NEW YORK STATE OF OPPORTUNITY. | Department of Financial Services

23-NYCRR-500

DFS Cybersecurity Regulation

December 6, 2017

NYS Department Of Financial Services (“DFS”)

- Established in 2011 by merging the former Departments of Insurance and Banking and under the new Financial Services Law, the New York Department of Financial Services (DFS) regulates insurance, banking and other financial services institutions with the goal of promoting robust financial services in New York, safeguarding markets from financial crises and protecting both consumers and the industry from fraud

- Under the leadership of the Superintendent, DFS supervises and regulates:

1400 insurance companies with assets of more than $4.3 trillion

- 200 life insurance companies
- 1,100 property/casualty insurance companies
- 100 health insurers and managed care organizations
- 300,000 insurance licensees

1500 banking and other financial institutions with assets totaling more than $2.6 trillion

- 140 state-chartered commercial banks, savings banks and bank holding companies
- 90 branches of foreign banks and agencies
- 20 credit unions
- 380 licensed financial services companies
- 7,600 mortgage loan originators and servicers

Why the Need for 23-NYCRR-500?

- **The goal of the regulation is to prevent cyber-attacks. Two main principles**:
  - Provide minimum standards to prevent cybersecurity threats
  - Strong governance of Covered Entities in the area of cybersecurity as a component of safety and soundness
- **Crucial to protect information** and **financial systems** with consumer information
- Critical area where regulator and regulated institutions must be on the same page to protect markets
- **Cybercriminals exploit** technology **to access** sensitive **data**
- **Examples** of major **breaches**:
  - Anthem: 78.8 million records of PII accessed of data that was unencrypted
  - Bangladesh Bank: $81 million heist through hacking SWIFT
  - Equifax: Access to accounts of 145 million of its customers PII

How 23-NYCRR-500 was Finalized?

2014-15 Regulatory Exploration and Research

- May 2014, initial study on cybersecurity issues in the banking sector
- April 2015, second study on issues related to Third Party Service Providers
- December 2014, DFS expanded IT examinations to focus more on cybersecurity
- February 2015, third study related to cybersecurity in the insurance industry
- DFS surveyed 200 institutions to obtain insight on cybercrime prevention

September 13, 2016 Proposed Cyber Regulation

DFS promulgated proposed regulation: 45 day comment period, received numerous comments from various industry participants and other interested parties

Revised Regulation to Address Comments

Examples of items adjusted in response to comments:

- Risk based nature of the requirements clarified
- Definitions and standards clarified to ensure consistency with other standards
- Implementation time periods developed to address industry comments on effort required

December 28, 2016 Revised Regulation

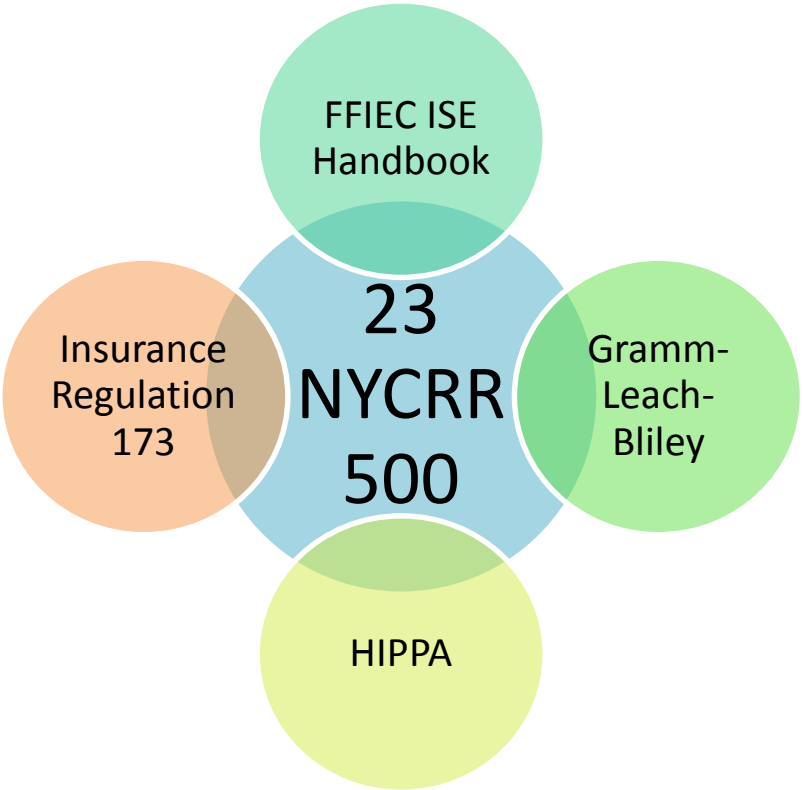
DFS promulgated a revised regulation for a second comment period of 30 days.

