



Amended Cybersecurity Regulation

Second Amendment 23
NYCRR Part 500

Effective November 1, 2023

Agenda

1. Background
2. Amendment Process
3. Rules Better Tailored to Business' Risk Profiles
4. Implementation and Compliance Timeline
5. Upcoming Requirements Explained
6. Resources



Background



Cybersecurity Regulation Background

First-in-the-nation cybersecurity regulation adopted in 2017

- Financial services sector is a significant target of cyber threats
- Cyber attacks cause significant financial losses for New York businesses and consumers

Part 500 became the model for many federal and state regulations, including the FTC Safeguards Rule, NAIC Model Law, and CSBS Nonbank Model Data Security Law.



Who Is Covered?

Part 500 applies to all entities and individuals chartered, licensed, or approved to operate in New York state by DFS under Banking, Insurance, and Financial Services Laws (Covered Entities or CEs). (See §500.1(e) for exact language of the definition)

Entities range from small brokers to the largest and most complex international banking and insurance entities and include:

- Insurance companies, producers, agents and brokers
- Banks, trusts and foreign bank branches
- Mortgage banks, brokers and lenders
- Money transmitters, check cashers, and other non-depository financial institutions



Amendment Process



Research and Lessons Learned

Research

- DFS examined the cybersecurity programs of hundreds of regulated entities.
- DFS investigated hundreds of cyber incidents reported by regulated entities.
- DFS discussed current industry practice with internal and external experts.

Lessons Learned

- The overwhelmingly majority of cyber incidents involve cybercriminals using the same common, well-known techniques.
- Organizations can protect themselves from 90+ percent of the cyber threats they face daily.
- Implementation of standard cyber controls is essential to protect against cyber threats.



Why Amend the Regulation?

Significant changes in the cybersecurity landscape since 2017:

- Threat actors have become more sophisticated and prevalent
- Cyber attacks have become easier to perpetrate (e.g., via ransomware as a service)
- Cyber attacks have become more expensive to remediate
- More and better controls are available to manage cyber risk at reasonable cost

The amended regulation incorporates current best practices to better protect businesses, consumers, and their data from these emerging cyber threats.



Thorough and Open Process

DFS published proposed revisions and detailed information on the Department's Cybersecurity Resource Center:

- June 2021: Guidance on Ransomware
- October 2021: Guidance on Adoption of an Affiliate's Cybersecurity Program
- December 2021: Guidance on Multifactor Authentication (MFA)
- FAQs and other detailed information



Thorough and Open Process

DFS published drafts of the Second Amendment and considered more than 1200 comments:

- July 2022: Pre-proposal published on DFS website (300+ comments received)
- November 2022: Proposed Second Amendment published in New York State Register (600+ comments received)
- June 2023: Revised Proposed Second Amendment published in New York State Register (300+ comments received)

DFS publicized the opportunity to submit comments, including via emails to regulated entities and individuals regarding the proposal.

DFS announced adoption of the Second Amendment on November 1, 2023.



Emphasizing Governance

The Amendment maintains Part 500's **risk-based approach** and continues to require CEs to implement comprehensive cybersecurity programs based on their risk assessments that:

- Protect the confidentiality, integrity, and availability (CIA) of their information systems and the nonpublic information (NPI) stored on them.
- Cover recognized core cybersecurity functions of identifying risks, defending against unauthorized access, and detecting, responding to, and recovering from cybersecurity events.
- Allow each CE to assess its specific risk profile and design a program that addresses their particular risks (given the wide range of sizes and business types DFS regulates).

This approach has proven flexible and durable.



Rules Better Tailored to Business' Risk Profiles



Tailored Requirements

Requirements are now tailored to better fit different sizes and types of entities in New York State's financial services sector. The tailored requirements take into account DFS-regulated entities' risks and resources, and have been amended to include:

1. New requirements for Larger Entities
 - (§§500.1(d), 500.2(c), 500.7(c), and 500.14(b))
2. Expanded scope of Covered Entities that qualify for limited exemptions
 - (§500.19(a), (c), and (d))
3. More types of Covered Entities that qualify for full exemptions
 - (§500.19(b), (e), and (g))



Three Categories of Covered Entities

Large (“Class A”) Companies

Must comply with all requirements.

Small (“Exempt”) Companies

Expanded availability of limited and full exemptions for some Covered Entities.

Non-Class A, Non-Exempt (“Standard”) Companies

Must comply with most requirements. A majority of Covered Entities are in this category.



Class A Qualifications and Requirements

Have at least \$20 million in gross annual revenue in each of the last two years from **ALL business operations of the Covered Entity** and the **New York business operations of its Affiliates**, and either:

- More than 2,000 employees averaged over the last two years, **including employees of both the Covered Entity and all Affiliates** no matter where located, or
- Over \$1 billion in gross annual revenue in each of the last two years from **ALL business operations of the Covered Entity and all Affiliates** no matter where located.

For purposes of this definition, when calculating the number of employees and gross annual revenue, **Affiliates shall include only those that share information systems, cybersecurity resources or all or any part of a cybersecurity program with the covered entity.** (§500.1(d))



More Businesses Qualify for Full Exemptions

Previously

These Covered Entities qualified as fully exempt:

- Charitable annuity societies, non-NY Chartered risk retention groups, and accredited reinsurers or certified reinsurers under Part 125 of the Insurance regs (§500.19(f))
- Employees, agents, representatives, or designees of another Covered Entity, as long as they are covered by the cybersecurity program of that other Covered Entity (§500.19(b))

Now

Those, and more Covered Entities qualify as fully exempt:

- Wholly owned subsidiaries covered by the cybersecurity program of another Covered Entity (i.e., parent Covered Entity) (§500.19(b))
- Inactive individual insurance brokers (for 1+ years) who do not otherwise qualify as a Covered Entity (§500.19(e))
- Inactive individual insurance agents and individual MLOs (§500.19(g))
- Reciprocal jurisdiction reinsurers recognized pursuant to 11 NYCRR Part 125 (§500.19(g))



More Businesses Qualify for Limited Exemptions

More companies now qualify for limited exemptions.

There are 3 types of Covered Entities that qualify for limited exemptions:

1. Entities that do not have information systems and do not maintain Nonpublic Information (NPI) (§500.19(c))
2. Captive insurance companies (Covered Entities under Article 70 of the Insurance Law) that do not and are not required to maintain NPI (§500.19(d))
3. Small businesses (§500.19 (a))

While 1 and 2 remain unchanged, the parameters to qualify for the **small business limited-exemption** have changed.



Small Business Qualifications Expanded

To qualify for the small business limited-exemption, a Covered Entity must have less than:

- 20 employees and independent contractors including those of its Affiliates;
- \$7.5 million in gross annual revenue including revenue from the New York business operations of Affiliates; or
- \$15 million in year-end total assets including those of its Affiliates

Small Companies

Expanded availability of limited and full exemptions for Covered Entities.



Standard Companies

- Covered Entities that do not qualify for full or limited exemptions or as Class A Companies, will be referred to for this training as “Standard” Companies
- Standard companies must comply with most, but not all, requirements in the amended regulation.
- The majority of DFS-regulated entities are Standard Companies.

Non-Class A, Non-Exempt (“Standard” Companies)

Must comply with most requirements. A majority of Covered Entities are in this category.



Implementation and Compliance Timeline



Phased Compliance Deadlines

Adoption Date Nov. 1, 2023

- 500.19: Exemption parameters
- 500.20: Enforcement provisions



180 Days

Apr. 29, 2024

- 500.2(c): Class A requirement to design and conduct independent audits
- 500.3: New areas to include in cybersecurity policies
- 500.5(a)(1), (b), and (c): new vulnerability management requirements
- 500.9: New Risk Assessment requirements
- 500.14(a)(3): new cybersecurity awareness training
- All other provisions not mentioned elsewhere



1 Year

Nov. 1, 2024

- 500.4: Cybersecurity governance
- 500.15: Encryption
- 500.16: Incident response and business continuity
- 500.19(a): Small businesses increased requirements (MFA, cybersecurity training)

18 Months

May 1, 2025

- 500.5(a)(2): Automated information systems scan requirements
- 500.7: Access privileges & management; Class A requirements to monitor privileged access, implement PAM and commonly-used password blocking
- 500.14(a)(2): protect against malicious code
- 500.14(b): Class A requirements for EDR and SIEM



2 Years

Nov. 1, 2025

- 500.12: MFA
- 500.13(a): Asset inventory



30 Days

Dec. 1, 2023

- 500.17(a): Cybersecurity incident notifications
- 500.17(b): Annual notification requirements
- 500.17(c): New Extortion payment notifications



Key Dates

November 1, 2023

Section 500.19

More businesses qualify for limited and full exemptions.

Exempt Companies

December 1, 2023

Section 500.17

Reporting cybersecurity events to DFS continues to be required. Ransomware deployment and any ransom payments made must be reported as well.

