New York's Cybersecurity Requirements for DFS Licensees:

A New Item at the Top of the To-Do List

Authored by: Theodore P. Augustinos

May 2017

This article was reprinted with permission from the May 2017 issue of the Intellectual Property & Technology Law Journal.

With the compliance date only a few months away, licensees of the New York Department of Financial Services (DFS) must start taking action immediately to comply with the coming cybersecurity requirements, which will be more onerous and difficult than any existing requirements in the United States. The regulation became effective March 1, 2017, with transition periods that will require compliance with various provisions beginning August 28, 2017, and over the next two years. This article identifies who will be subject to the new requirements, what is required and by when, and what steps should be taken to comply.

The new requirements deserve attention from persons and companies throughout the banking, insurance, and other regulated financial industries, as it is likely that other states will look to the New York requirements as a model. The New York requirements also serve as a new and robust checklist for any business to consider for improving its cybersecurity risk profile.

Who Is Affected?

The proposed regulation applies to Covered Entities, defined to mean each individual or nongovernmental entity that operates or is required to operate under a license, registration, or other authorization under the New York banking, insurance, or financial services laws, therefore, nearly any DFS Licensee is affected. There is a limited exemption from many (but not all) of the requirements for Covered Entities with fewer than 10 employees (including independent contractors) of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, or less than $5 million in revenue in each of the past three years from New York business operations of the Covered Entity and its affiliates, or less than $10 million in year-end total assets according to GAAP (including affiliates).

Exempt from nearly all of the requirements is any person or entity that does not directly or indirectly have any Information Systems or any Nonpublic Information. A Covered Entity that is an employee, agent, representative or designee of a Covered Entity and is covered by the cybersecurity program of the Covered Entity is exempt from the regulation. Certain captive insurance companies also are exempt from many of the requirements. Covered Entities claiming an exemption under these provisions must file a Notice of Exemption on a prescribed form. In addition, certain charitable annuity societies, risk retention groups not chartered in New York, and accredited and certified reinsurers also are exempt.

What Systems and Information Must Be Protected?

Information Systems used to collect, process, and otherwise handle electronic information, and also any specialized systems such as for industrial/process controls, telephone switching, private branch exchange, and environmental control must be protected.

It also is necessary to protect electronic information that is not publicly available, (i) the tampering with which, or unauthorized disclosure, access or use of which, would have a material adverse impact on the Covered Entity; (ii) personal information (as the term is commonly used in other privacy and security requirements); or (iii) certain health related information.

What Is Required?

Administrative Safeguards

The new rules establish requirements for several policies, procedures, and actions, most of which have particular guidelines for documentation and content.

1. ***Risk Assessment.*** A risk assessment is required periodically, to include: (a) evaluating and categorizing cybersecurity risks and threats; (b) assessing the confidentiality and security of Information Systems and Nonpublic Information; and (c) mitigating identified risks. While not repeated throughout this summary, and not listed first in the regulation, nearly every other administrative and technical requirement of the regulation is tied to the risk assessment.
2. ***Cybersecurity Program.*** A cybersecurity program must be designed to protect the confidentiality, integrity, and availability of the Covered Entity's information systems, based on the required risk assessment, and to perform stated core cybersecurity functions.

3. ***Cybersecurity Policy.*** A cybersecurity policy approved by a senior officer or the governing board must provide for the protection of Information Systems and Nonpublic Information, based on the required risk assessment, and cover 14 specified areas including data governance and classification, systems and network security, data privacy, and incident response.
4. ***Vendor Management.*** Policies and procedures must be adopted to protect the security of Information Systems and Nonpublic Information accessible to third party vendors.
5. ***Personnel, Training, and Monitoring.*** A qualified individual must be designated as the Chief Information Security Officer (CISO), responsible for the cybersecurity program and the cybersecurity policy. The CISO must report at least annually in writing to the Covered Entity's governing board concerning cybersecurity. Other cybersecurity personnel must be engaged, trained, and updated on cybersecurity risks, and all personnel must have regular cybersecurity awareness training. The Covered Entity also must implement safeguards to monitor the activity of Authorized Users and detect unauthorized access to, use of, or tampering with Nonpublic Information.
6. ***Access Control.*** User access to Information Systems must be limited, and periodically reviewed.
7. ***Application Security.*** All internally and externally developed applications must be secure, and procedures related to application security must be reviewed, assessed, and updated periodically.
8. ***Testing and Auditing.*** Monitoring and testing of Information Systems for vulnerabilities must be conducted, including an annual penetration test and bi-annual vulnerability assessments. Systems able to reconstruct material financial transactions must be maintained. Records of Cybersecurity Events (which include unsuccessful attempts) must be maintained for five years.
9. ***Data Retention and Destruction.*** Personal information and health information no longer needed to be retained must be securely destroyed.
10. ***Incident Response Plan.*** A written incident response plan must be established to guide the response to, and recovery from, Cybersecurity Events.

