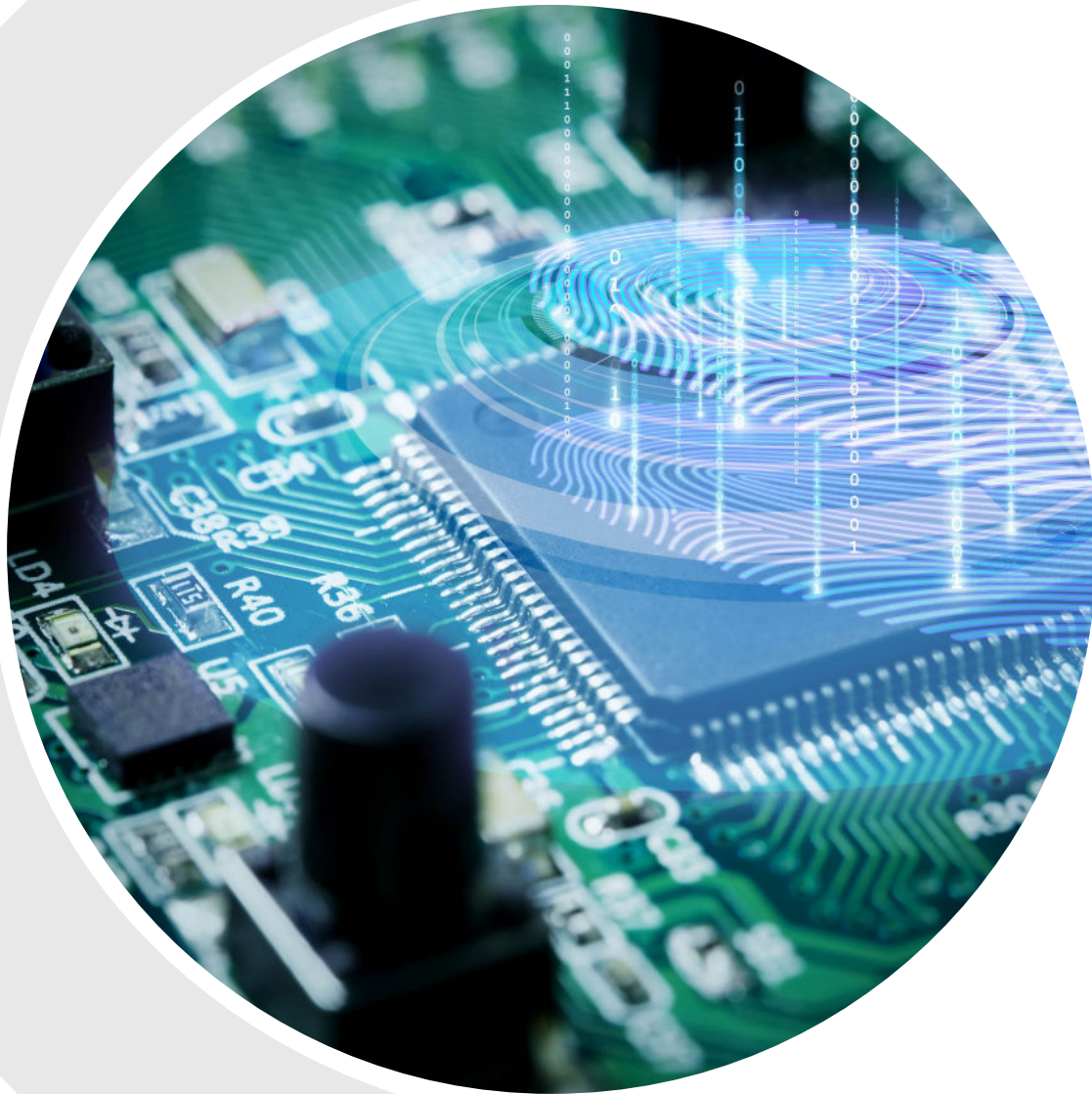




SBC MONTHLY CYBER FORUM:

**YOUR NEW OBLIGATIONS
UNDER THE NYDFS
AMENDED CYBERSECURITY
REGULATIONS**



MONTHLY SBC CYBER FORUM

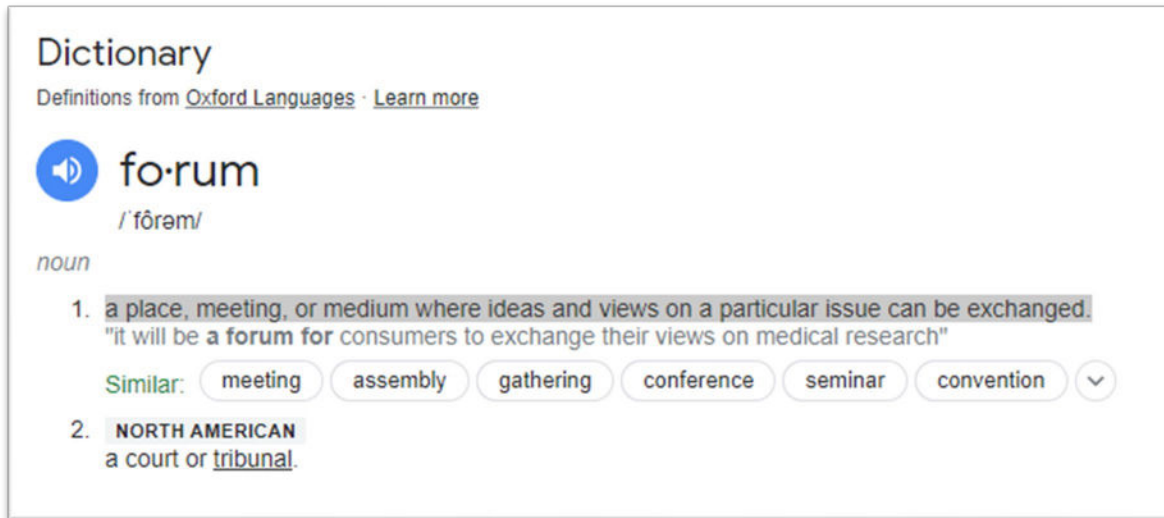
A Forum for Understanding How to:

- 1. Be Compliant with SEC, FINRA, and State Cybersecurity Regulations and Guidance**
- 2. Prevent the Theft of Information**
- 3. Prevent Fraud (i.e., the Theft of Money)**

Be Compliant. Be Secure.



MONTHLY SBC CYBER FORUM: VISION / GUIDING PRINCIPLES



SBC Monthly Cyber Forum

Be Compliant. Be Secure.

1. **SOLUTION ORIENTED:** Define Problems Common to the Audience & Focus on Solutions to Problems.
2. **PEER TO PEER IDEA EXCHANGE:** Share Best Practices with One Another.
3. **OPEN, INDEPENDENT:** Eliminate Bias.
4. **INTELLIGENCE SHARING OPPORTUNITIES:** Participants are Encouraged to Participate in an Information Sharing.

TODAY'S SPEAKERS



Guest Expert: John Cooney

John Cooney is a United States Marine Corps combat veteran and has a combined 29 years of business, legal, and technical experience, with a focus on federal/state investigations and the Cybersecurity arena.

[View John's Bio Here](#)



SBC Forum Host: Paul Osterberg

Paul Osterberg is Managing Director of Security Basecamp, a cybersecurity services firm. Over the past nine years, he has spent more than 17,500 hours assisting clients manage information security program and his firm has completed over 350 Cybersecurity Risk Assessments.