Limited-Exempt Companies
Standard Companies
Class A Companies

By April 15, 2024

Section 500.17(b)

Submit either a Certification of Material Compliance or an Acknowledgment of Noncompliance for calendar year 2023 signed by the highest-ranking executive at the CE and the CISO.

Limited-Exempt Companies
Standard Companies
Class A Companies



Key Dates

Section 500.9

Risk assessments, which continue to be required, must be reviewed and updated at least annually and whenever a change in the business or technology causes a material change to the business' cyber risk.

Limited-Exempt Companies
Standard Companies
Class A Companies

Section 500.3

Cybersecurity policies must be annually reviewed and approved by the senior governing body or a senior officer and procedures must be documented. After assessing risks, Covered Entities must update policies and procedures to address specified additional areas as needed.

Small Business Limited-Exempt Companies
Standard Companies
Class A Companies

Section 500.14(a)(3)

Cybersecurity awareness training for all personnel must now include social engineering and must be provided at least annually.

Standard Companies
Class A Companies



Key Dates

April 29, 2024 (continued)

Section 500.5(a)(1), (b), and (c)

- Conduct at least annual penetration testing from inside and outside information systems' boundaries.
- Have a monitoring process in place to promptly inform of new security vulnerabilities.
- Prioritize and timely remediate vulnerabilities based on risk.

Standard Companies
Class A Companies

Section 500.2(c)

Design and conduct independent audits of cybersecurity program.

Class A Companies

November 1, 2024

Section 500.12(a)

Implement multi-factor authentication (MFA) requirements as outlined in this section of the regulation to the extent they are not already in place.

Small Business Limited-
Exempt Companies



Key Dates

November 1, 2024 (continued)

Section 500.14(a)(3)

Cybersecurity awareness training for all personnel must now include social engineering and must be provided at least annually.

Section 500.15

- Implement a written policy requiring encryption that meets industry standards.
- Use of effective compensating controls for encryption of NPI at rest that have been approved by the CISO may continue to be used, but that approval must now be in writing.
- Effective alternative compensating controls for encryption of NPI in transit over external networks can no longer be used.

Small Business Limited-Exempt
Companies

Standard Companies
Class A Companies



Key Dates

November 1, 2024 (continued)

Section 500.4

- CISO's written report to senior governing body must include plans for remediating material inadequacies.
- CISO required to timely report to senior governing body or senior officer(s) on material cybersecurity issues, such as significant cybersecurity events and significant changes to the cybersecurity program.
- Senior governing body must exercise oversight of its cybersecurity risk management, as outlined in this section of the regulation.

Standard Companies

Class A Companies



Key Dates

November 1, 2024 (continued)

Section 500.16

- Incident response plans continue to be required, but they must be updated as specified.
- Ensure business continuity and disaster recovery plans that are reasonably designed to address a cybersecurity-related disruption are in place.
- Covered entities must also:
 - Train all employees involved in plan implementation;
 - Test plans with critical staff;
 - Revise plans as necessary;
 - Test the ability to restore critical data and information systems from backups; and
 - Maintain and adequately protect backups necessary to restore material operations.

Standard Companies

Class A Companies



Key Dates

May 1, 2025

Section 500.7

- Implement enhanced requirements regarding limited user access privileges.
- Review access privileges and remove/disable accounts and access that are no longer necessary.
- Disable or securely configure all protocols that permit remote control of devices.
- Promptly terminate access following personnel departures.
- Implement a reasonable written password policy.

Small Business Limited-Exempt Companies

Standard Companies

Class A Companies

Section 500.5(a)(2)

Conduct automated scans of information systems and manual reviews of systems not covered by those scans to discover, analyze, and report vulnerabilities at a frequency determined by the risk assessment, and promptly after any material system change.

Standard Companies

Class A Companies



Key Dates

May 1, 2025 (continued)

Section 500.14(a)(2)

Implement controls to protect against malicious code, including those that monitor and filter web traffic and email to block malicious content.

Section 500.14(b)

- Implement an endpoint detection and response solution and a centralized logging and security event alert solution.
- CISO can approve reasonably equivalent or more secure compensating controls, but approval must be in writing.

Standard Companies
Class A Companies

Class A Companies

November 1, 2025

Section 500.12

- Implement MFA for all individuals accessing any of a CE's information systems.
- CISO can approve use of reasonably equivalent or more secure compensating controls, to be reviewed at least annually.

Small Business Limited-Exempt
Companies
Standard Companies
Class A Companies



Key Dates

November 1, 2025 (continued)

Section 500.13(a)

- Implement written policies and procedures designed to produce and maintain a complete, accurate and documented asset inventory of information systems.
- Policies and procedures must include a method to track specified key information for each asset, such as owner and location, and frequency required to update and validate asset inventory.

Limited-Exempt Companies

Standard Companies

Class A Companies



Upcoming Requirements Explained



Key Dates

November 1, 2023

Section 500.19

More businesses qualify for limited and full exemptions.

Exempt Companies

December 1, 2023

Section 500.17

Reporting cybersecurity events to DFS continues to be required. Ransomware deployment and any ransom payments made must be reported as well.

Limited-Exempt Companies
Standard Companies
Class A Companies

April 15, 2024

Section 500.17(b)

Submit either Certification of Material Compliance or Acknowledgment of Noncompliance for calendar year 2023. Both annual submissions must be signed by the highest-ranking executive and the CISO.

Exempt Companies
Standard Companies
Class A Companies



Reporting Cybersecurity Incidents

All CEs are required to report certain cybersecurity events to DFS within 72 hours of determining a reportable Cybersecurity Event has occurred. Reportable events are those that:

- Impact the CE and require it to notify another government body, self-regulatory agency, or any other supervisory body, or
- Have a reasonable likelihood of materially harming any material part of the normal operation of the CE, or
- Beginning on **December 1, 2023**, result in the deployment of ransomware within a material part of the CE's information systems.

As of **December 1, 2023**, CEs also will be required to:

- Report such events whether they occur at the CE itself, at an affiliate, or at a third-party service provider.
- Promptly provide DFS with any information requested regarding the event, and update DFS “with material changes or new information previously unavailable.”



Reporting Extortion Payments

As of **December 1, 2023**, Covered Entities are required to:

- Notify DFS within 24 hours of any extortion payment made; and
- Within 30 days of a payment, provide DFS with a written description of the reasons payment was necessary, alternatives to payment considered, diligence performed to find alternatives to payment and to ensure compliance with applicable regulations, including those of the Office of Foreign Assets Control. (500.17(c))

DFS continues to discourage making extortion payments.

Extortion payments and cybersecurity incidents should still be reported online through the DFS Portal.



Key Dates

November 1, 2023

Section 500.19

More businesses qualify for limited and full exemptions.

Exempt Companies

December 1, 2023

Section 500.17

Notifying DFS of cybersecurity events continues to be required. Ransomware deployment and any ransom payments made must be reported.

Exempt Companies
Standard Companies
Class A Companies

April 15, 2024

Section 500.17(b)

Submit either a Certification of Material Compliance or an Acknowledgment of Noncompliance for calendar year 2023 signed by the highest-ranking executive at the CE and the CISO.

Limited-Exempt Companies
Standard Companies
Class A Companies



Submitting an Annual Compliance Notification

As of **April 15, 2024**, Covered Entities will have the option to submit either a certification that they have **materially complied** with the requirements of Part 500 during the prior calendar year, or an **Acknowledgement of Noncompliance**, which:

- Acknowledges that, for the prior calendar year, the Covered Entity did not materially comply with all applicable requirements of Part 500;
- Identifies all sections of Part 500 that the Covered Entity has not complied with and describes the nature and extent of such noncompliance; and
- Provides a remediation timeline or confirmation that remediation is complete.

The Certifications of Material Compliance and Acknowledgments of Noncompliance must be signed by the highest-ranking executive at the Covered Entity and the CISO.



Key Dates

April 29, 2024

Section 500.9

Risk assessments, which continue to be required, must be reviewed and updated at least annually and whenever a change in the business or technology causes a material change to the business' cyber risk.

Limited-Exempt Companies
Standard Companies
Class A Companies

Section 500.3

Cybersecurity policies must be annually reviewed and approved by senior governing body or senior officer(s) and procedures must also be documented. After assessing risks, Covered Entities must update policies and procedures to address specified additional areas as needed.

Exempt Companies
Standard Companies
Class A Companies

Section 500.14(a)(3)

Cybersecurity awareness training must now include social engineering and must be provided at least annually.

Standard Companies
Class A Companies



New Risk Assessment Requirement

Instead of periodically, CEs must now review and update risk assessments:

- At least annually, and
- “Whenever a change in the business or technology causes a material change to the covered entity’s cyber risk.” (§500.9)

New definition of Risk Assessment: *“The process of identifying, estimating and prioritizing cybersecurity risks to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, customers, consumers, other organizations and critical infrastructure resulting from the operation of an information system. Risk assessments incorporate threat and vulnerability analyses, and consider mitigations provided by security controls planned or in place.”* (§500.1(p))



Key Dates

April 29, 2024

Section 500.9

Risk assessments, which continue to be required, must now be reviewed and updated at least annually and whenever a change in the business or technology causes a material change to the business' cyber risk.

