Law serving fewer than fifty-thousand50,0001 service connections, as defined in subdivision (c) of section five-hundred-and-one-point-one501.1 of this Title;

(2) aA cable television company, as defined in subdivision one-1 of section two-hundred-and-twenty-one221 of the Public Service Law, with fewer than fifty-thousand50,000 subscribers;

(3)(2) Aan electric corporation, as defined in subdivision thirteen-13 of section two-2 of the Public Service Law, maintaining fewer than fifty-thousand50,000 service lines, as defined in subdivision (b) of section ninety-eight-point-one98.1 of this Title;

(4)(3) aA gas corporation, as defined in subdivision eleven-11 of section two-2 of the Public Service Law, that constitutes a small business as defined in subdivision eight-8 of section one-hundred-and-two102 of State Administrative Procedure Law;

(5)(4) Aa telephone corporation, as defined in subdivision seventeen-17 of section two-2 of the Public Service Law, servicing fewer than fifty-thousand50,000 access customers;

(6)(5) aAny person operating solely as a telegraph corporation, as defined in subdivision nineteen-19 of section two-2 of the Public Service Law;

(7)(6) aA municipal corporation as defined in section one-hundred-nineteen119-n of the General Municipal Law;

(8)(7) aAn employee, agent, representative or designee of a cCovered eEntity, who is itself a cCovered eEntity, provided that such employee, agent, representative or designee is covered by the cybersecurity program of the cCovered eEntity.

(d) *Cybersecurity Event* means

(1) any successful or unsuccessful attempt to gain unauthorized access to, disrupt or misuse iInformation tTechnology owned or controlled by a cCovered eEntity or information stored on such iInformation tTechnology; or

(2) the unauthorized dissemination, intentionally or unintentionally, of nonpublic information stored on iInformation tTechnology owned or controlled by a cCovered eEntity.

(e) *Cybersecurity Incident* means a cCybersecurity eEvent that

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

(2) actually or imminently jeopardizes the confidentiality, integrity or availability of the cCovered eEntity's iInformation tTechnology or the continuing functionality of any aspect of the cCovered eEntity's business or operations; or

(3) results in loss of operational data of the Ccovered Ecntity; or

(4) includes a demand for payment of a ransom to restore access to the cCovered eEntity's iInformation

tTechnology sSystem; or

(5) results in the dissemination of nonpublic information stored on iInformation tTechnology owned or controlled by a cCovered EEntity; 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 iInformation tTechnology does not include oOperational tTechnology.

(h) *Least Privilege* means the principle that a system should restrict the access privileges of aAuthorized uUsers (or processes acting on behalf of aAuthorized uUsers) 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) sSomething the user knows; or

(2) sSomething the user has; or

(3) sSomething the user is.

(j) *Nonpublic Information* means all electronic information that is not pPublicly aAvailable iInformation and is:

(1) bBusiness-related information of a cCovered EEntity 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 cCovered cEntity; or

(2) aAny 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) aAny (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) aAny 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 cCustomer consumption or use data.

(k) *Penetration Testing* means a test methodology during which assessors attempt to circumvent or defeat the security features of an iInformation Ttechnology system by attempting penetration of the system from outside or inside the cCovered eEntity's Information tTechnology 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 cCovered eEntity has a reasonable basis to believe is lawfully made available to the general public from (i) Ffederal, Sstate or local government records; (ii) widely distributed media; or (iii) disclosures to the general public that are required to be made by Ffederal, Sstate or local law.

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

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

(ii) wWhether 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 cCovered eEntity is required to conduct under section 1200.9 of this Part.

1200

(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, iInformation tTechnology, compliance and/or risk of a cCovered eEntity.

(q) *Third Party Service Provider(s)* means a pPerson that (1i) is not an Aaffiliate of a cCovered eEntity, (ii2) provides services to a cCovered eEntity, and (iii3) maintains, processes or otherwise is permitted access to nNonpublic Iinformation through its provision of services to a cCovered eEntity.

(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 cCovered eEntity must maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the cCovered eEntity's iinformation tTechnology.

(b) The cybersecurity program must be based on the cCovered eEntity's Rrisk aAssessment 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 nNonpublic iInformation stored on the cCovered eEntity's iInformation tTechnology;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the cCovered eEntity's iInformation tTechnology systems, and nNonpublic iInformation stored on those systems, from unauthorized access, use or other malicious acts;

(3) detect cCybersecurity eEvents;

(4) respond to identified or detected cCybersecurity eEvents to mitigate any negative effects;

(5) recover from cCybersecurity eEvents and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

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

(d) All documentation and information relevant to the cCovered eEntity'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~~ 10 calendar days of a request.

Section 1200.3 Cybersecurity Policy.

(a) Each Ccovered Ecntity must implement and maintain a written cybersecurity policy or policies, approved by a sSenior oOfficer, the Ccovered eEntity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the cCovered eEntity's policies and procedures for the protection of its iInformation tTechnology and nNonpublic iInformation. The cybersecurity policy must be based on the cCovered eEntity's rRisk aAssessment and must address the following areas to the extent applicable to the cCovered eEntity'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 tThird pParty sService pProvider management;

(15) risk assessment;

(16) incident response; and

(17) implementation of controls to allow segmentation of its iInformation tTechnology from its oOperational tTechnology in the event of a cCybersecurity iIncident.

(b) All documentation and information relevant to the cCovered cEntity's cybersecurity PpolicyPolicy 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~~ 10 calendar days of a request.

Section 1200.4 Chief Information Security Officer.

