THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 50 No. 13 July 19, 2017

THE NEW YORK STATE DFS CYBERSECURITY REGULATION: PREPARING FOR COMPLIANCE

Compliance with a significant portion of the New York State DFS cybersecurity regulation is required by August 28 of this year. The authors discuss the background and coverage of the regulation. They then address key provisions of the six basic functions and 14 topics of the required cybersecurity program. They note that the chairperson of the board of directors (or a senior officer) must certify annually to DFS that the program complies with the DFS rule.

Jeffrey P. Taft, Lawrence R. Hamilton, Stephen Lilley, and Matthew Bisanz *

Financial services companies, like businesses across the U.S. economy, have invested heavily in the development and implementation of risk-based cybersecurity practices. In doing so, financial services companies have assessed and responded to the specific threats facing their enterprises, and the particular systems they operate and data they hold. Substantial collaboration between the public and private sectors has supported this risk-based approach. In particular, the NIST Cybersecurity Framework reflects the joint efforts of public and private stakeholders to develop and implement risk-based security practices.[1]

One basic assumption behind this approach has been that there is no one-size-fits-all cybersecurity standard for American businesses. In a similar vein, key stakeholders in the private and public sectors have warned against the issuance of static, prescriptive regulations, which would mistakenly turn cybersecurity into a compliance exercise driven by static checklists

[1] NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (Feb. 12, 2014).

* *JEFFREY P. TAFT is a partner in the Financial Services Regulatory & Enforcement practice in Mayer Brown LLP's Washington D.C. office. LAWRENCE R. HAMILTON is a partner in the firm's insurance practice at its Chicago office. STEPHEN LILLEY is a litigation partner in the firm's Washington D.C. office. MATTHEW BISANZ is an associate in the Financial Services Regulatory & Enforcement practice in Mayer Brown LLP's Washington D.C. office. Each is a member of the firm's Cybersecurity and Data Privacy practice. Their e-mail addresses are jtaft@mayerbrown.com, lhamilton@mayerbrown.com, slilley@mayerbrown.com, and mbisanz@mayerbrown.com.*

RSCR Publications LLC Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call (937) 387-0473 or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 0884-2426.

rather than a dynamic exercise in enterprise risk management.

Nonetheless, a growing number of regulatory agencies at the federal and state levels also have pressed for mandatory adoption of certain cybersecurity practices. The cybersecurity regulation issued by the New York State Department of Financial Services ("DFS") is a noteworthy example of such efforts – and the resulting compliance burdens for businesses subject to DFS's authority. This regulation (the "DFS Rule") mandates detailed cybersecurity standards for all institutions authorized by DFS to operate in New York, including many banks, consumer financial services companies, insurance entities, and insurance professionals ("Covered Entities"). As a result, Covered Entities must ensure both that they have adopted cybersecurity programs that effectively manage cyber risk *and* that their programs achieve compliance with the DFS Rule.

In this article, we discuss key considerations for companies as they prepare to comply with the DFS Rule. In particular, we discuss the coverage of the DFS Rule and highlight some of the key requirements it imposes. While this discussion is by no means comprehensive, this article addresses some of the key issues that Covered Entities face as they work toward compliance with the DFS Rule.

BACKGROUND

On February 16, 2017, DFS finalized regulations that mandate cybersecurity standards for all institutions authorized by DFS to operate in New York, including many banks, insurance entities, and insurance professionals doing business in New York. The DFS Rule, titled "Cybersecurity Requirements for Financial Services Companies," implements a significantly revised version of DFS's September 13, 2016 proposal.[2] The DFS Rule became effective on March 1, 2017 and compliance with a significant portion of the regulation will be required on August 28, 2017 (e.g., cybersecurity program and policies, and incident response).[3] Further compliance dates in 2018 and 2019 apply to other elements of the regulation that are being phased in over time.[4] In addition, DFS issued frequently asked questions (the "FAQs") with corresponding answers on March 13, 2017 and has subsequently updated those FAQs.[5]

The DFS Rule makes clear that DFS wants cybersecurity to be a focus area for Covered Entities. DFS has issued a wide range of requirements and expects Covered Entities to address them in a risk-based, programmatic manner across their enterprises. The DFS Rule is largely keyed to the protection of "nonpublic information," which consists of three categories of data: (1) business-related information, the unauthorized disclosure or destruction of which would cause a material adverse impact on the Covered Entity; (2) certain personal information; and (3) certain health related information.[6]

The DFS Rule requires each Covered Entity to assess its specific cyber risk profile and design a program that addresses its risks in a robust fashion.[7] The DFS Rule calls for senior management engagement on this issue, and for a resulting program that will both ensure the safety and soundness of the institution and protect its customers.[8] Thus, the DFS Rule requires the Covered

[2] DFS, Cybersecurity Requirements for Financial Services Companies, XXXIX (No. 9) N.Y. Reg. 3 (Mar. 1, 2017) (*codified at* N.Y. Comp. Codes R. & Regs. tit. 23, pt. 500).

[3] *Id.* §§ 500.21, 500.22. As of August 28, 2017, a Covered Entity must have satisfied the (1) cybersecurity program; (2) cybersecurity policy; (3) Chief Information Security Officer designation; (4) access privileges; (5) cybersecurity personnel and intelligence; (6) incident response plan; and (7) Cybersecurity Event notification requirements.

[4] DFS Rule § 500.22.

[5] DFS, *Frequently Asked Questions Regarding 23 NYCRR Part 500* (updated June 29, 2017), *available at* http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

[6] DFS Rule § 500.01(g).

[7] *Id.* § 500.00.

[8] *Id.*

Entity to protect personal data and to address risks to the institution and the financial system more broadly.

COVERAGE

The DFS Rule applies to any Covered Entity, which is any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation, or similar authorization under the New York Banking, Insurance, or Financial Services Laws.[9] Determining whether and to what extent an institution and its affiliates fall within that scope is the necessary first step to any compliance analysis. Here we discuss some of the key features of the DFS Rule's coverage in two areas: (1) banking and consumer financial services and (2) insurance.

Banking and Consumer Financial Services

From the banking and consumer financial services perspective, there are a number of types of Covered Entities, including New York State-chartered banks and New York branches, agencies, and representative offices of foreign banks. Because of the broad definition, loan production offices and domestic representative offices arguably would also be captured as Covered Entities, but DFS has stated through the FAQs that New York branches and offices of out-of-state domestic banks would receive a degree of deference to home-state regulation through the 1997 Nationwide Cooperative Agreement for interstate branch supervision. National banks and federal branches and agencies of foreign banks, however, are not Covered Entities. That said, it remains unclear how the DFS intends to apply these regulations or the exemptions to types of Covered Entities that consist of offices where very limited functions are being performed. Depending upon how DFS interprets the 1997 Nationwide Cooperative Agreement and decides to handle these types of offices, an institution could face a situation where the "tail wags the dog." For example, an institution that was a Covered Entity solely because it has a loan production or representative office in New York still may be required to report all "Cybersecurity Events" occurring outside of New York to DFS.

In the consumer financial services field, Covered Entities would include institutions licensed as mortgage bankers, mortgage brokers, mortgage loan servicers, sales finance companies, check cashers, licensed lenders, and money transmitters.[10] Certain smaller financial services licensees may receive relief under the rule's exemptions.[11] However, two points about the exemptions merit emphasis. First, a Covered Entity will need to file a Notice of Exemption with DFS in order to rely on an exemption.[12] Second, exempt Covered Entities are not excused from complying with all of the requirements imposed by the DFS Rule.[13] For example, even an exempt Covered Entity needs to have a cybersecurity program.

Insurance

Under the DFS Rule, Covered Entities include insurance companies that are licensed to do business in New York, as well as New York-licensed insurance agencies, brokers, and claim-adjusting firms/third-party administrators. However, the DFS Rule exempts accredited reinsurers, certified reinsurers, non-New York risk retention groups, and charitable annuity societies from the definition of "Covered Entity."[14] DFS staff have also confirmed by e-mail to one of the authors that excess and surplus line insurers are not "Covered Entities."

The coverage analysis is more nuanced for insurance professionals, such as individual insurance agents and brokers. The term "Covered Entity" is defined as any New York-licensed "Person," and "Person" is defined as "any individual or any non-governmental entity."[15] It consequently is possible for an individual licensee to be a Covered Entity. However, there are two potential exemptions available to an individual licensee. First, employees, agents, representatives, or designees of a Covered Entity, even though they themselves fall within the definition of Covered Entity, are exempt from the DFS Rule and do not need to develop their own cybersecurity program to the extent they are covered by the Covered Entity's program.[16] Second, for those

[9] *Id.* § 500.01(c).

[10] We understand that the DFS is considering requests to exempt certain types of entities from the DFS Rule. These entities include passive servicers granted an exemption from the mortgage servicer registration requirements and exempt entities.

[11] *Id.* § 500.19.

[12] *Id.* § 500.19(e).

[13] *Id.* § 5001.19(b)-(d).

[14] *Id.* § 500.19(f).

[15] *Id.* § 500.01(c), (i).

[16] *Id.* § 500.19(b).

individual licensees who are not employees or representatives of any Covered Entity, it is likely that such persons would be eligible for one of the *de minimis* exemptions, such as the exemption for Covered Entities that have fewer than 10 employees.[17] Neither of those exemptions is self-executing, however. The exempt individuals will need to file a Notice of Exemption with DFS in order to avail themselves of either exemption (which can be done online at a DFS web portal).[18]

Insurance companies that are not themselves licensed in New York but that have New York-licensed affiliates are not Covered Entities. However, there are still a number of ways that they could be indirectly impacted.

First, the DFS Rule expressly permits a Covered Entity to meet the requirements of the regulation by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate.[19] To the extent a Covered Entity relies on an affiliate's cybersecurity program in whole or in part, that program must be made available for examination by DFS.

Second, the DFS has stated in the FAQs that when a subsidiary or other affiliate of a Covered Entity presents risks to the Covered Entity's information systems or the nonpublic information stored on those information systems, those risks must be evaluated and addressed in the Covered Entity's risk assessment, cybersecurity program, and cybersecurity policies.[20]

Third, an incidental effect could result from the interaction between the DFS Rule and the enterprise risk reporting requirement that applies to the ultimate control person of an insurance holding company system that includes one or more New York licensed insurers. It is possible that DFS will decide that every New York enterprise risk report should include a discussion of cybersecurity risks and specifically whether each member of the holding company system has implemented the types of protective measures specified in the DFS Rule.

Fourth, once an affiliated group of insurance companies has adopted a New York-compliant cybersecurity program for its New York-licensed members that are Covered Entities, there are likely to be practical incentives to implement it for the *non*-New York-licensed members of the group. A parent company may choose to implement its cybersecurity program both for its New York-licensed subsidiaries and for its other subsidiaries, for example, to ensure consistency and efficiency, and to help withstand scrutiny after a Cybersecurity Event at one of the subsidiaries that is *not* licensed in New York.

Finally, it merits note that a task force of the National Association of Insurance Commissioners (NAIC) has been trying for some time to develop an Insurance Data Security Model Law.[21] It is very possible that any model rule issued by that task force will resemble the DFS Rule. Any resulting standardization of state law around such an approach would make the New York/non-New York distinction less important.

KEY REQUIREMENTS

In many respects, the DFS Rule draws upon accepted best practices for cyber risk management. However, in doing so, the DFS Rule also layers on prescriptive requirements, adding specific compliance elements to the general need to pursue risk-based cybersecurity. As a result, even Covered Entities with mature cyber risk management programs will be well-served to ensure that their programs satisfy the various elements of the DFS Rule. Here, we describe some of the key requirements of the DFS Rule for Covered Entities.

Cybersecurity Program and Written Policies

The tailoring of a cybersecurity program to assessed risks and the development of supporting written policies and procedures are generally accepted best practices for cyber risk management. Both concepts are reflected in the NIST Cybersecurity Framework, for example, as well as in guidance from a variety of regulators.

Under the DFS Rule, a Covered Entity is required to maintain a cybersecurity program that is based on its risk assessment and designed to accomplish six basic functions, the first five of which map to the NIST framework.[22] The six functions are:

- identify and assess cybersecurity risks;
- protect information systems and nonpublic Information;

[17] *Id.* § 500.19(a).