[View Paul's Bio Here](#)

TODAY'S TOPICS:

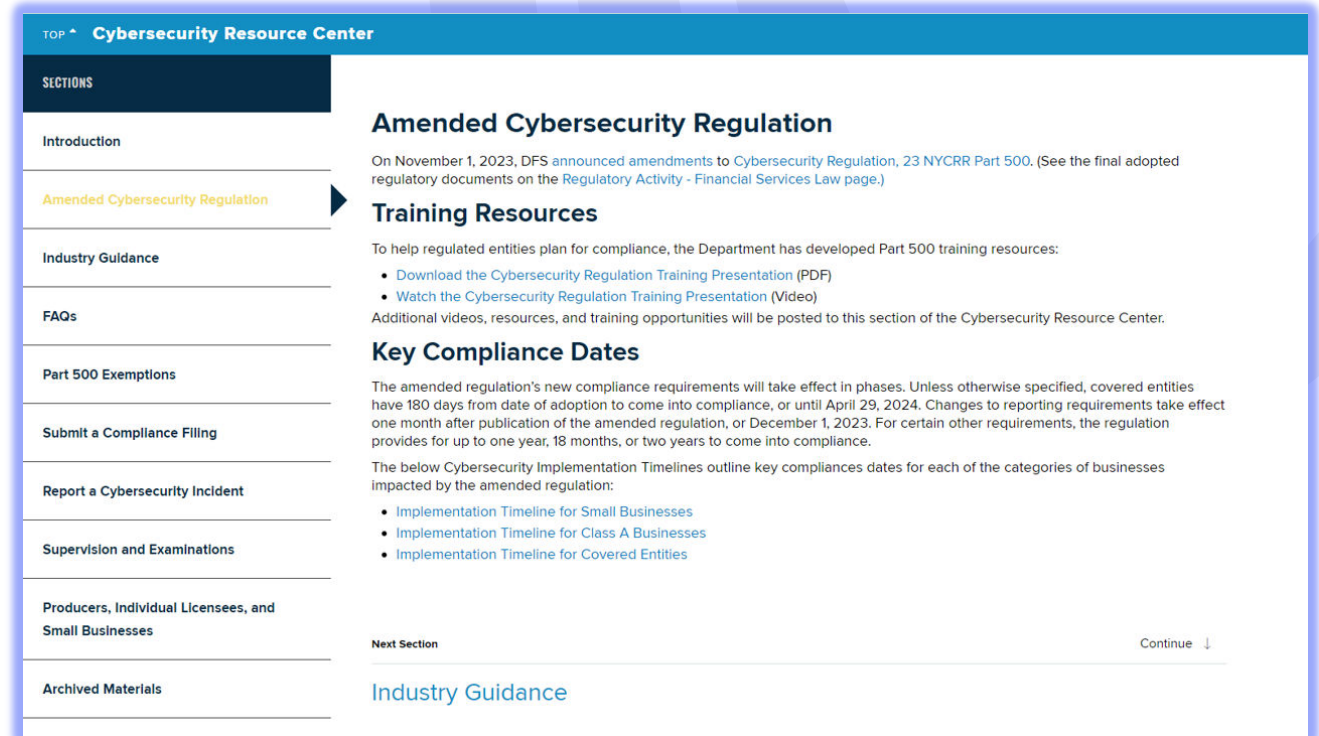
1. **UNDERSTAND COMPLIANCE WITH THE NYDFS CYBERSECURITY REGULATION**
2. **WHAT ARE THE AMENDMENTS TO THE NYDFS CYBERSECURITY LAW**
 1. **WHO IS REGULATED?**
 2. **WHAT ACTIONS ARE NEEDED?**
3. **CYBERSECURITY BEST PRACTICES**



NYDFS CYBERSECURITY REGULATION

In November 2023, the NYDFS:

- [Announced Amendment to Cybersecurity Regulation, 23 NYCRR Part 500.](#) (See the final adopted regulatory documents on the [Regulatory Activity - Financial Services Law page.](#))
- Provided Training Resources to help regulated entities be compliant with the law.
- Read the FAQs.



The screenshot shows the 'Cybersecurity Resource Center' website. The left sidebar lists sections: Introduction, Amended Cybersecurity Regulation (highlighted), Industry Guidance, FAQs, Part 500 Exemptions, Submit a Compliance Filing, Report a Cybersecurity Incident, Supervision and Examinations, Producers, Individual Licensees, and Small Businesses, and Archived Materials. The main content area is titled 'Amended Cybersecurity Regulation' and includes a paragraph about the November 1, 2023 announcement, a 'Training Resources' section with links to a PDF and a video, and a 'Key Compliance Dates' section with implementation timelines for Small Businesses, Class A Businesses, and Covered Entities. A 'Next Section' link for 'Industry Guidance' is at the bottom.

Source: https://www.dfs.ny.gov/industry_guidance/cybersecurity (Web, February 2024)

The Purpose of Today: Help You Understand the Law, its Amendments, and How to Be Compliant and Secure.



NYDFS CYBERSECURITY LAW: AN OVERVIEW



Amended Cybersecurity Regulation

Second Amendment 23
NYCRR Part 500

Effective November 1, 2023

LEVERAGE GREAT RESOURCES!

MITRE ATT&CK® AND DEFEND® FRAMEWORKS: EFFECTIVELY USING CYBERSECURITY RESOURCES

- [MITRE ATT&CK® Framework](#)
- Globally-Accessible Knowledge Base of Adversary Tactics and Techniques
- Understand Mitigations that Can Be Employed to Prevent Attacks.
- [MITRE DEFEND® Framework](#)



CISA: EFFECTIVELY USING CYBERSECURITY RESOURCES

- Access Insights Into Threat Intelligence & See the Future of Cybersecurity Tech in Action.
- Subscribe to Alerts and Guidance
- [Cybersecurity & Infrastructure Security Agency \(CISA\)](#)
- [Resources & Tools | CISA](#)
- [CISA Tabletop Exercise Packages | CISA](#)
- [Zero Trust Maturity Model Version 2.0 \(cisa.gov\)](#)



NYDFS CYBERSECURITY RESOURCE CENTER

Today we will extensively utilize the resources the NYDFS makes available:

- NYDFS Training Resources:
 - [NYSDFS: Cybersecurity Training Deck presentation - November 8, 2023](#)
 - [General Overview: Amended Cybersecurity Regulation \(youtube.com\)](#)
- Key Compliance Dates:
 - [Implementation Timeline for Small Businesses](#)
 - [Implementation Timeline for Class A Businesses](#)
 - [Implementation Timeline for Covered Entities](#)

Make Sure to Know and Use the Resources the NYDFS is Making Available.



Amended Cybersecurity Regulation

Second Amendment 23
NYCRR Part 500

Effective November 1, 2023

Source: [NYDFS Cybersecurity Regulation Public Training Deck 11.8.23](#) (Web, February 2024)

[Cybersecurity Regulation with New Amendments Annotated](#) (Web, February 2024)



A CLEAR SIGNAL TO "GET INTO ACTION"

Governor Hochul Announces Updates To New York's Nation-Leading Cybersecurity Regulations



**Be Ready! Leverage What the NYDFS Makes Available.
There is Major Emphasis for a Reason.**

PROPERLY MANAGING INCIDENTS: ESSENTIAL

Among other things, SolarWinds' remote access setup was found to be "not very secure"

CISO had internally notified company executives that "current state of security leaves us in a very vulnerable state for our critical assets"

A pivotal point for the role of a CISO, transforming it into one that requires a lot more professional scrutiny and personal responsibility



by Shweta Sharma
Senior Writer

SEC sues SolarWinds and its CISO for fraudulent cybersecurity disclosures

News
Oct 31, 2023 · 4 mins

CSO and CISO Cyberattacks

SEC has accused SolarWinds and its CISO of understating cybersecurity risks to stakeholders and said the company missed numerous red flags.

Source: <https://www.csoonline.com/article/657599/sec-sues-solarwinds-and-its-ciso-for-fraudulent-cybersecurity-disclosures.html> (Web, CSO, November 2023)

The Security and Exchange Commission (SEC) has filed charges against SolarWinds and its chief information security officer, Timothy G. Brown for misleading investors by not disclosing "known risks" and not accurately representing the company's cybersecurity measures.