(a) Chief Information Security Officer. Each cCovered cEntity must designate a qualified individual responsible for overseeing and implementing the cCovered cEntity'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 cCovered cEntity, one of its aAffiliates or a tThird pParty SsService pProvider. To the extent this requirement is met using a tThird pParty sService pProvider or an aAffiliate, the cCovered cEntity must:

(1) retain responsibility for compliance with this Part;

(2) designate a senior member of the cCovered cEntity's personnel responsible for direction and oversight of the tThird pParty sService pProvider; and

(3) require the tThird pParty sService pProvider to maintain a cybersecurity program that protects the cCovered cEntity in accordance with the requirements of this Part.

(b) Report. At least ~~annually~~early, the CISO of each c~~C~~overed e~~E~~ntity must report in writing to the ~~C~~covered e~~E~~ntity'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 s~~S~~enior o~~O~~fficer of the c~~C~~overed e~~E~~ntity responsible for the c~~C~~overed e~~E~~ntity's cybersecurity program. The CISO must report on the c~~C~~overed e~~E~~ntity's cybersecurity program and material cybersecurity risks. The CISO must consider to the extent applicable:

(1) the confidentiality of n~~N~~onpublic i~~I~~nformation and the integrity and security of the ~~C~~covered e~~E~~ntity's i~~I~~nformation t~~T~~echnology;

(2) the c~~C~~overed e~~E~~ntity's cybersecurity policies and procedures;

(3) material cybersecurity risks to the c~~C~~overed e~~E~~ntity;

(4) the overall effectiveness of the c~~C~~overed e~~E~~ntity's cybersecurity program; and

(5) c~~C~~ybersecurity i~~I~~ncidents involving the c~~C~~overed e~~E~~ntity during the time period addressed by the report.

Section 1200.5 Continuous Monitoring, Penetration Testing and Vulnerability Assessments.

(a) The cybersecurity program for each c~~C~~overed e~~E~~ntity must include monitoring and testing, developed in accordance with the c~~C~~overed e~~E~~ntity's r~~R~~isk a~~A~~ssessment, designed to assess the effectiveness of the c~~C~~overed e~~E~~ntity's cybersecurity program. The monitoring and testing must include continuous monitoring or periodic p~~P~~enetration t~~T~~esting and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in i~~I~~nformation t~~T~~echnology that may create or indicate vulnerabilities, c~~C~~overed e~~E~~ntities must conduct:

(1) p~~P~~enetration t~~T~~esting of the c~~C~~overed e~~E~~ntity's i~~I~~nformation t~~T~~echnology ~~at least every eighteen 18 months~~ based on relevant identified risks in accordance with the ~~R~~risk a~~A~~ssessment at least every 12 months; and

(2) ~~bi-annual~~ vulnerability assessments, including any systematic scans or reviews of i~~I~~nformation t~~T~~echnology reasonably designed to identify publicly known cybersecurity vulnerabilities in the c~~C~~overed e~~E~~ntity's ~~I~~information Technology based on the Risk Assessment at least every 6 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 ~~seven~~ 10 calendar days of a request.

Section 1200.6 Audit Trail.

(a) Each c~~C~~overed ~~E~~entity must securely maintain systems that:

(1) are designed to reconstruct material changes to i~~I~~nformation t~~T~~echnology sufficient to reconstruct and restore normal operations of the c~~C~~overed e~~E~~ntity at the time of a c~~C~~ybersecurity i~~I~~ncident disrupting service; and

(2) include audit trails designed to detect and respond to c~~C~~ybersecurity i~~I~~ncidents that have a reasonable

likelihood of harming any part of the normal operations of the cCovered cEntity.

(b) Each cCovered cEntity must maintain audit trail records required by ~~paragraph~~ subdivision (a) of this section for not fewer than ~~five~~ three years.

Section 1200.7 Access Privileges.

(a) As part of its cybersecurity program, each cCovered cEntity must limit user access privileges to iInformation tTechnology that provides access to nNonpublic iInformation and must review such access privileges yearly based on the cCovered cEntity's rRisk aAssessment.

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

(c) Each cCovered cEntity must create a written policy to employ cElectronic mMasking of sensitive information, determining what information is masked for which aAuthorized uUsers according to the principle of lLeast Pprivilege.

Section 1200.8 Application Security.

(a) Each cCovered cEntity'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 cCovered Eentity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the cCovered cEntity within the context of the cCovered cEntity's technology environment.

(b) All such procedures, guidelines or standards must be reviewed, ~~yearly and~~ assessed, and updated at least once every two years ~~as necessary~~ by the CISO (or a designee) of the Ccovered cEntity.

Section 1200.9 Risk Assessment.

(a) At least once every two years~~yearly~~, each cCovered cEntity must conduct a rRisk aAssessment of the cCovered Eentity's iInformation tTechnology sufficient to inform the design of the cCybersecurity pProgram required by section 1200.2 of this Part. Such rRisk aAssessment should be updated as reasonably necessary to address changes to the cCovered cEntity's iInformation tTechnology, nNonpublic iInformation or business operations. The Ccovered cEntity's rRisk Aassessment should allow for revision of controls to respond to technological developments and evolving threats and should consider the particular risks of the cCovered cEntity's business operations related to cybersecurity, nNonpublic iInformation collected or stored, iInformation tTechnology utilized and the availability and effectiveness of controls to protect nNonpublic Iinformation and iInformation tTechnology.

(b) The rRisk aAssessment 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 cCovered cEntity;

(2) criteria for the assessment of the confidentiality, integrity, security, and availability of the cCovered

cEntity's iInformation tTechnology and Nnonpublic Iinformation, 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 rRisk aAssessment and how the cybersecurity program will address the risks.