[18] *Id.* § 500.19(e).

[19] *Id.* § 500.02(c).

[20] DFS, *Frequently Asked Questions*, *supra* note 5, #3.

[21] *See generally* NAIC, Cybersecurity (EX) Working Group, *available at* http://www.naic.org/cmte_ex_cswg.htm.

[22] DFS Rule § 500.02.

- detect Cybersecurity Events;
- respond to identified or detected Cybersecurity Events, and mitigate any negative effects;
- recover from Cybersecurity Events; and
- fulfill applicable regulatory reporting obligations.

A Covered Entity is required to implement this cybersecurity program through written policies that are based on its risk assessment.[23] The DFS Rule requires that a Covered Entity's policies address, to the extent applicable, the following 14 topics:

- information security;
- data governance and classification;
- asset inventory and device management;
- access controls and identity management;
- business continuity, and disaster recovery planning and resources;
- systems operations and availability concerns;
- systems and network security;
- systems and network monitoring;
- systems, application development, and quality assurance;
- physical security and environmental controls;
- customer data privacy;
- vendor and third-party service provider management;
- risk assessment; and
- incident response.

These policy elements are not defined in the DFS Rule and only some of them are elaborated upon in the context of other requirements. Moreover, broad reading of some of the terms could create duplication (e.g., a broad reading of "Customer data privacy" could either duplicate issues relating to "Information security," or incorporate a range of data collection and use issues beyond the stated scope of the regulation). Generally, however, the inclusion of these policy elements in the DFS Rule is not surprising, as each is a familiar element of cyber risk management programs. Consequently, most large financial services companies already will have thought through most, if not all, of these issues. Significantly, however, the DFS Rule makes clear that Covered Entities will need to address these issues through written policies that are approved by senior management.[24] As a result, even Covered Entities that already have sophisticated, risk-based cybersecurity programs will want to consider whether their policies are adequately documented for purposes of the DFS Rule; whether they are appropriately tailored to assessed risks; and whether documentation and supporting processes give senior management the information it needs to approve the written policies and procedures. Covered Entities will also want to ensure that the inevitable emphasis on compliance with these specific requirements does not turn cybersecurity into a check-the-box compliance exercise.

Risk Assessments and Penetration Testing

The risk assessment process and resulting documentation are likely to be particularly important to ensuring compliance with the regulation. As noted above, a Covered Entity's cybersecurity policy must be based on its risk assessment.

Under the DFS Rule, a Covered Entity must conduct a periodic risk assessment of its information systems to inform its cybersecurity program.[25] The risk assessment needs to reflect changes in controls and technology, as well as evolving threats and cybersecurity risks to the Covered Entity. The risk assessment must be documented, be conducted in accordance with written policies and procedures, and include specifications for how the Covered Entity will accept or mitigate identified risks.

Compliance with this risk-assessment provision is required by March 2018.[26] Covered Entities may well benefit from this delayed compliance date given the complexity of developing effective procedures for identifying and then accepting or mitigating risks. A Covered Entity that fails to get this process right may

[23] *Id.* § 500.03.

[24] *Id.*

[25] *Id.* § 500.09.

[26] *Id.* § 500.21(b)(1).

overlook or overstate the risks that it actually faces, or may prioritize issues inaccurately. And, because of the documentation requirements, any such errors may be magnified in the harsh light of regulatory scrutiny or private litigation after a data breach or other cybersecurity incident.

In addition, the DFS Rule specifically directs Covered Entities to perform (1) annual penetration testing based on relevant identified risks in accordance with the risk assessment and (2) biennial vulnerability assessments to gauge the effectiveness of its cybersecurity program.[27] The DFS Rule provides an exception, however, for Covered Entities that engage in effective continuous monitoring or use other systems to identify vulnerabilities. In the FAQs released through its website, DFS clarified that continuous monitoring means that the Covered Entity "has the ability to continuously, on an ongoing basis, detect changes or activities within a Covered Entity's Information Systems that may create or indicate the existence of cybersecurity vulnerabilities or malicious activity," and that manual log review and firewall configurations would not qualify under this definition.[28] Covered Entities will likely want to think carefully about relying on this exception. Practically speaking, unless DFS provides further clarification, it appears likely that many Covered Entities will perform the penetration testing and vulnerability assessments contemplated by the DFS Rule.