ESSENTIAL ELEMENTS OF ALL CYBER PROGRAMS

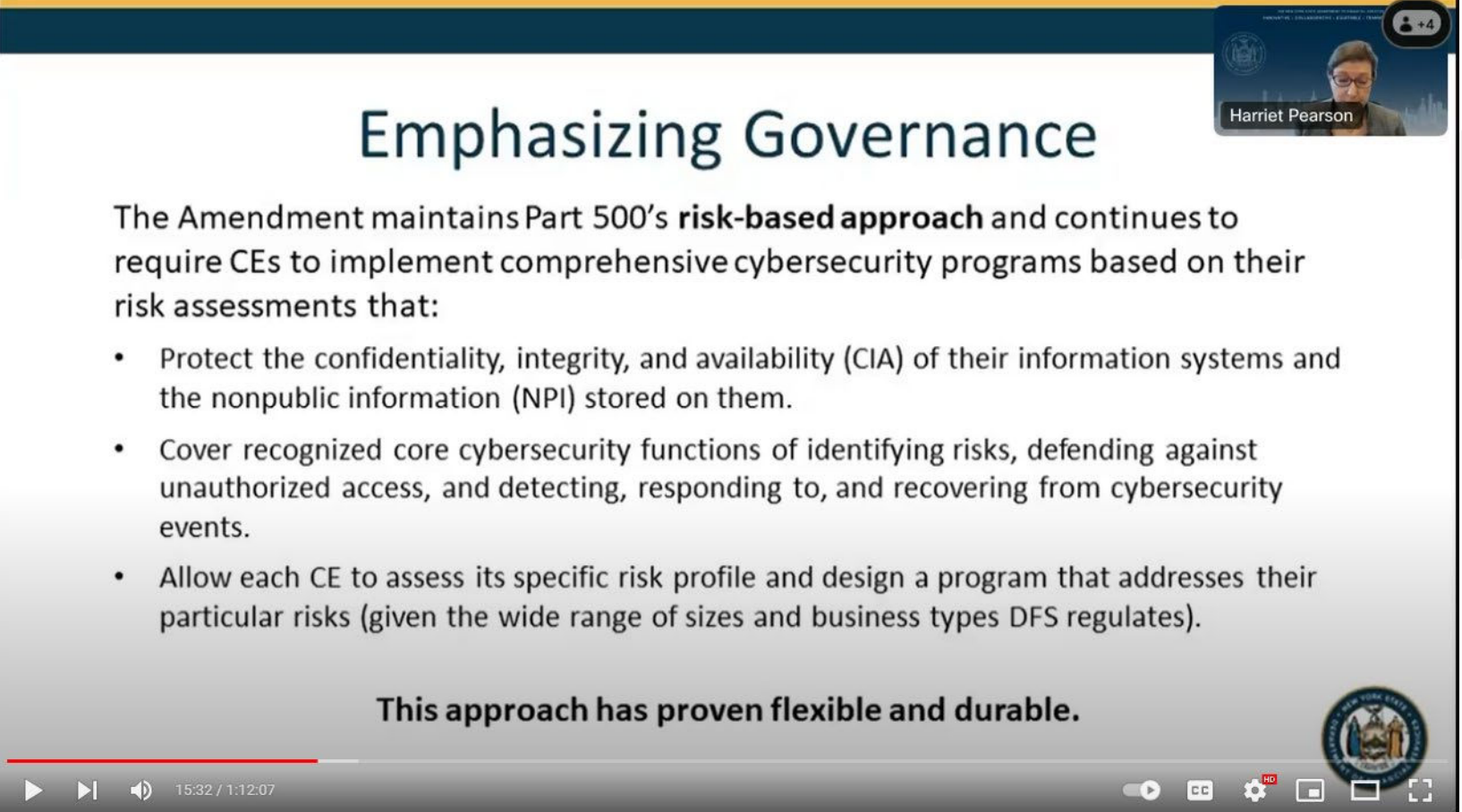
- Guidance and Requirements of Applicable Cybersecurity Regulation (e.g., FINRA, SEC, NFA, NY-DFS, etc.) and Frameworks (e.g., NIST, ISO 27001) are Substantially Similar
- See the SBC Website for Insights:
 - [SBC-Alert-NYDFS-Cybersecurity-Rule-Updates-01.15.24-2.pdf \(securitybasecamp.com\)](#)
 - [SBC Alert -Summary of Cybersecurity Guidance from Financial Services Regulators 01.01.21](#)
 - [SBC Regulatory Alert - Proposed Rules 206\(4\)-9 and 38a-2 -02.09.22](#)
 - [SBC Regulatory Alert - Proposed Rule 10 - 02.15.23](#)
 - [Create Alert for Proposed Reg S-P Changes](#)
 - [Create Alert for Proposed Reg SCIR Changes](#)