Technical Safeguards

The new rules also require particular technical safeguards that extend beyond existing requirements in the United States.

1. ***Encryption.*** Generally, Nonpublic Information held or transmitted by the Covered Entity must be encrypted, both in transit and at rest. To the extent that encryption is determined to be infeasible, alternative compensating controls may be substituted, subject to review by the CISO at least annually.
2. ***Multi-Factor Authentication.*** To protect against unauthorized access to Nonpublic Information or Information Systems, each Covered Entity must use Multi-Factor Authentication or Risk-Based Authentication (as these terms are defined in the regulation). As an alternative, the CISO can approve other access controls that are at least as secure.

Notices

1. ***Breach Notices.*** Notice is required to the DFS superintendent as promptly as possible, but no later than 72 hours from a determination that a Cybersecurity Event has occurred, where notice is required to any other governmental or supervisory body, or self-regulatory agency, or where the event has a reasonable likelihood of materially harming any material part of the Covered Entity's operations.
2. ***Annual Compliance Certification.*** An annual compliance certification on the prescribed form must be submitted to the DFS superintendent by February 15 of each year, starting in 2018. Documentation supporting the certificate must be maintained for examination by the DFS for five years.
3. ***Confidentiality.*** All information provided by a Covered Entity pursuant to the regulation is exempt from disclosure under public records laws.

When Are the New Requirements Effective?

The regulation went into effect March 1, 2017, and Covered Entities will have until August 28 to comply with the first of the requirements. The table below indicates the actual compliance date for the various requirements, given the separate deadline for the annual compliance certificate, and three different transition periods of the regulation.

Compliance Date	Provision (with Regulation Section reference)
August 28, 2017	1. Cybersecurity Program (§ 500.02)
	2. Cybersecurity Policy (§ 500.03)
	3. CISO (§ 500.04(a))
	4. Access Privileges (§ 500.07)
	5. Cybersecurity Personnel (§ 500.10)
	6. Incident Response Plan (§ 500.16)
	7. Notice of Cybersecurity Event (§ 500.17(a))
	8. Filing for Limited Exemption (§ 500.19(d))

Compliance Date	Provision (with Regulation Section reference)
February 1, 2018	Annual Compliance Certification (§ 500.17(b))
March 1, 2018	1. CISO's annual report to the governing board (§ 500.04(b))
	2. Pen Testing and Vulnerability Assessments (§ 500.05)
	3. Risk Assessment (§ 500.09)
	4. Multifactor Authentication (§ 500.12)
	5. Cybersecurity Awareness Training for all Personnel (§ 500.14(a)(2))
September 1, 2018	1. Audit Trail (§ 500.06)
	2. Application Security (§ 500.08)
	3. Data Retention Limits (§ 500.13)
	4. Monitoring and Detection of activity of Authorized Users (§ 500.14(a)(1))
	5. Encryption (§ 500.15)
March 1, 2019	Third Party Vendor Security (§ 500.11)

What Steps Should Be Taken?

Each Covered Entity should start now to review existing programs, policies, and procedures to determine what is needed to satisfy the new requirements by the compliance dates mapped above. It is difficult to imagine any Covered Entity that would not have to take some action to comply with the new requirements. The following project steps are suggested for consideration by Covered Entities:

1. Determine whether or not the limited exemption for small businesses, or one of the other exemptions, would apply.
2. Identify and gather the project team, consisting of internal decision makers, IT personnel, and internal and experienced external legal and regulatory resources.
3. Identify outside resources that will be required for various functions, such as pen testing.
4. Catalogue all existing programs, policies, and procedures related to cybersecurity.
5. Assign team members responsible for reviewing and, as necessary, revising each existing program, policy, and procedure, and to draft any new documentation needed to comply with the new requirements.
6. Map the timeline of deliverables to achieve compliance by the effective date and the various transition dates.

ABOUT THE AUTHOR

Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com

Ted Augustinos is a partner at Locke Lord LLP advising clients in various industries on privacy and data protection, and on a wide variety of transactions, regulatory compliance, and corporate matters. He may be reached at ted.augustinos@lockelord.com.