HINMAN STRAUB P.C.
ATTORNEYS AT LAW

121 State Street
Albany, New York 12207-1693
Tel: 518-436-0751
Fax: 518-436-4751

TO: **Memo Distribution List**

LeadingAge New York

FROM: Hinman Straub P.C.

RE: Revised Proposed Cybersecurity Regulations Overview

DATE: January 3, 2017

NATURE OF THIS INFORMATION: This is information explaining new requirements you need to be aware of or implement.

DATE FOR RESPONSE OR IMPLEMENTATION: An additional 30 day comment period accompanies the proposed regulation, with comments due on January 27, 2017.

HINMAN STRAUB CONTACT PEOPLE: Sean Doolan, Cheryl Hogan and Kelly Ryan

THE FOLLOWING INFORMATION IS FOR YOUR FILING OR ELECTRONIC RECORDS:
Category: #4 Regulatory Process Suggested Key Word(s):

I. Introduction

On December 28, the Department of Financial Services ("DFS") issued a revised proposed regulation requiring regulated entities to establish cybersecurity programs and policies. DFS' original proposed regulation was explained in our memorandum dated September 23, 2016. Although a number of changes to the original proposed regulation that we requested are included in the revision, most notably a shift toward flexibility based on risk analysis, many are not. We will continue to press for those changes.

An additional 30 day comment period accompanies the proposed regulation, with comments due on January 27. This memorandum summarizes key changes from the first proposed regulation.

II. Scope and Basic Requirements

A. Scope

- Small company exemption. While the definition of covered entity was not altered, the proposed regulation has been modified to change applicable exemptions. Previously, there was a limited exemption for covered entities with fewer than 1000 customers in each of the last three calendar years, less than $5 million in gross annual revenue for each of the last three fiscal years, and less than $10 million in year-end total assets. The revised proposed regulation includes separate exemptions for covered entities with fewer than 10 employees (including independent contractors), entities with less than $5 million in gross annual revenue, and entities with less than $10 million in year-end total assets. In other words, entities can meet any of the tests (with the 1000 customer test changed to 10 employees) instead of needing to meet all of the tests to be eligible for an exemption.

- HIPAA/HITECH Safe harbor. Given the broad scope of these regulations, and more targeted, industry-specific federal legislation already in place, we pressed for safe harbor provisions that would recognize compliance with requirements such as those in HIPAA and HITECH to avoid complicated or conflicting compliance mandates. Safe harbor language was not included in the revised proposed regulation.

B. Definitions

- "Nonpublic information" is defined as "any information that is not Publicly Available Information" and is:

    - Any business related information which would cause a material adverse impact to the business, operations, or security of the covered entity if tampered with;

    - Any information concerning an individual which 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) SSN, (ii) drivers' license number or non-driver ID number, (iii) 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. *This more specific provision replaces problematic language that included any information provided to a covered entity in connection with seeking or obtaining a financial product or service, or resulting from a transaction*;

- Any information, except age and gender, <u>in any form or medium</u> that is created by, derived or obtained from a health care provider or any individual that relates to the past, present, or future physical, mental, or behavioral health or condition of any individual or member of the individual's family or household, or from the provision of or payment for health care (*emphasis depicts revision);*

- *Language related to information used to distinguish or trace an individual's identity or any information that is linked or linkable to an individual, including but not limited to medical, educational, financial, occupational, or employment information, information about an individual used for marketing purposes or any password or other authentication factor was deleted from the definition of "nonpublic information."*

- The definition of "person" is revised to explicitly exclude governmental entities.

- The definition of "penetration testing" is revised to specifically include "attempting unauthorized penetration of databases or controls from outside or inside the covered entity's Information Systems."

- A new definition of "risk assessment" is added to reference revised requirements which are discussed in further detail below.

- A new definition of "third party service provider" is added to mean a Person that (i) is not an affiliate of the covered entity, (ii) provides services to the covered entity, and (iii) maintains, processes or otherwise is permitted to access nonpublic information through its provision of services to the covered entity. This definition narrows the scope of provisions related to third parties, as discussed in further detail below.

We had raised concerns regarding the scope of a number of definitions (e.g. cybersecurity event, information system) that were <u>not</u> amended. However, the clear shift toward a risk-based approach in the regulation addresses many of the concerns we raised regarding scope.

B. <u>Effective Date</u>

The regulation would now be effective March 1, 2017, as opposed to January 1, 2017, with a general 180 day transition period. Additionally, a number of other transition periods apply. These additional transition periods address concerns we raised about compliance timeframes and they provide important additional time to comply with many of the substantive provisions of the regulation.

Covered entities have one year from the effective date (i.e., March 1, 2018) to comply with the following provisions:

- CISO annual report to the board of directors;
- Penetration testing and vulnerability assessments;
- Risk assessment;
- Multi-factor authentication;
- Provide cybersecurity awareness training.

Covered entities have eighteen months from the effective date (i.e., August 1, 2018) to comply with the following provisions:

- Audit trails;
- Application security;
- Limitations on data retention;
- Implement policies, procedures, and controls to monitor activity of authorized users and detect unauthorized access;
- Encryption of non-public information.