“THE MOST IMPORTANT PART OF THE REGULATION IS THAT IT IS RISK-BASED”, HARRIET PEARSON

“You exercise judgement based upon a risk assessment”

No specific technology solutions; that said, important essential controls are mandated



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.

Harriet Pearson

15:32 / 1:12:07

Source: [General Overview: Amended Cybersecurity Regulation - YouTube](#) (Web, February 2024)

NYDFS: THREE SIZES OF COMPANIES REGULATED

Large ("Class A") Companies

Must comply with all requirements.

- \$20 Million / year in NY; \$1 Billion overall no matter the location.
- > 2,000 employees

Small ("Exempt") Companies

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

- < \$7.5 Million / year in NY, or
- < \$15 Million in EOY Assets, or
- < 20 Employees

Non-Class A, Non-Exempt ("Standard") Companies

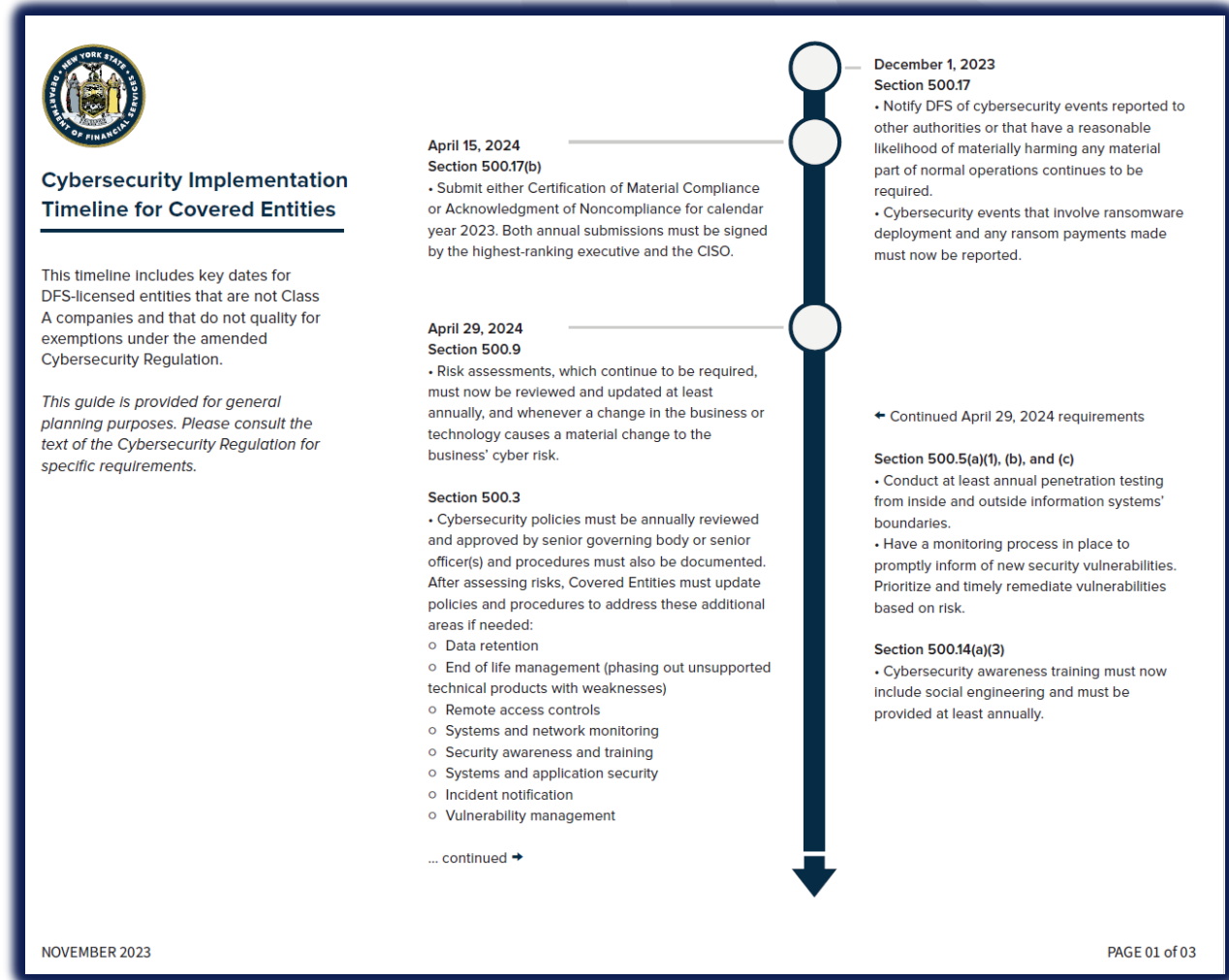
Must comply with most requirements. A majority of Covered Entities are in this category.