Chief Information Security Officer

The DFS Rule also requires each Covered Entity to designate a Chief Information Security Officer (or "CISO").[29] The CISO's required duties include:

- overseeing and implementing the Covered Entity's cybersecurity program and enforcing its policy;
- providing an annual report to the board that assesses material cybersecurity risks, compliance with the cybersecurity program, Cybersecurity Events, and the overall effectiveness of the cybersecurity program;
- approving and periodically reviewing the application of security policy;
- approving any nonuse of multi-factor authentication on external networks; and
- annually reviewing the approved use of compensating controls in place of encryption.

Certain CISO functions can be outsourced to an affiliate or third-party service provider, but a Covered Entity nevertheless remains responsible for complying with the DFS Rule's CISO requirements.

A Covered Entity is also required to employ cybersecurity personnel sufficient to maintain and execute the Covered Entity's cybersecurity program.[30] The cybersecurity personnel must be subject to ongoing subject-matter training requirements, and all of a Covered Entity's personnel must undergo regular cybersecurity awareness training that is updated to reflect the risks identified in the periodic risk assessment. The Covered Entity also must implement risk-based controls to monitor the activities of authorized personnel to detect unauthorized access or use of nonpublic information.[31]

Annual Certification

Beginning in 2018, the chairman of the board of directors (or a senior officer) of the Covered Entity is required to submit an annual certification to DFS by February 15 of each year.[32] The certification form is an appendix to the DFS Rule, and it states that to the best of the certifying individual's knowledge, the Covered Entity's cybersecurity program complies with the DFS Rule. DFS has indicated in its FAQs that if a Covered Entity is not in compliance with all applicable requirements of the DFS Rule, then it is not permitted to submit a certification. The DFS Rule thus creates a binary world. Either a Covered Entity is in compliance and it so certifies, or it is not in compliance and it cannot certify. To the extent that a Covered Entity that is in compliance identifies areas of needed improvement, it is required to document those issues and the plan for remediating them, to keep that documentation available for inspection by DFS, and to retain it for five years.

Under state corporate law, the business and affairs of a corporation are managed by or under the direction, and subject to the oversight, of its board of directors. The directors have fiduciary duties, including a duty of care.

---

[27] *Id.* § 500.05.

[28] DFS, *Frequently Asked Questions*, *supra* note 5, #14.

[29] DFS Rule § 500.04.

[30] *Id.* § 500.10.

[31] *Id.* § 500.14.

[32] *Id.* § 500.17(b).

Under the DFS Rule, directors and officers of Covered Entities now have additional duties. In particular, boards will want to prepare for:

- making sure the Covered Entity has a written cybersecurity policy that is in compliance with the DFS Rule,
- the appointment of a CISO and receiving regular reports from the CISO; and
- the annual certification to DFS that the Covered Entity is in compliance.

As a result of the DFS Rule, directors and officers who do not take steps to oversee compliance arguably could be deemed to be breaching their duty of care to the Covered Entity. If a Covered Entity is not in compliance with the DFS Rule – and if that noncompliance leads to a regulatory enforcement action or a private lawsuit against the company – there potentially could be exposure to a directors' and officers' liability (D&O) claim. While the business judgment rule and other defenses may well prevent such a claim from succeeding, board members likely will want to consider the requirements of the DFS Rule. Moreover, scrutiny of a Covered Entity's compliance with the DFS Rule may well become part of the D&O insurance underwriting process in order to address any associated risk exposure.

Incident Response

A Covered Entity must put in place a written incident response plan designed to enable the entity to promptly respond to and recover from a Cybersecurity Event materially affecting the confidentiality, integrity, or availability of its systems.[33] The DFS Rule specifically requires an incident response plan to address seven areas consisting of:

- internal processes for responding to a Cybersecurity Event;
- goals of the plan;
- definition of clear roles, responsibilities, and levels of decision-making authority;
- external and internal communications and information sharing;
- identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
- documentation and reporting regarding Cybersecurity Events and related incident response activities; and
- the evaluation and revision as necessary of the plan following a Cybersecurity Event.

