Financial Institutions Gain Some Flexibility in Revised New York Cybersecurity Regulation

February 01, 2017

Overview

The changes in the New York State Department of Financial Services' (NYDFS) revised proposed cybersecurity regulation (Revised Regulation) reflect an effort to respond to industry concerns about the original proposed regulation (Proposed Regulation) and to permit covered entities some flexibility in tailoring their cybersecurity programs to their individual risk assessments.

However, the Revised Regulation as it stands presents a heavy burden, especially on many of the smaller financial institutions that will be covered. It is not yet clear whether these changes will render the requirements workable for all covered entities.

Background

On December 28, 2016, the NYDFS issued a revised proposed cybersecurity regulation. Although it provides greater flexibility for covered entities, the Revised Regulation retains the basic framework of the original Proposed Regulation.

The NYDFS received more than 100 comment letters on the Proposed Regulation and industry concern regarding its burdensome requirements led the New York State Assembly's Standing Committee on Banks to hold a public hearing regarding the Proposed Regulation on December 19, 2016. Both the comment letters and testimony at the hearing emphasized concerns with the Proposed Regulation's compliance costs and inflexibility that failed to account for varying degrees of cybersecurity risk for institutions of different sizes.

The Revised Regulation added an additional 30-day comment period, which closed on January 27, 2017. Unless modified further, the Revised Regulation will become effective on March 1, 2017, subject to certain longer transition periods for specific provisions as discussed further below.

For more details on the Proposed Regulation, which was issued on September 13, 2016, please refer to our previous client alert on the subject. We have also prepared a comparison of the Revised Regulation against the Proposed Regulation to illustrate the difference.

Revised Requirements

The Revised Regulation did not modify the scope of the Proposed Regulation, which still generally applies to any person "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation, or similar authorization under the Banking Law, the Insurance Law, or the Financial Services Law."

However, the Revised Regulation did alter several aspects of the Proposed Regulation.

Most importantly, the Revised Regulation provides covered entities with greater flexibility in complying with the cybersecurity program requirements. Some of the key changes in the Revised Regulation include:

- ***Risk-Based Approach.*** The Proposed Regulation required an annual risk assessment of a covered entity's information systems. The Revised Regulation only requires periodic risk assessments, and, more importantly, provides that a covered entity may use the risk assessment as a basis for designing its cybersecurity program. Other requirements may also be based on these periodic risk assessments, including the cybersecurity policy, penetration testing, and vulnerability assessments; audit trails; third-party service provider security polices; multi-factor authentication; and encryption.
- ***Encryption of "Nonpublic Information."*** Covered entities will be required to encrypt all "Nonpublic Information," both in transit and at rest. However, the Revised Regulation clarifies the encryption requirements and provides for compensating controls where encryption at rest is infeasible. It also narrows the definition of "Nonpublic Information."
- ***Reporting Cybersecurity Events.*** The Revised Regulation narrows the requirement for reporting "Cybersecurity Events" to the NYDFS. Under the Revised Regulation, notice to the NYDFS is required when: (1) notice of the Cybersecurity Event is required to be provided to any government body, self-regulatory agency or any other supervisory body; and (2) the Cybersecurity Event has a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity."
- ***Audit Trails*.** The Revised Regulation relaxes the audit trail requirement and reduces the retention period from 6 to 5 years.
- ***Affiliate Cybersecurity Programs.*** The Revised Regulation will permit Covered Entities to adopt an affiliate's cybersecurity program to satisfy the cybersecurity requirements.
- ***Additional Exemptions.*** Although the "small covered entity" exemption was not significantly changed, the Revised Regulation does provide additional exemptions. It adds an exemption from certain of the requirements for a "Covered Entity that does not directly or indirectly operate, maintain, utilize, or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive, or possess Nonpublic Information." The Revised Regulation also adds a requirement for exempt entities to file a notice with the NYDFS.
- ***Confidentiality*.** The Revised Regulation adds a provision providing that information provided by a covered entity to the NYDFS as required by the Revised Regulation is exempt from disclosure under the New York banking law, insurance law, financial services law, public officers law, or any other applicable state or federal law.

Transitional Periods

Covered entities will generally have 180 days from the effective date of March 1, 2017 to comply. However, the Revised Regulation added to and expanded the transitional periods for several key provisions.

Covered entities will have 1 year from the effective date to comply with the following:

1. First CISO report to the board of directors
2. Penetration testing and vulnerability assessments
3. Risk assessment
4. Multifactor authentication
5. Cybersecurity training for all personnel

Covered entities will have 18 months from the effective date to comply with the following:

1. Audit trail
2. Application security
3. Limits on data retention
4. Policies and procedures and controls for monitoring activity of authorized users
5. Encryption

Finally, covered entities will have 2 years from the effective date to comply with the third-party service provider security policy requirement.

Comparison to FFIEC Guidelines

As a point of comparison, we note that the Revised Regulation's requirements are largely consistent with the cybersecurity protections outlined in the Federal Financial Institutions Examination Council's (FFIEC) Information Technology Examination Handbook – Information Security Booklet (rev. Sept. 2016) (FFIEC Guidelines). The FFIEC Guidelines are not strict requirements, but rather provide guidance to examiners and address factors necessary to assess the level of security risks to a financial institution's [1] information systems.

Comparing the FFIEC Guidelines and Revised Regulation, we see that both provide for penetration testing, vulnerability assessments, and risk assessments. Both regimes also require the appointment of an information security officer, a written cybersecurity policy, reports to the board of directors, and training.

Despite many similarities, there are also differences between the regimes where the Revised Regulation goes further. For example, the FFIEC Guidelines do not provide for encryption of information at rest as well as in transit. The FFIEC Guidelines also do not explicitly require destruction of nonpublic information no longer in use. The Revised Regulation requires annual certification of compliance by a senior officer—something not required by the FFIEC Guidelines—and its multi-factor authentication requirements are also more stringent.

We also note that several FFIEC members (the Federal Reserve Board, the OCC and the FDIC) recently extended the comment period on an advance notice of proposed rulemaking regarding enhanced cyber risk management standards for large and interconnected entities subject to supervision and those entities' service providers

("ANPR"). The comment period for the ANPR, which was originally issued on October 26, 2016, was extended until February 17, 2017.

For further information on this topic, please contact a member of the firm's Consumer Financial Services Group.

---

[1] The term "financial institution" includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions.