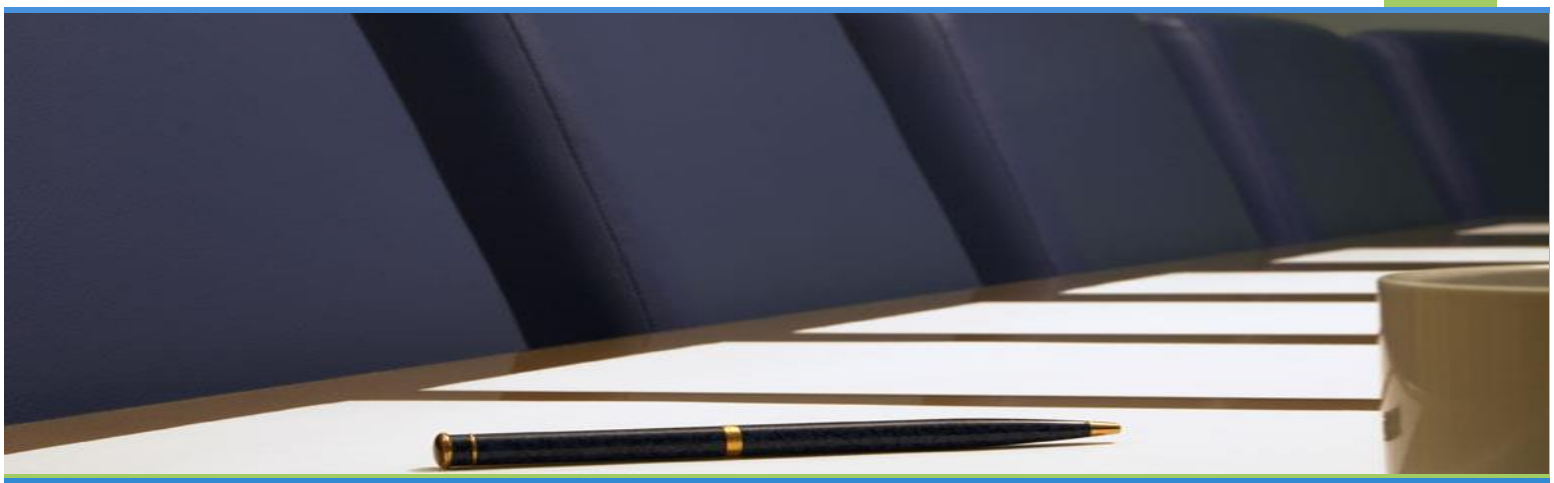
GT GreenbergTraurig



New York Government Law & Policy | Alert

January 2017

NYS Department of Financial Services Releases Revised Proposal Addressing Cybersecurity Requirements for Financial Institutions

On December 28th, 2016, the New York State Department of Financial Services (DFS or the Department) published a revised version of its proposed regulation governing cybersecurity requirements for all entities required to operate in New York under a license, registration, or similar authorization issued by the Department (the Revised Proposal). Its provisions are scheduled to take effect on March 1, 2017, with phased-in implementation dates. DFS received over 150 comments in response to its originally proposed cybersecurity regulation (the Original Proposal), which led to the issuance of the Revised Proposal. Many of the comments addressed the perceived rigidity and excessively prescriptive requirements of the Proposal's core provisions. Although the Revised Proposal included some significant revisions addressing those comments, a number of open questions remain. The publication of the Revised Proposal triggers a new opportunity for public comment, which continues until January 27th, 2017. The final version of the regulation could have a significant impact on entities nationwide, as the DFS language has the potential to become a template used throughout the country.

The DFS Revised Proposal

The DFS Revised Proposal is the most comprehensive and detailed regulatory framework for cybersecurity advanced to date by any federal or state governmental agency. Its provisions would require entities to implement a broad range of controls, across various platforms, systems, and operations designed to protect "nonpublic information" and the "information systems" that store or transmit that information. The specified controls are detailed and prescriptive and require, for example, that each entity:

- Implement a cybersecurity program and a cybersecurity policy, each with prescribed elements aimed at protecting its information systems and nonpublic information;
- Conduct regular penetration testing and vulnerability assessments across all of its information systems;

- Encrypt all nonpublic information it holds or possesses, whether in transit or at rest, unless encryption is determined to be infeasible;
- Require multi-factor authentication or a reasonable equivalent for external users accessing the entity's internal networks; and
- Implement policies relating to the security of nonpublic information accessible to, or held by, third party service providers.

Risk-based Approach

Many of the public comments in response to the Original Proposal focused on the detailed nature of the specific requirements and its overly broad definitions of certain key terms, which, together, posed serious operational and financial challenges to the entities required to implement them. Those challenges were made more onerous by the proposal's failure to incorporate risk-based principles that would permit entities to tailor their implementation of the requirements to meet the unique nature and extent of the specific underlying targeted risks. This was despite the fact that a risk-based approach has been adopted in existing federal cybersecurity guidance and regulations, including regulations promulgated under the Gramm-Leach-Bliley Act, and in guidance issued by standard-setting agencies such as the National Institute of Standards and Technology.

The most notable change to the Original Proposal reflects the Department's willingness to permit a risk-based approach. Specifically, under the Revised Proposal, entities are permitted to calibrate their implementation of a number of core, specific cybersecurity measures in accordance with their assessment of the underlying targeted risk. This would afford entities more flexibility in implementing key elements of the Revised Proposal, including the requirements for a cybersecurity program and policy, penetration testing and vulnerability assessments, encryption of nonpublic information, multi-factor authentication and third-party information security. Entities would be required to undertake a periodic risk assessment for the purpose of assessing the vulnerability of their information systems and nonpublic information, and to revise that assessment as necessary to address evolving threats. The results of this assessment would then guide their implementation of the required measures. However, in its publication of the Revised Proposal, the Department also stated that an entity's risk assessment "is not intended to permit a cost-benefit analysis of acceptable losses where an institution is faced with cybersecurity risks." It remains unclear under the Revised Proposal what specific factors may inform a covered entity's risk assessments, and further guidance from DFS may be required.