While most Covered Entities will already have an incident response plan, the DFS Rule may require certain changes.

First, a Covered Entity may need to broaden the scope of incidents covered by its plan. The DFS Rule broadly defines a "Cybersecurity Event" as any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse, an information system or information stored on such information system.[34] The DFS Rule's definition thus goes well beyond incidents involving customer or sensitive personal information, and would capture other hacking and attempted intrusions into the Covered Entity's systems.

Second, a Covered Entity may well need to modify its incident response plan to the extent necessary to reflect the new reporting obligations to DFS. Under the DFS Rule, Covered Entities are required to notify DFS within 72 hours after becoming aware of any Cybersecurity Event (1) which has a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" or (2) for which notice must be provided to any government body, self-regulatory agency, or other supervisory body.[35] Under the first category of reportable events, the obligation to report a Cybersecurity Event is limited to events with a reasonable likelihood of materially harming any part of its normal operations. Despite this materiality qualifier, this could require a Covered Entity to report a Distributed Denial of Service (DDoS) attack or other event that interrupts a Covered Entity's customer-facing website or its ability to offer products and services. The second category of reportable events may have broader ramifications from a reporting perspective and will require Covered Entities to track and coordinate their responses. For example, if a Covered Entity files

[33] *Id.* § 500.16.

[34] *Id.* § 500.01(d).

[35] *Id.* § 500.17(a).

notification with another state regarding a breach involving customer information, it would need to notify DFS even though no New York residents were involved and no notice was required under the New York data breach law. For banks and money services businesses who file Suspicious Activity Reports (SARs) pursuant to FinCEN guidance from October 2016 regarding "Cyber-Events and Cyber-Enabled Crime," there may also be an obligation to file notice with DFS of the underlying Cybersecurity Event (while not disclosing the filing of the SAR).

Third-Party Service Providers

Third-party vendor risk management has been a hot-button issue with the federal banking regulators for many years and the subject of substantial recent compliance guidance. Its importance to cybersecurity was made clear by a number of high-profile data breaches where vendors were identified as the point of entry into the company's systems. DFS has tried to address this concern in the regulations by (1) broadly defining third-party service provider as any person who (a) is not an affiliate of the Covered Entity, (b) provides services to the Covered Entity, and (c) maintains, processes, or otherwise is permitted access to nonpublic information through its provision of services to the Covered Entity and (2) requiring Covered Entities to take a number of steps to ensure that these service providers have adequate cybersecurity policies.[36] In contrast, third-party service providers do not have any direct obligations under the DFS Rule despite the fact that Covered Entities will be required to pass through many of the requirements via minimum mandatory contractual terms.

As was seen in the context of the Gramm-Leach-Bliley Act's Safeguarding Rules and the Massachusetts data security regulation, the DFS Rule has a long phase-in period with respect to vendor compliance obligations. Between now and March 1, 2019, Covered Entities will need to (1) identify their relevant vendors, (2) review their vendor contracts, and (3) provide vendors with notices of any required changes. As companies learned from the Gramm-Leach-Bliley Act and the Massachusetts security regulation, modifying their vendor contracts can be time-consuming. Also, given the broad but somewhat ambiguous definition of "third-party service provider," some vendors may assert that they are outside the scope of the definition. In particular, one likely question is whether the vendor maintains, processes, or is otherwise permitted access to nonpublic information through its provision of the services to the Covered Entity.

CONCLUSION

Whether the DFS Rule proves to be a model for other state regulators remains an open question. What is clear at this point is that implementation of the DFS Rule is likely to be watched closely by other state regulators. Covered Entities accordingly will benefit from focusing on compliance with the DFS Rule – but doing so in a way that does not distract them from effective cyber risk management processes. Indeed, businesses will want to pay attention to the effective coordination of compliance and risk management functions. In that way, they will be best situated to effectively manage both regulatory and operational risk once compliance with the DFS Rule is required. ■

[36] *Id.* §§ 500.01, 500.11.