(c) All documentation and information relevant to the cCovered Eentity's rRisk aAssessment 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~~ 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 cCovered cEntity must:

(1) utilize qualified cybersecurity personnel of the Ccovered cEntity, an aAffiliate or a tThird Pparty Sservice pProvider sufficient to manage the cCovered Ecntity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in sSection 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 cCovered cEntity may choose to utilize a qualified tThird pParty sService pProvider 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 cCovered cEntity must implement written policies and procedures designed to ensure the security of iInformation tTechnology and nNonpublic iInformation that are accessible to, or held by, tThird pParty sService pProviders or aAffiliates. Such policies and procedures should be based on the rRisk aAssessment of the cCovered cEntity and must address to the extent applicable:

(1) the identification and risk assessment of tThird pParty sService pProviders and aAffiliates;

(2) minimum cybersecurity practices required to be met by such tThird Pparty sService pProviders or aAffiliates in order for them to access the Iinformation tTechnology or nNonpublic iInformation of a cCovered cEntity; and

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such tThird Pparty sService pProviders or aAffiliates.

(b) Such policies and procedures must be reassessed ~~yearly~~ every two years based on the risk such tThird

pPparty sSservice pPproviders or aAffiliates 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 Tthird pPparty sSservice pPproviders or aAffiliates including, to the extent applicable, guidelines addressing:

(1) the tThird pPparty sSservice pProvider or aAffiliate's policies and procedures for access controls, including its use of mMulti-fFactor aAuthentication as required by section 1200.12 of this Part, to limit access to relevant iInformation tTechnology and nNonpublic iInformation;

(2) the tThird pParty sService pProvider or aAffiliate's policies and procedures for use of encryption as required by section 1200.15 of this Part to protect nNonpublic iInformation in transit and at rest;

(3) notice to be provided to the Ccovered eEntity in the event of a cCybersecurity iIncident directly impacting the cCovered eEntity's iInformation Ttechnology or the cCovered eEntity's nNonpublic iInformation being held by the tThird pParty sService pProvider or aAffiliate; and

(4) representations and warranties addressing the tThird Pparty Sservice pProvider or aAffiliate's cybersecurity policies and procedures that relate to the security of the cCovered Eentity's iInformation tTechnology or nNonpublic iInformation.

(d) Limited Exception. An agent, employee, representative or designee of a cCovered eEntity who is itself a cCovered Eentity need not develop its own tThird pParty iInformation Ssecurity pPolicy pursuant to this section if the agent, employee, representative or designee follows the policy of the Ccovered Eentity that is required to comply with this Part.

Section 1200.12 Access Controls

(a) Multi-Factor Authentication. Based on its rRisk aAssessment, each cCovered eEntity must select access controls, which may include Mmulti-fFactor aAuthentication and/or rRisk-Bbased aAuthentication, to protect against unauthorized access to nNonpublic iInformation or iInformation tTechnology.

(b) Multi-fFactor Aauthentication must be utilized for any aAuthorized uUser accessing the cCovered eEntity's internal networks from an external network, such as that from a virtual private network, remote access, or remote desktop, unless the cCovered eEntity'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 cCovered eEntity must include policies and procedures for the secure disposal on a periodic basis not exceeding once every three years of any nNonpublic iInformation 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 cCovered Eentity, 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 cCovered cEntity must:

(a) implement risk-based policies, procedures and controls designed to monitor the activity of aAuthorized uUsers and detect unauthorized access, use of or tampering with nNonpublic iInformation by such Aauthorized uUsers; and

(b) provide ~~regular~~ annual cybersecurity awareness training for all personnel that is updated to reflect risks identified by the cCovered cEntity in its rRisk aAssessment.

Section 1200.15 Encryption of Nonpublic Information.

(a) As part of its cybersecurity program, based on its rRisk aAssessment, each cCovered cEntity must implement controls, including encryption, to protect nNonpublic iInformation held or transmitted by the cCovered cEntity both in transit over external networks and at rest.

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

(2) To the extent a cCovered cEntity determines that encryption of nNonpublic ~~i~~information at rest is not feasible, the cCovered cEntity may instead secure such nNonpublic iInformation using effective alternative compensating controls reviewed and approved by the cCovered cEntity'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~~yearly.

Section 1200.16 Incident Response Plan.

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

(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 cCybersecurity iIncident;

(4) the internal processes for recovering from a cCybersecurity iIncident;

(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 ~~i~~Information ~~T~~technology to normal operations in a way that minimizes disruption to

customers;

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

(9) documentation and reporting regarding cCybersecurity iIncidents and related incident response activities;

(10) segmentation of iInformation tTechnology from oOperational tTechnology during a cCybersecurity iIncident; and

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

(c) At least biannuallyyearly, each cCovered cEntity 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 nNonpublic iInformation and update the plan based on the results within 90 days of said testing.

(d) All documentation and information relevant to the cCovered cEntity's iIncident rResponse pPlan 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 10 calendar days of a request.

Section 1200.17 Audits by Department Staff

(a) Not more than yearly, cCovered cEntities 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 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 Staff of the Department of Public Service are to be granted for inspection by Staff of the Department of Public Service all physical and digital assets necessary access to all assets of cCovered cEntities to prepare their audits upon request within seven 10 calendar days of a request.

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

Section 1200.18 Third Party Audits

(a) On an annual yearly basis, covered entities must cause to be conducted a third-party audit of the cybersecurity of their iInformation tTechnology and nNonpublic iInformation. Such third-party audits must, at a minimum, assess:

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

(2) policies and procedures related to protection of nNonpublic iInformation 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) t~~T~~he 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 c~~C~~ybersecurity i~~I~~ncident;

(9) s~~S~~upply chain risk and t~~T~~hird p~~P~~arty risk;

(10) the c~~C~~overed e~~E~~ntity's ability to effectively segment its i~~I~~nformation t~~T~~echnology from its o~~O~~perational t~~T~~echnology during a c~~C~~ybersecurity i~~I~~ncident; and

(11) compliance with the requirements of this Part.

