



NYS DFS 500 Amendment



What the NYS DFS 500 Amendment means for regulated entities

The New York State Department of Financial Services (NYS DFS) is responsible for ensuring the safety and soundness of financial institutions, protecting consumers, and promoting the growth of the NY financial services sector. It supervises thousands of institutions with assets of more than \$8.8 trillion. In 2017, the NYS DFS enacted a Cybersecurity Regulation (23 NYCRR Part 500) which was intended to ensure that covered entities establish and maintain strong cybersecurity practices to protect consumers and to defend the stability of the financial system against the increasing pace and growing sophistication of cyber criminals targeting the industry.

The regulation applies to banks, insurance companies, mortgage lenders, and other financial institutions operating in the state of New York, not just those based in New York. Non-compliance can result in multi-million-dollar penalties. A dozen firms have already been disciplined, with the average penalty being about \$3,000,000.

Sometime in 2023, the NYS DFS will implement revisions to the Cybersecurity Regulation. These revisions, known as the Second Amendment, will require changes in how covered entities operate if they are to remain compliant.

Why is this happening?

The NYS DFS found shortcomings in the existing regulations. Looking at operational conditions and drawing findings from enforcement actions, the department is now looking to eliminate ambiguity for covered entities and improve protection for consumers and the financial industry.

Under the original regulation, covered entities were required to:

- Perform risk assessments
- Designate a qualified CISO to implement and enforce a cybersecurity program and policies
- Maintain effective cybersecurity functions, including identity and access management, third-party service provider oversight, and incident response
- Notify NYS DFS of cybersecurity incidents within 72 hours of occurrence and submit an annual certification of their compliance with the regulation

There have been 47 enforcement actions — the legal measures that NYS DFS takes against covered entities that violate its regulations — since 2020. Of those, 11 were related to the Cybersecurity Regulation.

All the actions stemmed from a security incident except one, which was due to violations identified through a regulatory exam. The average monetary penalty has been about \$3 million. Findings from the enforcement actions, as well as the evolving threat landscape, have led to the additions and changes that are part of the Second Amendment.

Changes raise the bar for covered entities

All covered entities that have been compliant under the NYS DFS Cybersecurity Regulation must be aware of and prepare for the changes coming under the Second Amendment. Reversesec has identified a number of “bar raisers”—changes that will require action even from companies currently in compliance—that should have the attention of CEO and CISO alike.

These include:

- Annual Certification of Compliance must be signed by the CEO
- CISO must have adequate authority and sufficient resources to manage cybersecurity risks
- Updated and in-depth requirements for risk assessments
- Entities must notify NYS DFS and provide justification if they make a ransomware payment
- The board of directors (BoD) is responsible for risk management oversight
- The BoD must have cyber security knowledge and expertise

- Workplace social engineering exercises—for example, phishing simulations—must be conducted
- Business continuity/disaster recovery plan development and maintenance

These requirements simplify matters in some ways by being more specific in expectations—but they also place more responsibility on covered entities. Planning ahead and making the necessary changes before the Second Amendment comes into effect can save time, money, and reputational damage.

The Second Amendment also creates a new category called “Class A companies,” which are larger institutions subject to heightened requirements. These Class A companies have annual revenues of at least \$20 million in the state of New York and have over 2,000 employees or at least \$1 billion in annual revenue, whether from inside or outside of New York.

How Reversesec can help

Reversesec analyzed the details of NYS DFS compliance actions in the context of the previous regulation and the new regulation. We found the changes to the regulation to be substantial. At a high level, of the 276 sections in the document, 114 (41%) are new, 38 (14%) have been amended, and 124 (45%) carry over from the original regulation. With more than half of the sections being new or revised, a thorough assessment of an organization's status is needed to ensure continued compliance.

We also found that the NYS DFS 500 Second Amendment included 72% of the mitigating controls that could have prevented the incidents, versus 54% in the original regulation. This shows it is important that financial institutions continue to proactively manage their risks and security posture, in addition to maintaining compliance with regulatory requirements. Reversesec expects at least 10 of the changes will be costly and complex for regulated entities to implement and manage effectively, and at least 34 others are likely to present significant challenges. Reversesec believes the following new requirements will be the most impactful to regulated entities:

1. Timely vulnerability remediation
2. Automated vulnerability scans and manual reviews
3. Asset inventory
4. Centralized SIEM solution
5. Endpoint detection and response solution
6. Privileged access management solution
7. Business continuity/disaster recovery plan development, maintenance, and testing
8. Secure backups and backup/restore testing
9. Annual independent audit of the cybersecurity program
10. Risk assessments performed by an external expert every three years

The scope of the changes coming means it is important for covered entities to begin planning for the changes as soon as possible. The changes will affect budgets, staffing, and ways of working. They will require substantial change management to ensure that staff follow through on changes to policies and procedures. And good planning starts with an assessment of the current state of cybersecurity health. Reversesec offers a range of services that can help, including—among others—risk assessment, cybersecurity program design, and incident response plan testing.

The coming changes are not a one-time event that can be fulfilled and filed away. Companies must recognize that compliance with NYS DFS requirements is an ongoing process. The cybersecurity regulatory environment will continue to become more rigorous and prescriptive, with other regulators likely to follow NYS DFS and developments in European Union compliance requirements. Moving decisively to understand and implement the coming changes will reduce the risk of both cybersecurity incidents and enforcement actions.

To learn more about the NYS DFS Cybersecurity Regulation (23 NYCRR Part 500) and how Reversesec can help you plan with purpose to meet the challenges, please contact us online at reversesec.com.



About ReverseSec

ReverseSec, a new name in cybersecurity consulting, helps organizations worldwide tackle their most complex cybersecurity challenges.

With a focus on continuous research, practical solutions and knowledge sharing, ReverseSec's findings provide the rationale behind informed security decisions.

With over 30 years of experience, ReverseSec brings together the expertise of renowned companies MWR Infosecurity, F-Secure, WithSecure, Digital Assurance, nSense, and Inverse Path.

ReverseSec.com

REVERSESEC