March 1, 2017: Final Regulation Adopted

After the Comment Periods:

- DFS incorporated final comments and published final regulation
- FAQs and discussions thereafter to answer questions for Covered Entities as they aim to meet transitional compliance deadlines

500.00 - Introduction



- Establishes a governance framework
- Sets minimum regulatory standards
- Requires a risk based approach to cybersecurity
- Scalable approach to accommodate the breadth of entities regulated by DFS
- Consistent with existing cybersecurity standards including NIST, HIPPA, GLB etc.

500.01- Covered Entity

Entities covered by the DFS regulation are broadly construed. The regulation applies to any entity that is chartered, licensed, or approved to operate in NYS by DFS under the NYS Banking, Insurance or Financial Services Laws, including :

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

Covered institutions range from small brokers to the largest and most complex international banking and insurance entities.

500.01- Nonpublic Information

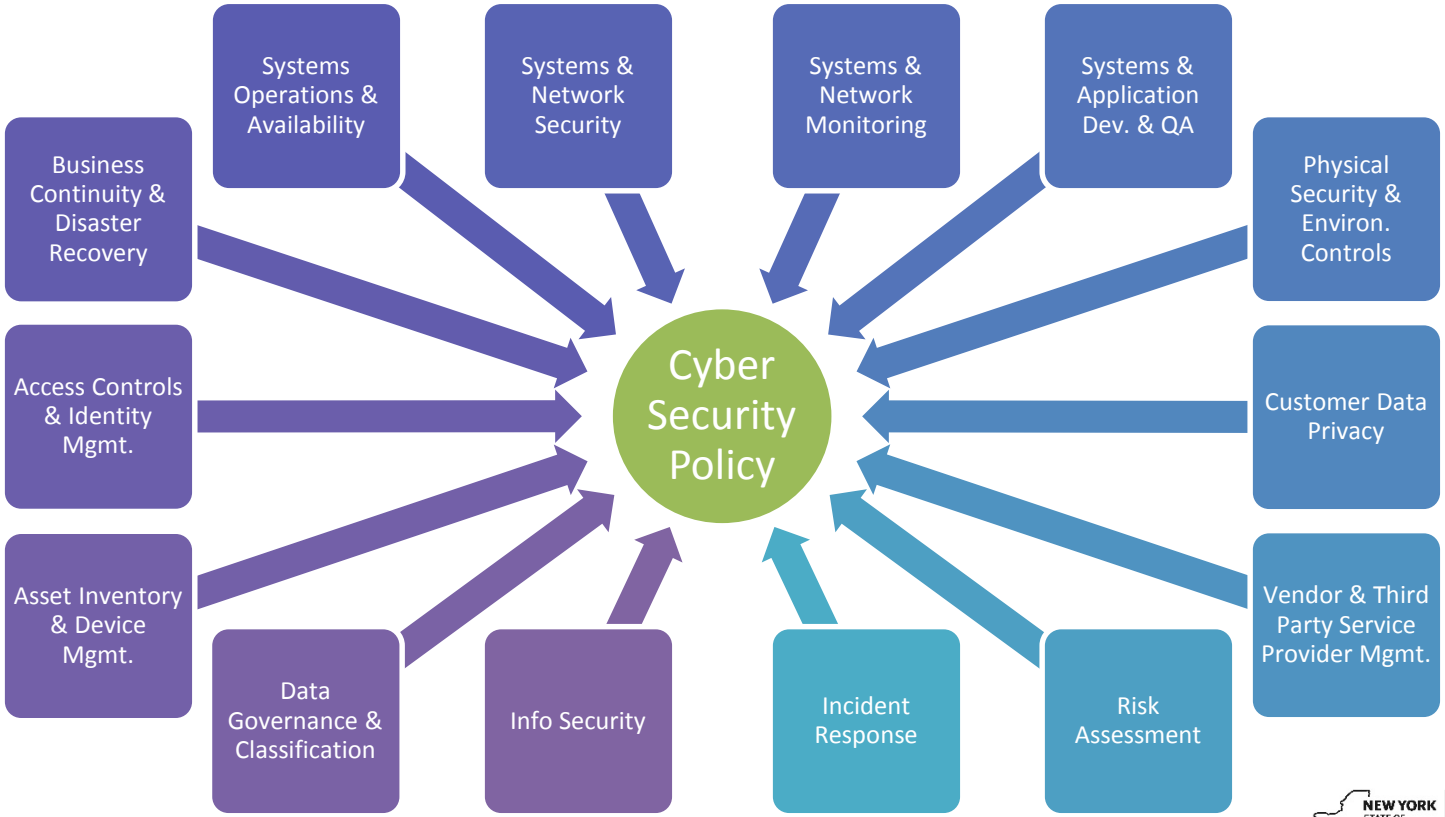
Key to the regulation is its definition of nonpublic information that is consistent with other related laws (i.e. privacy laws, HIPPA) and comprehensive to include all important elements. All electronic information that is not Publicly Available Information and is:

Business Related Information	Tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity
Personal Customer Information	Specifically defined but including: i. social security number ii. drivers' license number iii. account number, credit or debit card number iv. any security code, access code or password that would permit access to an individual's financial account v. biometric records
Healthcare Information	Specifically defined but including information created by or derived from a health care provider that relates to: i. the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family ii. the provision of health care to any individual, or iii. payment for the provision of health care to any individual.

500.02- Cybersecurity Program

- Based on the specific risks of an entity as identified through the Risk Assessment conducted by the Covered Entity
- Each entity must be able to perform the same core functionality:
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
  - Report

500.03- Cybersecurity Policy



500.04- Chief Information Security Officer

- Personnel Element
  - CISO must be appropriately qualified
  - Oversees the cybersecurity program
  - May be outsourced to a third party or an affiliate*
  - Position, not a title
- Reporting Element
  - CISO reports to entity's governing body on cybersecurity program and risks
  - At least annually

* Provided the Covered Entity and a senior manager of the Covered Entity retain responsibilities for oversight and direction

500.05- Penetration Testing & Vulnerability Assessments

DFS Regulation requires entities to:

- Implement monitoring and testing as part of their cybersecurity program. As part of this monitoring and testing, the program must include:
  - continuous monitoring ***or***
  - penetration testing ***and*** vulnerability assessment.
- If a Covered Entity determines continuous monitoring to be infeasible, it must conduct penetration testing and vulnerability assessments as an alternative.

500.05- Penetration Testing & Vulnerability Assessments

Penetration Testing

- At least annually
- Tester poses as an attacker
- Tester attempts to gain unauthorized access to a system

Vulnerability Assessment

- At least bi-annually
- Automated scan of systems
- Identifies known vulnerabilities of systems and devices
- Identifies needed, available patches
- Many significant cyber attacks would have been prevented if the entity had updated its systems with patches that addressed known vulnerabilities

500.06- Audit Trail

Logs must be able to:

- Reconstruct financial transactions
- Detect and respond to Cybersecurity Events
  - What happened?
  - How did it happen?
- Records must be kept for at least 5 years