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

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

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

Section 1200.19 ~~Third Party~~ Forensic Investigation~~s~~

(a) Each c~~C~~overed e~~E~~ntity must establish a contractual relationship with a qualified third-party vendor to conduct forensic investigations into a c~~C~~ybersecurity i~~I~~ncident or a suspected c~~C~~ybersecurity i~~I~~ncident.

(b) In the event of a suspected c~~C~~ybersecurity i~~I~~ncident, the c~~C~~overed e~~E~~ntity 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 ~~C~~covered e~~E~~ntity ~~must~~ to include its third-party vendor.

(c) At the completion of a forensic investigation the c~~C~~overed e~~E~~ntity 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~~ 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 c~~C~~overed e~~E~~ntity must establish a contractual relationship with a credit monitoring service for use in the event of a possible compromise of p~~P~~rivate i~~I~~nformation, as defined in paragraph b of subdivision ~~one~~ 1 of section ~~eight hundred and ninety-nine~~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 c~~C~~overed e~~E~~ntity is required to make notice to any person of a breach in the security of its system as required by subdivision ~~two~~ 2 of section ~~eight hundred and ninety-nine~~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 c~~C~~overed ~~E~~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 c~~C~~overed e~~E~~ntity 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 c~~C~~overed e~~E~~ntity reasonably believes a ~~C~~cybersecurity i~~I~~ncident affecting the ~~I~~information t~~T~~echnology or ~~N~~on p~~-P~~ublic i~~I~~nformation of the c~~C~~overed e~~E~~ntity or those of an a~~A~~ffiliate, or those of a t~~T~~hird p~~P~~arty ~~P~~provider has occurred or is occurring.

(b) Notwithstanding the provisions of subdivision (a) of this section, each c~~C~~overed e~~E~~ntity is required to maintain a log of all c~~C~~ybersecurity e~~E~~vents and c~~C~~ybersecurity i~~I~~ncidents, regardless of whether the events are subject to the notice requirements of subdivision (a), for a period of no fewer than ~~five~~ three calendar years. All documentation and information relevant to the c~~C~~overed e~~E~~ntity's c~~C~~ybersecurity e~~E~~vents 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 ~~seven~~ 10 calendar days of a request.

(c) ~~Annually~~Yearly, each c~~C~~overed e~~E~~ntity 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 c~~C~~overed e~~E~~ntity is in compliance with the requirements set forth in this Part. Each c~~C~~overed e~~E~~ntity must maintain for examination by the ~~D~~department all records, schedules and data supporting this certificate for a period of five years. To the extent a c~~C~~overed e~~E~~ntity has identified areas, systems or processes that require material improvement, updating or redesign, the c~~C~~overed e~~E~~ntity 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 dDirector, or designee, within ~~seven~~ 10 calendar days of a request.

Section 1200.22 Confidentiality.

Information provided by a cCovered cEntity pursuant to this Part is subject to exemptions from disclosure under the Public Service Law, Public Officers Law or any other applicable Sstate or Ffederal law.

Section 1200.23 Exemptions.

(a) Notwithstanding any other Part of these regulations, a cCovered cEntity that does not directly or indirectly operate, maintain, utilize or control any iInformation tTechnology, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess nNonpublic iInformation 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 cCovered cEntity 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 cCovered cEntity is exempt.

(2) In the event that a cCovered cEntity, as of its most recent fiscal year end, ceases to qualify for an exemption, such cCovered cEntity 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~~ June 1, 2026. Covered Entities will be required to ~~annually~~ 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 cEntities 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.~~

~~(b)~~(c) The following provisions include additional transitional periods. Covered cEntities 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.

~~(3) Two years from the effective date of this Part to comply with the requirements of section 1200.11 of this~~

Formatted: Font: 11 pt

Formatted: List Paragraph, Left, No bullets or numbering, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: Not at 0.71"

~~Part.~~

Section 1200.26 Severability.

If any provision of this Part or the application thereof to any ~~P~~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 p~~P~~ersons 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]

SUMMARY OF REVISED PROPOSED RULE FOR 25-M-0302SP1

The Public Service Commission (Commission) is considering adopting a new rule creating a 16 NYCRR, Chapter XII, Subchapter A, Part 1200, relating to Information Technology Cybersecurity Requirements for Covered Entities.

The revised regulations define a Covered Entity as any public utility company, as defined in subdivision twenty-three of section two of the Public Service Law, with certain exceptions. Specifically, water-works corporations and electric corporations servicing fewer than fifty-thousand customers would be exempted. All telegraph corporations and telephone companies would be exempted. Additionally, gas corporations that constitute a small business, as defined in subdivision eight of section one-hundred and two of State Administrative Procedure Law, would be exempted. Municipal corporations, as defined in section one hundred nineteen-n of the General Municipal Law, would be exempted. Finally, an employee of a Covered Entity that might otherwise meet the definition of a Covered Entity would be exempted.

The revised regulations require Covered Entities to conduct a risk assessment of the vulnerabilities of their Information Technology Systems and to update those assessments biennially. Based on the assessment, Covered Entities must develop and maintain a cybersecurity policy, which must address a number of specific areas. Generally, the policy must address ways to mitigate risk using generally accepted techniques like data masking, multifactor authentication, and other access controls. It must involve a plan to both respond to cyberattacks and recover from them.

To conduct the assessment and develop the policy, Covered Entities must employ a qualified Chief Information Security Officer, who must make yearly reports to

the company's leadership on the state of cybersecurity preparations. On a yearly basis, a senior officer of the company must certify compliance with the proposed regulations. To ensure compliance, companies must submit to regular audits by staff of the Department of Public Service as well as yearly third-party audits.

The full text of the proposed regulations and the full record of the proceeding may be reviewed online at the Department of Public Service web page: www.dps.ny.gov.