Covered entities have two years from the effective date (i.e., March 1, 2019) to comply with the following provision:

- Third Party Service Provider Security Policy.

The first annual report to the Department, as described below, would be due February 15, 2018.

III. Cybersecurity Policy

Under the proposed regulation, covered entities must implement and maintain a written cybersecurity policy. The required scope of the policy is tempered in the revised regulation to reflect the risk assessment, discussed in further detail below. To the extent applicable, the following items should be addressed in a cybersecurity policy:

1. Information security;
2. Data governance and classification;
3. Asset Inventory and Device Management (new);
4. Access controls and identity management;
5. Business continuity and disaster recovery planning 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. Custom data privacy;
12. Vendor and third-party service provider management;
13. Risk assessment; and

14. Incident response

"Capacity and performance planning" was removed as an element of the cybersecurity policy.

Board review and approval requirements were also softened to allow a senior officer or appropriate committee of the Board to review and approve, per our recommendation.

IV. Cybersecurity Program

Covered entities must maintain a cybersecurity program that ensures the confidentiality, integrity, and availability of covered entities' IT systems. Broad parameters regarding what must be included in the program, as informed by the entity's risk assessment, include:

- Identify and assess internal and external cyber risks that may threaten the security or integrity of the nonpublic information stored on information systems;
- Use a defensive infrastructure and the implementation of policies and procedures to protect information systems and nonpublic information from unauthorized access, use, or other malicious acts;
- Detect cyber security events;
- Respond to identified or detected cybersecurity events to mitigate any negative effects;
- Recover from cybersecurity events and restores normal operations and services; and
- Fulfill all regulatory reporting obligations.

V. Risk Assessment and Impact on Other Requirements

Perhaps the most significant change in the revised proposed regulation is a shift toward permitting a covered entity to use a risk assessment analysis to guide the development and implementation of its cybersecurity policy and program. The need for a risk-based approach was consistent theme requested by stakeholders in a range of regulated industries and was a central element of our comments to DFS. The Department is clear, however, that risk assessment should not simply consist of a cost-benefit analysis.

Now, instead of a risk assessment simply being an element of a cybersecurity program, it is the critical step that guides other aspects of the program. Throughout the proposed regulation, many requirements that were applicable in all circumstances are now informed by the risk assessment and applicable where warranted based on the results of the risk assessment.

Specific requirements include:

A. Penetration Testing

Specific annual and quarterly testing and assessment requirements have been replaced with a requirement to monitor and test periodically in accordance with the risk assessment. If a covered entity does not use continuous monitoring to detect vulnerabilities or changes, then annual penetration testing and bi-annual vulnerability assessments but be conducted.

B. Audit Trail

Audit trail requirements have been scaled back in the revised proposed regulation, and are also informed by the risk assessment. To the extent applicable, covered entities must securely maintain systems that are designed to reconstruct material financial transactions sufficient to support the normal operations and obligations of the covered entity, and include audit trails designed to detect and respond to cybersecurity events that are reasonably likely to materially harm any material part of the entity's normal operations. Covered entities must retain records required by audit trail requirements for five years, which is down from the six year requirement in the earlier version of the proposed regulations.

We sought clarification as to the scope of data which must be retained under audit trail requirements. Although audit trail requirements were generally tempered and data retention requirements were shortened from six years to five years, clarification regarding the scope of data was not included in the revised proposed regulation.

C. Access Privileges

Based on the risk assessment, covered entities must limit access to IT systems that provide access to nonpublic information and periodically review such permissions.

D. Application Security

The cybersecurity program must include written procedures, guidelines, and standards to ensure that in-house developed applications are developed securely, as well as procedures for assessing and testing the security of all externally-developed applications used by the covered entity. These procedures, guidelines, and standards must be reviewed, assessed, and updated by the Chief Information Security Officer at least annually. The revised proposed regulation permits the required review, assessment, and update to be conducted by a qualified designee of the CISO.

E. Data Retention

Requirements related to data retention were modified to require the "secure disposal on a periodic basis" of nonpublic information relating to individuals that is no longer needed for business operations or a legitimate business purpose. In addition to permitting information that is required to be maintained pursuant to law or regulation to be retained, the proposed regulation now also permits retention where targeted disposal is not reasonably feasible due to the manner in which the information is retained.

F. Training and Monitoring

Covered entities must implement risk-based policies, procedures, and controls to monitor the activity of authorized users to detect unauthorized access or use of nonpublic information by authorized users.

Additionally, covered entities must offer regular cybersecurity awareness training sessions that are updated to reflect risks identified by the covered entity in its annual risk assessment. A requirement that the covered entity must require all personnel to attend trainings was deleted.

G. Encryption

We had raised encryption requirements as an issue of significant concern. The revised proposed regulation substantially scales back encryption requirements. Instead of requiring all covered entities to encrypt all nonpublic information held or transmitted both in transit and at rest, encryption is now one of a range of controls that can be utilized by a covered entity, based on its risk assessment. If encryption in transit or at rest is infeasible, effective alternative compensating controls may be used as reviewed and approved by the CISO. There is no time limitation on the flexibility to use alternative approaches as was the case in the earlier version of the regulation. While requested clarification regarding appropriate alternative compensating controls was not included in the revisions, the shift away from mandatory encryption when not feasible or warranted based on a risk assessment is an important revision.