Class A Companies
Non-Class A, Non-Exempt
Exempt Companies

Section 500.3

Cybersecurity policies must be annually reviewed and approved by senior governing body or senior officer(s) and procedures must also be documented. After assessing risks, Covered Entities must update policies and procedures to address specified additional areas as needed.

Small Business Limited-Exempt Companies
Standard Companies
Class A Companies

Section 500.14(a)(3)

Cybersecurity awareness training must now include social engineering and must be provided at least annually.

Standard Companies
Class A Companies



Cybersecurity Policies: Areas to Address

Current required areas:

- Information security, data privacy
- Risk assessments
- Data governance and classification, and asset inventory and device management
- Vendor and TPSP management
- Controls: Access and identity management, physical and environmental security
- BCDR and IR
- Systems: operations and availability, network security, monitoring, application development and quality assurance

Additional required areas as of **April 29, 2024**:

- Data retention
- End of life management (phasing out unsupported technical products)
- Remote access controls
- Systems and network monitoring
- Security awareness and training
- Systems and application security
- Incident notification
- Vulnerability management – solar winds



Key Dates

Section 500.5(a)(1), (b), and (c)

- Conduct at least annual penetration testing from inside and outside information systems' boundaries.
- Have a monitoring process in place to promptly inform of new security vulnerabilities. Prioritize and timely remediate vulnerabilities based on risk.

Standard Companies
Class A Companies

Section 500.2(c)

Design and conduct independent audits of cybersecurity program.

Class A Companies

November 1, 2024

Section 500.12(a)

Implement multi-factor authentication (MFA) requirements as outlined in this section of the regulation to the extent they are not already in place.

Small Business Limited-Exempt
Companies



Multi-Factor Authentication (MFA)

Non-exempt CEs will be required to use MFA for any individual accessing any information system of the CE (aligning with FTC's Safeguards Rule).

CEs that qualify for the small business limited-exemption in §500.19(a) will be required to use MFA for:

- remote access to their information systems;
- remote access to third-party applications from which NPI is accessible; and
- all privileged accounts (§500.12)

The only exceptions DFS will permit are those approved by a CISO because other “reasonably equivalent or more secure compensating controls” are in place.



Cybersecurity Resources



Cybersecurity Resource Center (CRC)

DFS's CRC includes several resources on the amended regulation for businesses of all sizes, including:

- Full regulation
- Tailored timelines for the three categories of Covered Entities
- FAQs
- Filing and reporting instructions
- Tools for small businesses
- Training videos (coming soon)



www.dfs.ny.gov/cyber



Subscribe for Cybersecurity Updates

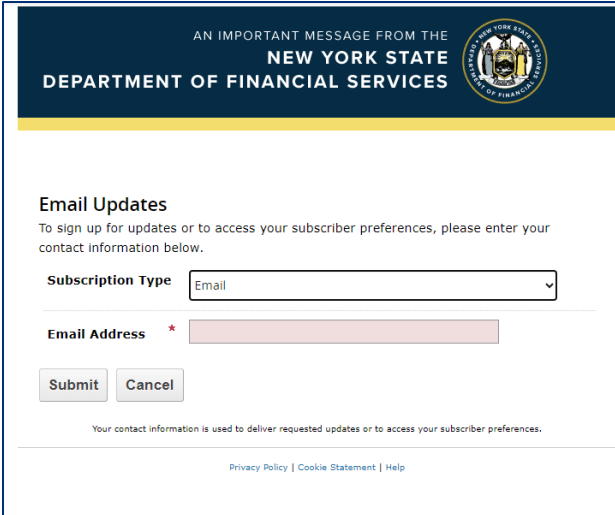
DFS will send out regular email updates ahead of each of the implementation dates.

Join the Cybersecurity Updates subscription list to get email updates:


<https://on.ny.gov/subscribeNYDFS>

Emails will come from nydfs@public.govdelivery.com.

Additional questions? Email cyberregsupport@dfs.ny.gov.



AN IMPORTANT MESSAGE FROM THE
NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES



Email Updates
To sign up for updates or to access your subscriber preferences, please enter your contact information below.

Subscription Type

Email Address *

Your contact information is used to deliver requested updates or to access your subscriber preferences.

[Privacy Policy](#) | [Cookie Statement](#) | [Help](#)





Amended Cybersecurity Regulation

Second Amendment 23
NYCRR Part 500

Effective November 1, 2023