NEW YORK PUBLIC SERVICE COMMISSION

REVISED REGULATORY IMPACT STATEMENT – INFORMATION TECHNOLOGY CYBERSECURITY REQUIREMENTS FOR COVERED ENTITIES

1. **Statutory authority:**

Gas and/or Electric Corporations:

Public Service Law:

Section 65(1): "Every gas corporation, every electric corporation and every municipality shall furnish and provide such service, instrumentalities and facilities as shall be safe and adequate and in all respects just and reasonable."

Section 66(1) "The commission shall: 1. Have general supervision of all gas corporations and electric corporations…" within the State.

Section 66(2) "The commission shall:… 2…. examine or investigate the methods employed by such persons, corporations and municipalities in manufacturing, distributing and supplying gas or electricity for light, heat or power… and have power to order such reasonable improvements as will best promote the public interest, preserve the public health and protect those using such gas or electricity and those employed in the manufacture and distribution thereof, and have power to order reasonable improvements and extensions of the works, wires, poles, lines, conduits, ducts and other reasonable devices, apparatus and property of gas corporations, electric corporations and municipalities…."

Section 66(5) "…whenever the commission shall be of opinion, after a hearing had upon its own motion or upon complaint, that the property, equipment or appliances of any such person, corporation or municipality are unsafe, inefficient or inadequate, the commission shall determine and prescribe the safe, efficient and adequate property, equipment and appliances thereafter to be used, maintained and operated for the security and accommodation of the public and in compliance with the provisions of law and of their franchises and charters."

Section 66(19)(d): "The commission shall have the power to provide for an annual audit of gas corporations and electric corporations relating to the adequacy of cyber-security policies, protocols, procedures and protections including, but not limited to, as such policies, protocols, procedures and protections relate to critical energy infrastructure as defined in subdivision fourteen of section 1-103 of the energy law and customer privacy including but not limited to customer electric and gas consumption data. The commission shall have the discretion to have such audits performed by its staff or by an independent third party."

Section 66(30): "The commission shall:… 30. Promulgate rules and regulations to direct electric or gas corporations to develop and implement tools to… (b) monitor and protect customer

privacy, including but not limited to customer electric and gas consumption data from unauthorized disclosure."

Water-Works Corporations:

Public Service Law:

Section 89-b(1): "Every water-works corporation shall furnish and provide such service, instrumentalities and facilities as shall be safe and adequate and in all respects just and reasonable."

Section 89-c(4): "…whenever the commission shall be of opinion, after a hearing had upon its own motion or upon complaint, that the property, equipment or appliances of any such corporation are unsafe, inefficient or inadequate, the commission shall determine and prescribe the safe, efficient and adequate property, equipment and appliances thereafter to be used, maintained and operated for the security and accommodation of the public and in compliance with the provisions of law…"

Section 89-c(15): "The commission shall provide for management and operations audits of water-works corporations having annual gross revenues in excess of ten million dollars….The commission shall have discretion to have such audits performed by its staff, or by independent auditors."

Steam Corporations:

Public Service Law:

Section 79(1): "Every steam corporation shall furnish and provide such service, instrumentalities and facilities as shall be safe and adequate and in all respects just and reasonable."

Section 80(1): "The commission shall: 1. Have general supervision of all steam corporations" authorized to operated in the State.

Section 80(2): "The commission shall… 2. Investigate and ascertain, from time to time, the methods employed by such persons and corporations in manufacturing, distributing and supplying steam for heat or power and have power to order such reasonable improvements as will best promote the public interest, preserve the public health and protecting those using such steam and those employed in the manufacture and distribution thereof, and have power to order reasonable improvements and extensions of the pipes, lines, conduits, ducts and other reasonable devices, apparatus and property of such corporation."

Section 80(4) "…whenever the commission shall be of opinion, after hearing had upon its own motion or upon complaint, that the property, equipment or appliances of any such person or corporation are unsafe, inefficient or inadequate, the commission shall determine and prescribe the safe, efficient and adequate property, equipment and appliances thereafter to be

used, maintained and operated for the security and accommodation of the public and in compliance with the provisions of law and of their franchises and charters."

2. **Legislative objectives:** For each category of regulated utility, the legislative objective is safe, adequate, and reliable service for customers and the public. To accomplish that goal, the legislature grants the Public Service Commission (Commission) sufficient power to ensure the intended safe, adequate, and reliable service. One aspect of adequate service is the protection of consumer personal identifiable information (PII). Moreover, safe and reliable service requires, at a minimum, some level of vigilance against threats that could compromise it. As it relates to Public Service Law section 66(30)(b), the legislative objective and mandate is the creation of mandatory, minimum, enforceable cybersecurity requirements for information technology (IT) to protect private consumer data.

3. **Needs and benefits:** It is widely acknowledged that cyberattacks on entities regulated by the Commission have increased in number, scope, and complexity. IT attacks can have devastating impacts on customers whose social security, bank account, or credit card data is stolen. It can also result in substantial losses to companies subject to ransomware attacks or downtime as the result of attacks. Moreover, one study concluded that three-quarters of attacks on Operational Technology systems began as attacks on IT systems, meaning that strong IT cybersecurity is necessary to secure critical infrastructure. Australian Cyber Security Centre et. al., Principles of Operational Technology Cyber Security 9–10. Finally, the draft regulations fulfill the mandate of Public Service Law section 66(30)(b), as described above.

4. **Costs:** The regulation would apply to most jurisdictional utilities regulated by the Commission serving more than 50,000 customers, except in the case of natural gas corporations where some smaller corporations would be within its ambit and in the case of telecoms, which are entirely exempted. Most requirements within the revised regulations are consistent with industry practice or previous Commission orders and therefore will not constitute new procedures for the companies. These pre-existing requirements include the duty to submit to yearly third-party audits and audits by the Department of Public Service (Department), as outlined in 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. For these pre-existing requirements and practices, the proposal imposes no increased costs. One new requirement is that companies employ a qualified Chief Information Security Officer (CISO). The Department estimates the cost to hire a CISO (if necessary) at between $160,000-$200,000 per year, plus any benefits and payroll taxes. The bulk of new paperwork and planning requirements, like the conduct of a periodic risk assessment, is the responsibility of the CISO to conduct; additional costs to conduct those functions should be negligible. However, the revised regulations do require companies to make changes to their cybersecurity programs based on the findings of their risk assessments; as

companies' risk profiles change, so too may future compliance costs. Incremental costs of complying with increased paperwork is anticipated to be minimal.

Currently, the Department conducts regular audits of all companies subject to the revised regulations. Thus, costs to the Department are not expected to increase.

5. **Local government mandates:** No programs, services, duties, or responsibilities will be imposed upon local governments.

6. **Paperwork:** The revised regulations require companies to create and implement written cybersecurity policies for IT and Nonpublic Information based on individual risk assessments. The risk assessments must be conducted in accordance with written procedures. It requires companies to maintain a written policy to employ electronic masking of sensitive information. If a company maintains applications developed in-house, it must maintain written procedures to ensure the use of secure development procedures. Companies that interact with third party providers must implement written policies and procedures to ensure security of IT and Nonpublic Information held by or accessible to the third parties. And companies must establish a written incident response plan for responding to a cyberattack. Each year, the chairperson of the board of directors or a senior officer responsible for cybersecurity must sign an attestation certifying that the company is in compliance with the regulations.

7. **Duplication:** This revised rulemaking does not duplicate, overlap, or conflict with existing State or federal rules or legal requirements.

8. **Alternatives:** Not promulgating regulations was considered but rejected because Public Service Law section 66(30)(b), as described above, requires promulgation of regulations. Alternatives of fewer or more frequent audits was considered but rejected to align with current practice under Case 13-M-0178, as described above. Higher minimum customer counts to qualify as a covered entity were considered but rejected based on a risk-based assessment of the level of cybersecurity necessary companies of the specified size. Less rigorous regulations were considered and rejected because it is believed they would be ineffective to meet the risks facing utilities. Specific comments on the previously proposed regulations were considered or rejected as outlined in the Assessment of Public Comments submitted with this revised rulemaking.

9. **Federal standards:** There are no current generally applicable Federal IT cybersecurity standards.

10. **Compliance schedule:** This rule will be effective June 1, 2026 and the notice requirements of section 1200.21 will take effect on that date. Covered Entities will be required to annually submit a Certification of Compliance under section 1200.21(c) of this Part commencing June 30, 2027. Additional transitional periods apply. 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.

INFORMATION TECHNOLOGY CYBERSECURITY
REQUIREMENTS FOR COVERED ENTITIES

NEW YORK PUBLIC SERVICE COMMISSION

REVISED STATEMENT IN LIEU OF REGULATORY FLEXIBILITY ANALYSIS FOR SMALL BUSINESSES AND LOCAL GOVERNMENTS – INFORMATION TECHNOLOGY CYBERSECURITY REQUIREMENTS FOR COVERED ENTITIES

A revised regulatory flexibility analysis for small businesses and local governments is not being submitted because the revised regulations do not impose any adverse economic impact or reporting, record keeping, or other compliance requirements on small businesses or local government. The revised rule applies to regulated electric, gas, water, and steam companies in the State of New York. Local governments operating such utilities are explicitly exempted from the revised rule. Other exemptions for size mean no small businesses, as defined in as defined SAPA § 102(8), are expected to be affected by the revised regulation, based on a review of records kept by the Department of Public Service. As such, there are no professional services, capital, or other compliance costs imposed on small businesses or local government as a result of these revised regulations.

INFORMATION TECHNOLOGY CYBERSECURITY
REQUIREMENTS FOR COVERED ENTITIES

NEW YORK PUBLIC SERVICE COMMISSION

REVISED RURAL AREA FLEXIBILITY ANALYSIS – INFORMATION TECHNOLOGY CYBERSECURITY REQUIREMENTS FOR COVERED ENTITIES

1. **Types and estimated numbers of rural areas:** The revised regulations will apply to all rural areas of the State. The Department of Public Service estimates the regulations will apply to thirteen large covered entities, ten of which cover service areas at least partially located in rural areas.

2. **Reporting, recordkeeping and other compliance requirements:** The revised regulations require certain large companies providing electric, gas, water, or steam service to customers and maintaining information technology systems to assess their cybersecurity risks, develop a comprehensive cybersecurity plan, maintain records of the plan and its implementation, and file a compliance certification on the yearly basis. In addition, companies must maintain all records for inspection and audit by the Department of Public Service.

3. **Costs:** Most companies covered by the revised regulations currently maintain the administrative capacity, personnel, and technology systems necessary to comply with the risk assessment, planning, mitigation, and reporting requirements. Most requirements contained within the revised regulations are consistent with industry practice or previous Commission orders and therefore will not constitute new procedures for the companies. These pre-existing requirements include the duty to submit to yearly third-party audits and audits by the Department of Public Service, as outlined in 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. For these pre-existing requirements and industry practices, the revised regulations will not involve increased costs. One new requirement is that companies employ a qualified Chief Information Security Officer (CISO). The Department of Public Service estimates the cost to hire a qualified CISO at between $160,000-$200,000 per year, in addition to any benefits and payroll taxes. The bulk of new requirements, like the conduct of a periodic risk assessment, is the responsibility of the CISO to conduct, and thus any additional costs to conduct it should be negligible. However, the revised regulations do require companies to make changes to their cybersecurity programs based on the findings of their periodic risk assessments; as companies' risks profiles change, so too may their costs. Since these potential costs rely on counterfactual future events they cannot be

accurately estimated. Any incremental costs of complying with increased paperwork is anticipated to be minimal.