Third Party Service Providers

The Revised Proposal also narrows third party information security policy requirements by expressly limiting the regulation's application to third party *service providers*, a newly-defined term capturing any non-affiliate that provides services to the entity and that maintains, processes, or otherwise is permitted access to nonpublic information through its provision of services to the entity. It also relaxes the original requirement to obtain specific contractual assurances from third party service providers, instead permitting representations and warranties "addressing the third party service provider's cybersecurity policies and procedures." The Revised Proposal also expressly carves-out governmental agencies -- many of which are routinely given access to the type of sensitive nonpublic information at issue -- from application of the third party oversight and other requirements under the Proposal, in perhaps a tacit acknowledgement of the challenges posed in implementing and enforcing the requirements.

Other Key Revisions

The Revised Proposal incorporates a number of other significant changes that appear to reduce the burden on implementing entities, including:

- Narrowing the definition of "nonpublic information" to health or treatment-related information concerning an individual or his or her family, or any information about an individual which, in combination with one or more additional, secure data points, such as a social security number, account passcode, or biometric information, can be used to identify the individual;

- Relaxing the absolute requirement for encryption of data in transit and at rest by permitting the indefinite use of alternative compensating controls for so long as the entity deems encryption to be infeasible;
- Permitting an entity to satisfy the cybersecurity program requirements in the Revised Proposal by adopting the cybersecurity program of its affiliate, provided the affiliate's program meets the applicable standards;
- Limiting the circumstances under which a cybersecurity event must be reported to the Department within 72 hours of occurrence to instances where the event is determined to require notice to any government agency, self-regulatory agency or other supervisory body, and the event has a reasonable likelihood of materially harming any material part of the entity's operations; and
- Incorporating new, extended deadlines for implementing various provisions. Notably, entities will be permitted two years for implementing the third party service provider requirements. Entities will also be permitted 18 months for implementing the audit trail requirements, application security requirements, data retention requirements, training and monitoring requirements, and data encryption requirements. Finally, entities will be permitted 12 months for implementing penetration testing and vulnerability assessment requirements, risk assessment requirements, multi-factor authentication requirements, and cybersecurity awareness training requirements.

Conclusion

In the Revised Proposal, the Department addressed a number of major concerns expressed during the comment period. DFS's incorporation of risk-based principles and other amendments that provide entities with greater flexibility in determining how, when, and to what extent they must implement the underlying requirements should make it easier for entities to comply with the yet to be adopted final regulation. Even with these amendments, however, the Revised Proposal retains a number of ambiguities and imposes operational and compliance burdens that may significantly challenge implementing entities.

Potentially regulated entities, along with any affected third parties, have until the close of the public comment period on January 27th, to submit written comments seeking additional amendments or clarifications. To the extent that this results in the Department making additional substantial changes, the regulation will have to be re-published and opened to further public comment. It appears that the Department is intent on moving quickly towards adopting a final version of the regulation. It is possible that the Revised Proposal, or substantially similar language, will become effective on March 1, 2017, and any lingering questions or concerns will have to be addressed through informal guidance from DFS.

This *GT Alert* was prepared by **Niall E. O'Hegarty**, **Harold N. Iselin**, **Joshua L. Oppenheimer**, and **Michael J. Murphy.** Questions about this information can be directed to:

- Niall E. O'Hegarty | +1 212.801.6879 | ohegartyn@gtlaw.com
- Harold N. Iselin | +1 518.689.1415 | iselinh@gtlaw.com
- Joshua L. Oppenheimer | +1 518.689.1459 | oppenheimerj@gtlaw.com
- Michael J. Murphy | +1 518.689.1411 | murphym@gtlaw.com
- Or your Greenberg Traurig attorney

Albany
+1 518.689.1400

Amsterdam
+ 31 20 301 7300

Atlanta
+1 678.553.2100

Austin
+1 512.320.7200

Berlin¬
+49 (0) 30 700 171 100

Berlin-GT Restructuring¯
+49 (0) 30 700 171 100

Boca Raton
+1 561.955.7600

Boston
+1 617.310.6000

Chicago
+1 312.456.8400

Dallas
+1 214.665.3600

Delaware
+1 302.661.7000

Denver
+1 303.572.6500

Fort Lauderdale
+1 954.765.0500

Houston
+1 713.374.3500

Las Vegas
+1 702.792.3773

London*
+44 (0)203 349 8700

Los Angeles
+1 310.586.7700

Mexico City+
+52 55 5029.0000

Miami
+1 305.579.0500

New Jersey
+1 973.360.7900

New York
+1 212.801.9200

Northern Virginia
+1 703.749.1300

Orange County
+1 949.732.6500

Orlando
+1 407.420.1000

Philadelphia
+1 215.988.7800

Phoenix
+1 602.445.8000

Sacramento
+1 916.442.1111

San Francisco
+1 415.655.1300

Seoul∞
+82 (0) 2.369.1000

Shanghai
+86 (0) 21.6391.6633

Silicon Valley
+1 650.328.8500

Tallahassee
+1 850.222.6891

Tampa
+1 813.318.5700

Tel Aviv^
+03.636.6000

Tokyo¤
+81 (0)3 4510 2200

Warsaw~
+48 22 690 6100

Washington, D.C.
+1 202.331.3100

Westchester County
+1 914.286.2900

West Palm Beach
+1 561.650.7900