

COMING ATTRACTIONS

Changes to the N.Y. Cybersecurity Regulation

BIG | NEW YORK
EDUCATION

1

NYS Department of Financial Services has proposed multiple changes to the cybersecurity regulation

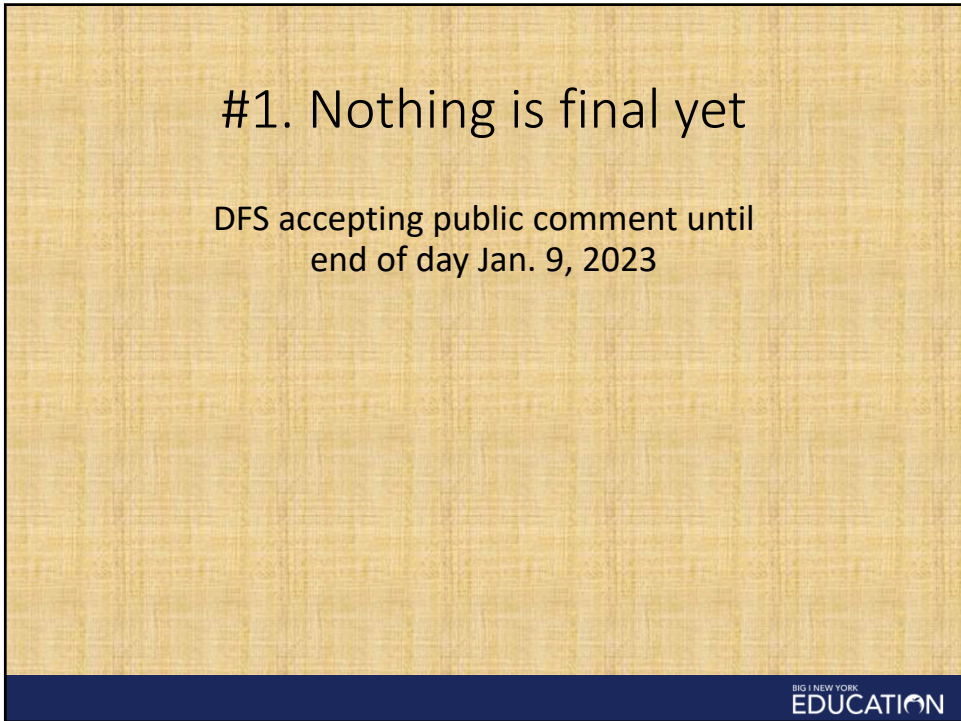
- You can comment to DFS right now
- Send comments to Joanne.Berman@dfs.ny.gov

BIG | NEW YORK
EDUCATION

2



3



4

#2. Compliance Will Be Months in the Future

- Deadline for most changes is 180 days after effective date
- New cyber event reporting requirement deadline = 30 days after
- Compliance with other new requirements = 1 to 2 years after effective date

#3. DFS has proposed some beneficial changes:

More small businesses qualify for limited exemptions

Qualify if any of these are true:

- Less than 20 employees/independent contractors (up from 10)
- Less than \$5 million in NY revenue (unchanged)
- Less than \$15 million in gross assets (up from \$10 million)

7

Inactive individual agents/brokers
will be exempt

8

#4. Some existing requirements
will be clarified

9

The mandatory risk assessments
will be required “annually”
instead of “periodically”

10

Cybersecurity policies & procedures
will have to be approved annually

Approval by entity's board of directors (if it has one)
or by senior officer responsible for cybersecurity

11

#5. There will be
new requirements

12

MFA

All entities of any size will have to implement multi-factor authentication (MFA) within 1 year after effective date

- Deadline is 18 months for implementing MFA for system admins
- MFA: Requires remote user to enter password & 1 other ID factor to login

13

Policies/Procedures

Policies & procedures will have to address

- End of life management of devices
- Remote access (if entity has remote/hybrid employees)
- Password requirements

14

System Administrators

New restrictions on granting system admin privileges

15

Inventory

New requirement to maintain written inventory of entity's technology assets

- Ex: Laptops, phones, tablets
- Deadline for compliance is 2 years after effective date

16

Reporting

New requirement for entities of any size to report:

- Hack of system admin's account
- Ransomware attack
- Making extortion payments
- Deadline for compliance is 30 days from effective date

17

Certification of Compliance

New requirement for annual certification of compliance

- Must report areas where entity is not compliant
- Must report plans for complying

18

New requirements for non-exempt entities

Policies procedures must address

- Systems/security monitoring
- Security awareness/training
- Application security
- Incident notification

New requirements for non-exempt entities

- New governance requirements for Chief Info. Security Officer (CISO) & governing bodies
- New requirements for managing security vulnerabilities
- Annual review of application development procedures

New requirements for non-exempt entities

- Cybersecurity awareness & training
- Encryption meeting industry standards
- Incident response/business continuity management

21

New requirements for large entities

\$20 million in gross annual NY revenue in each of past 2 fiscal years AND either:

- More than 2,000 average employee count in last 2 fiscal years
- More than \$1 billion in gross annual revenue from all operations in each of last 2 fiscal years

22

Violations

- For all entities:
 - Violation = failure to comply with any requirement for any 24-hour period
 - 15 factors DFS will consider when determining penalties

23

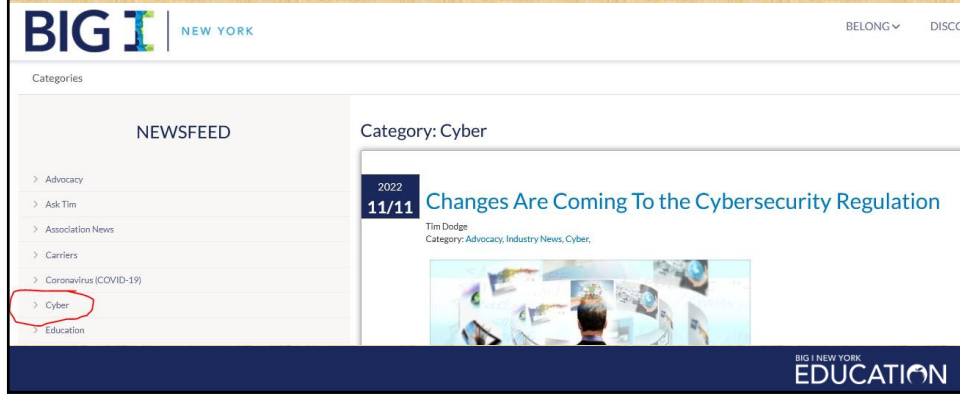
What's Next?

- Big I New York will submit comments to DFS
- We urge you to submit comments on your own
- Send to Joanne.Berman@dfs.ny.gov

24

For more information

Biginy.org/newsfeed – click on “Cyber” in left-hand column



25

For more information

dfs.ny.gov –> Industry Guidance –> Regulatory and Legislative Activities –> Proposed Regulations –> Financial Services



26

Submit Your Comments Before Jan. 9

Joanne.Berman@dfs.ny.gov

27

Tim Dodge, AU, ARM, CPCU

(315) 432-4229

tdodge@biginy.org



28