4. **Minimizing adverse impact:** In crafting the revised regulations, due regard was given to the needs of rural companies and consumers. In part, this is why these revised regulations largely focus only on larger companies with sufficient technical, administrative, and financial ability comply. Nevertheless, the risks of cyberattacks are as acute for rural companies as for metropolitan ones, and the revised regulations take a risk-based approach to cybersecurity.

5. **Rural area participation:** Prior to adopting the revised regulations, the Public Service Commission will provide for the opportunity to consider comments on the revised regulations in accordance with the State Administrative Procedures Act § 202(4-a).

INFORMATION TECHNOLOGY CYBERSECURITY
REQUIREMENTS FOR COVERED ENTITIES

NEW YORK PUBLIC SERVICE COMMISSION

REVISED STATEMENT IN LIEU OF JOB IMPACT STATEMENT– INFORMATION TECHNOLOGY CYBERSECURITY REQUIREMENTS FOR COVERED ENTITIES

Given that the revised regulations will enhance cybersecurity of informational technology across various utilities, it is evident from the subject matter of the revised proposal that it will likely have no impact, or a minor positive impact, on jobs and employment opportunities. Accordingly, a revised job impact statement is not being submitted for the revised regulations. The revised regulations are designed to protect consumer privacy, minimize financial losses of companies affected by cybersecurity breaches, and enhance cybersecurity for critical infrastructure. Cybersecurity breaches for critical infrastructure companies could have a negative impact on jobs or employment across the State, while preventing them will have a negligible or slightly positive impact.

ASSESSMENT OF PUBLIC COMMENTS FOR IT CYBERSECURITY REQUIREMENTS FOR COVERED ENTITIES, CASE 25-M-0302

On July 9, 2025, the Public Service Commission published a Notice of Proposed Rulemaking in the State Register requesting comments on proposed rules instituting mandatory, minimum, enforceable cybersecurity rules for information technology (IT) for electric, gas, water, steam, and telephone utilities as well as for cable corporations. The Commission received comments from utilities, telecoms, and industry groups including the U.S. Chamber of Commerce and TechNet. The industry comments were, in all cases, duplicative of comments made by one or more company. The comments and responsive changes, if any, are outlined below.

1. In joint comments eleven regulated utilities, including electric, gas, steam, and one water utility (the Joint Utilities)[1] requested clarification or revision to remove any requirement to grant physical or digital access to IT assets and recommended amending the requirement that a covered entity "file" an annual third part audit with the Commission to "make available." The Joint Utilities expressed concern that the proposed regulation might be interpreted to mean utilities must provide login credentials to Department of Public Service (DPS) auditors, who might inadvertently harm their systems.

   In response to the comments, section 1200.17(c) has been amended to read that "Covered entities must make available for inspection by staff of the Department all physical and digital assets necessary to prepare their audits upon request within 10 calendar days of a request." This is sufficient to make clear that auditors conduct discrete audits and need not be granted general login credentials. In addition, section 1200.18(c) has been amended to reflect the Joint Utilities' suggestion that third party audits be made available, not filed.

2. The Joint Utilities request that any Order issued promulgating new regulations provide utilities with cost recovery for costs to comply with new requirements above and beyond current practice.

   This request has been considered and requires no changes to the regulations.

[1] 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.

3. The Joint Utilities request that a third-party forensic investigation need not be required for every suspected cyber security incident.

   Although not every cyber incident will require a third-party forensic investigation, the Commission and the public must be confident in any investigation undertaken by a utility. An independent, third-party entity will sometimes be required. Section 1200.19(b) has been amended to give DPS staff discretion to order third-party participation in an investigation to ensure that investigations are thorough, impartial, and rigorous.

4. The joint utilities request that "The logs to be provided to DPS when requested should be 'cyber incident logs' rather than 'cyber event logs.'" In addition, the Joint Utilities request a change to the definition of "cybersecurity incident" to include a materiality component to "reduce ambiguity and limit over-reporting".

   Section 1200.21(b) has been amended to reflect that DPS may request either a cyber event or cyber incident log. While a change to the definition of "cybersecurity incident" was considered, the request is rejected. Materiality is itself an ambiguous term, which places too much onus on a utility to determine what is material. In the high-stakes area of cybersecurity, the danger of over-reporting is less than the danger of under-reporting.

5. The Joint Utilities request that the frequency of review of policies documents be changed from an annual review to a 3-5 year cadence. The Joint Utilities write that a yearly review would result in a constant review process.

   In all instances where yearly review was required the regulations have been amended to require review every two years, except as it relates to access privileges under section 1200.7, where a one-year review is necessary.

6. The Joint Utilities request that cybersecurity requirements should extend to Energy Service Companies (ESCOs) and Distributed Energy Resources (DERs).

   Because cybersecurity risks and IT infrastructure of ESCOs and DERs are fundamentally different from regulated utilities, the comment is considered but rejected.

7. The Joint Utilities ask that the terms "Third Party" and "Affiliate" be limited to high risk third parties and that the notice requirements to DPS should similarly apply to only high risk vendors.

   The proposed regulations define third party providers as a person who is not an affiliate, provides services to the covered entity, and "maintains, processors or otherwise is

permitted to access nonpublic information." Nonpublic information is inherently of high-value and in need of protection. Risk-tiering is therefore inappropriate for third-party providers with access to nonpublic information.

8. The Joint Utilities recommend combining all pre-existing assessments and orders into the regulations.

   Per section 1200.0 of the proposed regulations, "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." No further changes or explanation are needed in the proposed regulations.