VI. Information Security Officer and Personnel

Each covered entity must designate a qualified individual to serve as the Chief Information Security Officer (CISO). This individual is responsible for the implementation of the cybersecurity program and enforcement of the cybersecurity policy. Covered entities may delegate this function to an employee of an Affiliate or a Third Party Service Provider, but must maintain ultimate responsibility for compliance and must designate a senior employee to oversee the third party. The CISO must deliver a report at least annually to the Board of Directors. We sought clarification regarding the board reporting structure in the context of a corporate board versus the board of a New York entity, but this change was not included. The report must consider the following items:

- The confidentiality, integrity and availability of information systems;
- The covered entity's cybersecurity policies and procedures;
- Identification of material cyber risks;
- Assess the overall effectiveness of the cybersecurity program;
- Material cybersecurity events that affected the covered entity during the time period addressed by the report.

The reporting requirements in the proposed regulation are scaled back from the initial version, with more permissive language generally and the deletion of the requirement to propose steps to remediate inadequacies identified in the cybersecurity program.

VII. Confidentiality

A new provision was added to the proposed regulation clarifying that information provided by a covered entity to the Department pursuant to the regulation is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law. This was a change we specifically requested.

VIII. Third Party Service Provider Security Policy

The earlier version of the proposed regulation included sweeping requirements related to third parties that do business with covered entities, many of which were impracticable or impossible to implement. The revised proposed regulation scales back some of the requirements, and importantly, applies them only to "third party service providers," a considerably narrower universe. In addition to limiting the requirements of this section to third party service providers, which by definition have access to nonpublic information, the revised proposed regulation also employs risk-based principles with respect to the requirements.

Covered entities must implement written policies and procedures that are designed to ensure the security of IT systems and nonpublic information accessible to, or held by, third party service providers, and shall address, to the extent applicable:

- Identification and risk assessment of third party service providers covered by the requirements;
- Minimum cybersecurity requirements that must be met by third party service providers;
- Due diligence processes used to evaluate the adequacy of cybersecurity practices of third party service providers; and
- Periodic assessment of third party service providers and the adequacy of their cybersecurity policies on a periodic basis, (a requirement that review occur no less than annually was deleted).

The policies and procedures must also include guidelines for due diligence and/or contractual protections, including provisions addressing multi-factor authentication; use of encryption; prompt notice to the covered entity of a security event (this is already required under HIPAA); representations and warranties by the third party service provider that relate to the security of the covered entity's IT systems and nonpublic information.

The previous version of the proposed regulation required specific "preferred contractual provisions" related to these issues and included "identity protection services for customers materially impacted by a security event due to the third party's negligence or misconduct" as an issue to be addressed. The earlier version would have also required third parties to provide representations and warranties that its service or product is free from viruses, etc. that would impair the security of the covered entity's IT systems or non-public information and included the right of the covered entity to audit the third party.

The revised proposed regulation also includes a new limited exception indicating that an agent, employee, representative or designee of a covered entity that is itself a covered entity is exempt and does not need to develop its own cybersecurity policy if it is covered by the other covered entity's policy.

IX. Authentication Requirements

The revised proposed regulation also significantly scales back requirements related to multi-factor authentication. The previous version would have required multi-factor authentication for any individual accessing internal systems or data from an external network and for privileged access to database servers that allow access to nonpublic information. Similar to the approach taken with encryption, multi-factor authentication is now generally a control that may be utilized based on the covered entity's risk assessment.

Multi-factor authentication must be used by any individual accessing internal networks from an external network, unless the CISO has approved of a reasonably equivalent or more secure access control in writing.

X. Notice to Superintendent

In addition to existing requirements related to reporting security breaches and similar incidents, the original proposed regulation would have required a covered entity to notify the Superintendent of any cybersecurity event that "has a reasonable likelihood of materially affecting the normal operation of the entity or that affects nonpublic information" as promptly as possible, but no later than 72 hours after becoming aware of the event. This broad language raised concerns that the Department would receive a deluge of notices, many of which would not be useful. Under the revised proposed regulation, notice must be provided within 72 hours in relation to any event that must be reported to any government or self-regulatory agency and any event that has a reasonable likelihood of materially harming any material part of the normal operations of the covered entity. While the revised scope of events triggering notice addresses concerns we raised, the DFS did not change the 72 hour reporting requirement, which may create significant operational challenges.

In addition, covered entities must annually file a written statement with the Superintendent certifying compliance with the requirements of the regulation. An example of the attestation is included with the draft regulation and the form must be filed by February 15 of each year (was January 15). Related records, schedules, and data must be maintained for five years.

In the event weaknesses have been identified that require material improvement, updating or redesign, covered entities must document such plans and efforts and maintain this documentation for inspection by the Superintendent. A requirement that, in the event a material risk of imminent harm is identified, the covered entity must notify the Superintendent within 72 hours and include reference to such items in its annual report, has been deleted.