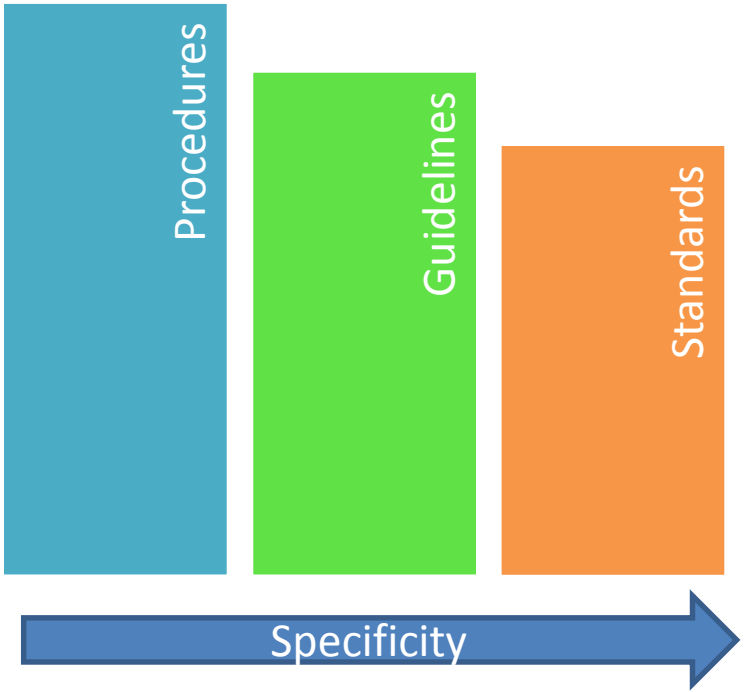
500.12- Access Controls

- Companies are required to adopt effective access controls to protect against unauthorized access to Nonpublic Information or Information Systems.
- Access controls can include:
  - Multi-Factor Authentication
  - Risk-Based Authentication

500.12- Multi-Factor Authentication

- User must authenticate at least **two** of the following:
  - A knowledge factor - something the user knows
  - A possession factor - something the user has
  - An inherence factor - something the user is
- Covered Entities must implement Multi-Factor Authentication when accessing an internal network from an external network
- Risk Based Authentication:
  - Assess access patterns
  - User may be asked to authenticate further based on detected variations in patterns

500.08- Application Security



- Written documentation for secure in-house development practices
  - In order of specificity
    - Procedures
    - Guidelines
    - Standards
- Develop procedures to assess whether or not third party applications are secure

500.09- Risk Assessment

- Is the heart of a cybersecurity program
  - Drives an entity's cybersecurity program
- Identifies the specific, inherent risks of an entity
- Conducted according to written policies and procedures
- *The Risk Assessment process is a valuable process to direct the organization's technology and to ensure appropriate governance as it requires the entire program and risks to be reviewed, assessed and addressed.*

500.09- Risk Assessment

- **Requires:**
  - Periodic updates
    - Ideally, a risk assessment should be in a constant state of update
  - Written procedures documenting:
    - How it is done
    - Definitions used
  - Comprehensive review of Nonpublic Information and controls to protect such information

- **Not Required:**
  - Standard format and content
    - Each will be individual to the entity that created it
  - Stand alone document
    - It may be included in an IT Risk Assessment or an entity's overall Risk Assessment

500.11- Third Party Service Provider Security Policy

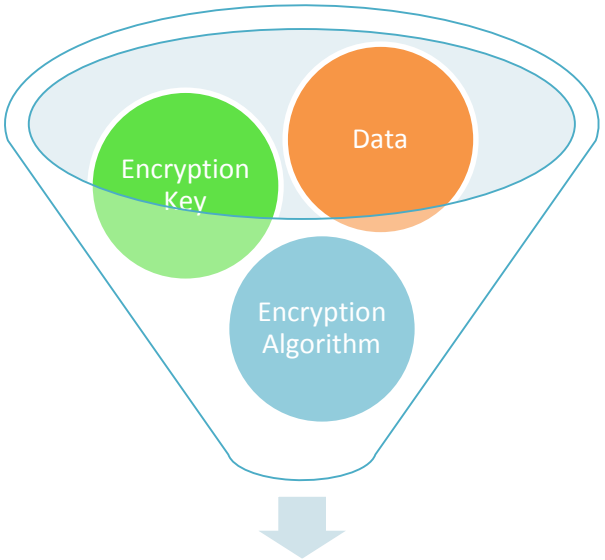
- Entities need to understand and address risks associated with Third Party Service Providers based on Risk Assessment
  - Develop policies and procedures for dealing with third parties with access to data and systems
  - Establish guidelines around third party access to the entity's Information Systems, data, and Nonpublic Information
    - E.g. Multiple health insurers used the same Third Party Medical Identification Card vendor. The vendor's security was compromised making names, addresses and ID numbers of customers public.