9. The Joint Utilities recommend revising the definition of nonpublic information to include "identifiable" customer consumption or usage data rather than simply "customer consumption or usage data."

   The revised rulemaking reflects this request.

10. The Joint Utilities request that section 1200.20(c) be changed to clarify that the costs of credit monitoring required under the proposed regulations may be paid for be a third-party vendor or insurance.

    The revised rulemaking reflects this request.

11. The Joint Utilities request that audit rubrics used by DPS staff should be made public and subject to rulemaking.

    Rulemaking for audits rubrics is not required by the State Administrative Procedure Act. In addition, to be effective, audit rubrics must be updated regularly to reflect new conditions, and an unnecessary process would slow down needful changes. For those reason that suggested edit is rejected. Moreover, publication of audit rubrics would risk disclosing areas of weakness to threat actors. For that the request for publication of rubrics is rejected.

12. The Joint Utilities request alignment with existing standards such that DPS document requests would be answerable in 10 calendar days rather than the 7 in the proposed regulation.

    The revised regulations reflect this request.

13. The Joint Utilities request that that portions of the proposed regulations that require the Chief Information Security Officer (CISO) to undertake certain actions be amended to read "CISO or designee."

    Good cybersecurity requires strong institutional governance. The proposed regulations accomplish this, in part, by assuring that one individual must be selected by the covered entity to perform important functions. For this reason, the proposed edits are rejected. The Joint Utilities also request "clarification" that the person named as CISO need not maintain that "exact job title." Part 1200.4 of the proposed regulations read "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")" (emphasis added). No clarification is required.

14. Similarly, the Joint Utilities seek confirmation "that the term 'written policy' in Part 1200 refers broadly to any formally documented guidance or requirements – regardless of naming convention – so long as it meets the regulation's substantive intent."

    No clarification is required.

15. Finally, the Joint Utilities request clarification of the definition of encryption and/or the level of stringency as referenced in section 1200.15.

    Cybersecurity is characterized by its fast-moving, every-changing technological landscape. For this reason, any definition of encryption or minimum level of stringency risks immediate obsolescence. No clarification can or should be provided, although the Commission expects that covered entities conducting proper risk assessments will utilize industry best practice security.

16. In a slew of comments submitted by the telecom industry, the industry argued that the Commission lacks authority to impose IT cybersecurity regulations on telephone and cable providers. Separately, the telecom industry argues that telephone and cable providers' market exposure, infrastructure, and cross-jurisdictional footprint render their cybersecurity posture distinct from that of the jurisdictional utilities.

    The comments regarding the Commission's statutory authority have been considered but rejected. Nevertheless, because of the distinct differences between the telecom industry and jurisdictional utilities, telephone and cable providers have been excised from the

revised regulations. The Commission reserves the right to promulgate regulations in the future to regulate telecom IT.

17. The telecom industry submitted comments raising concerns that the third-party annual audit requirement of section 1200.18 places high resource demands and significant costs upon covered entities. Instead, they request third-party audits occur once every three years or not at all. Notably, the joint utilities did not comment.

    These comments are considered but rejected. Although annual third-party audits do impose costs, they are necessary given the high level of risk associated with critical infrastructure. Jurisdictional utilities have been subject to yearly third-party audits for some time under existing Commission Orders, without incident.

18. The telecom industry object to section 1200.17, which allows for yearly audits by DPS staff. They argue yearly audits would require an "unprecedented" level of access and are inconsistent with the New York Sate Department of Financial Services (DFS) cyber regulations. They request the audits be dispensed with or greatly limited.

    These comments are considered but rejected. Jurisdictional utilities are already subject to regular DPS audits, and any inconsistency with DFS practice is justified by the criticality of the infrastructure regulated by DPS. Moreover, concerns about the level of access are addressed by the changes made in connection with the comments of the Joint Utilities, noted in paragraph (1).

19. The telecoms request changes to the definitions of cybersecurity event and cybersecurity incident, specifically the addition of a materiality component to the definition of cybersecurity incident.

    These comments have been considered and rejected, for the reasons noted in paragraph (4).

20. The telecoms request changes to section 1200.6, which requires logging of cybersecurity events for five years. They argue that this will be expensive and that the marginal benefit of this expense is not worth the cost. They suggest that logs be kept only for "material" cybersecurity events.

    For the same reasons explained in paragraph (4), 'materiality' is rejected. Moreover, logging of cybersecurity events is an important tool to detect long-term patterns and to thwart threat actors before they strike. It is also helpful for forensic investigators to

construct what occurred after a successful cyberattack. However, the revised rulemaking amends section 1200.16 to require logging of cybersecurity events for only three years.

21. The telecoms comment that section 1220.20's credit monitoring provides no "meaningful benefit" and will be prohibitively expensive.

    This comment is considered but rejected. Credit monitoring provides meaningful benefits to customers impacted by a data breach through no fault of their own.

22. The telecom industry argues that the requirements of the cybersecurity program outlined in the proposed regulations are overly prescriptive and too costly. As an alternative, they suggest simple compliance with the NIST Framework.

    The comments are considered but rejected. In promulgating mandatory, minimum, enforceable regulations an appropriate balance must be struck between overly prescriptive requirements and overly loose guidelines. Given the criticality of the utilities regulated, the appropriate balance has been struck. However, that balance may be inappropriate for telecoms. For this reason and others, telecoms have been removed from the revised regulations as outlined in paragraph (16).

23. Telecom industry members commented on the remediation component of section 1200.18(d), which requires that covered entities make "best efforts" to correct deficiencies noted in annual third-party audits. They comment that only material deficiencies should be remediated.

    The comment is considered but rejected. Covered entities are required to make best efforts to correct deficiencies, which itself suggests a risk-based ordering of priority.