Training and Cybersecurity Personnel

- Entities must implement policies to train and monitor their Authorized Users
  - Must be designed to detect inappropriate use
- Regular cybersecurity awareness training for all personnel
- Entities must hire qualified cybersecurity personnel who should be provided training and updates regarding technological developments

500.15- Encryption of Nonpublic Information

- Entities must implement encryption to protect data both:
  - In transit
  - At rest
- If the entity deems this infeasible, the CISO must approve effective alternative compensating controls
- Compensating controls must be reviewed annually by CISO



500.16- Incident Response Plan

- Cybersecurity Events will happen
- Entities must develop a written plan to respond and recover
- Need to clearly define roles and responsibilities to respond quickly

500.19- Exemptions

- Exemptions are generally limited, requiring entities to comply with some but not all the provisions of the regulation
- Designed to address the risks and circumstances of particular institutions including:
  - Smaller entities, including many insurance producers
  - Entities without information systems or data, or who have a limited amount of data

500.17- Notices to Superintendent

All notices filed through DFS secure cyber portal:

1. Annual Compliance Certification
   - ✓ Attests to compliance for the prior calendar year
   - ✓ Submitted annually by Feb 15, beginning 2018
   - ✓ Signed by the Chairman of the Board of Directors or a Senior Officer
   - ✓ All records supporting a certificate of compliance must be maintained for a *minimum* of 5 years
   - ✓ See Appendix A for Form Certification
2. Notice of Cybersecurity Events
   - ✓ Must be reported within 72 hours of determining an event is reportable:
     - ❑ Required to be reported to other agencies, including notices of data breaches that harm consumers
     - ❑ Has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity
   - ✓ Context and the approach of the attacker matter
   - ✓ Provide basic identifying and contact information and a description of the event; provides bases for lessons learned
3. Notice of Exemption
   - ✓ See Appendix A for Form Certification

500.22 Transitional Periods

End of Transitional Period	Sections
August 28, 2017	500.02- Cybersecurity Program 500.03- Cybersecurity Policy 500.04(a)- Chief Information Security Officer (Position) 500.07- Access Privileges 500.10- Cybersecurity Personnel and Intelligence 500.16- Incident Response Plan 500.17- Notices to Superintendent 500.18- Confidentiality 500.19- Exemptions 500.20- Enforcement 500.21- Effective Date 500.22- Transitional Periods 500.23- Severability

500.22 Transitional Periods

End of Transitional Period	Sections
March 1, 2018	500.04(b)- Chief Information Security Officer (CISO Report) 500.05- Penetration Testing and Vulnerability Assessments 500.09- Risk Assessment 500.12- Multi-Factor Authentication 500.14(b)- Training and Monitoring
September 3, 2018	500.06- Audit Trail 500.08- Application Security 500.13- Limitations on Data Retention 500.14(a)- Training and Monitoring 500.15- Encryption of Nonpublic Information
March 1, 2019	500.11- Third Party Service Provider Security Policy

NAIC Insurance Data Security Model Law

- DFS worked closely with NAIC to create a nationally consistent model law because it is critical to establish regulatory consistent standards in this complex arena
- The NAIC Data Security Model Law followed the DFS cybersecurity regulation and has no material differences
- Specific footnote states that regulated entities that already comply with 23 NYCRR 500 are complying with NAIC Insurance Data Security Model Law

DFS Examination Plans

Capacity

- Training current examination staff on 23-NYCRR-500 requirements, and additional higher level training for some examiners
- Developing specific exam protocols
- Hiring additional specialized Cybersecurity Examiners

Partner

- Working with other regulators including on joint examinations
- Ensure consistent regulatory standards
- Working with law enforcement agencies on cybersecurity practices, training and events

Focus

- Safety and soundness exams will review cybersecurity governance to assess strength of cyber framework
- IT/cyber specialist examinations will examine minimum technological standards and conduct target examinations as necessary
- Goal is to strengthen all institutions' cybersecurity protections

Wrap Up

- Questions
- Frequently Asked Questions Regarding 23 NYCRR Part 500
  - http://www.dfs.ny.gov/about/cybersecurity_faqs.htm