- Covered Entities that do not qualify for full or limited exemption or as Class A Companies

Most Firms are "Standard"; Pay Attention to Nuance. Visit the NYDFS Site to Understand Your Particular Requirements.

“STANDARD” COMPANIES: CYBERSECURITY IMPLEMENTATION TIMELINE

- A Majority of Covered Entities
- Must Comply with Most Requirements
- Let’s Walk Through the Timeline



The image shows a document page titled "Cybersecurity Implementation Timeline for Covered Entities" from the New York State Department of Financial Services. The page features a vertical timeline with three main milestones: April 15, 2024 (Section 500.17(b)), April 29, 2024 (Section 500.9), and December 1, 2023 (Section 500.17). The timeline is represented by a vertical line with circles at the top and bottom, and a downward-pointing arrow at the very bottom. The document includes detailed requirements for each date, such as submitting certifications, conducting risk assessments, reviewing policies, and performing penetration testing. A note indicates that the timeline applies to Class A companies and that specific requirements should be consulted in the regulation text. The page is dated November 2023 and is page 01 of 03.

Cybersecurity Implementation Timeline for Covered Entities

This timeline includes key dates for DFS-licensed entities that are not Class A companies and that do not qualify for exemptions under the amended Cybersecurity Regulation.

This guide is provided for general planning purposes. Please consult the text of the Cybersecurity Regulation for specific requirements.

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.

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.

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 these additional areas if needed:
 - Data retention
 - End of life management (phasing out unsupported technical products with weaknesses)
 - Remote access controls
 - Systems and network monitoring
 - Security awareness and training
 - Systems and application security
 - Incident notification
 - Vulnerability management

... continued →

December 1, 2023
Section 500.17

- Notify DFS of cybersecurity events reported to other authorities or that have a reasonable likelihood of materially harming any material part of normal operations continues to be required.
- Cybersecurity events that involve ransomware deployment and any ransom payments made must now be reported.

← Continued April 29, 2024 requirements

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.

Section 500.14(a)(3)

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

NOVEMBER 2023

PAGE 01 of 03

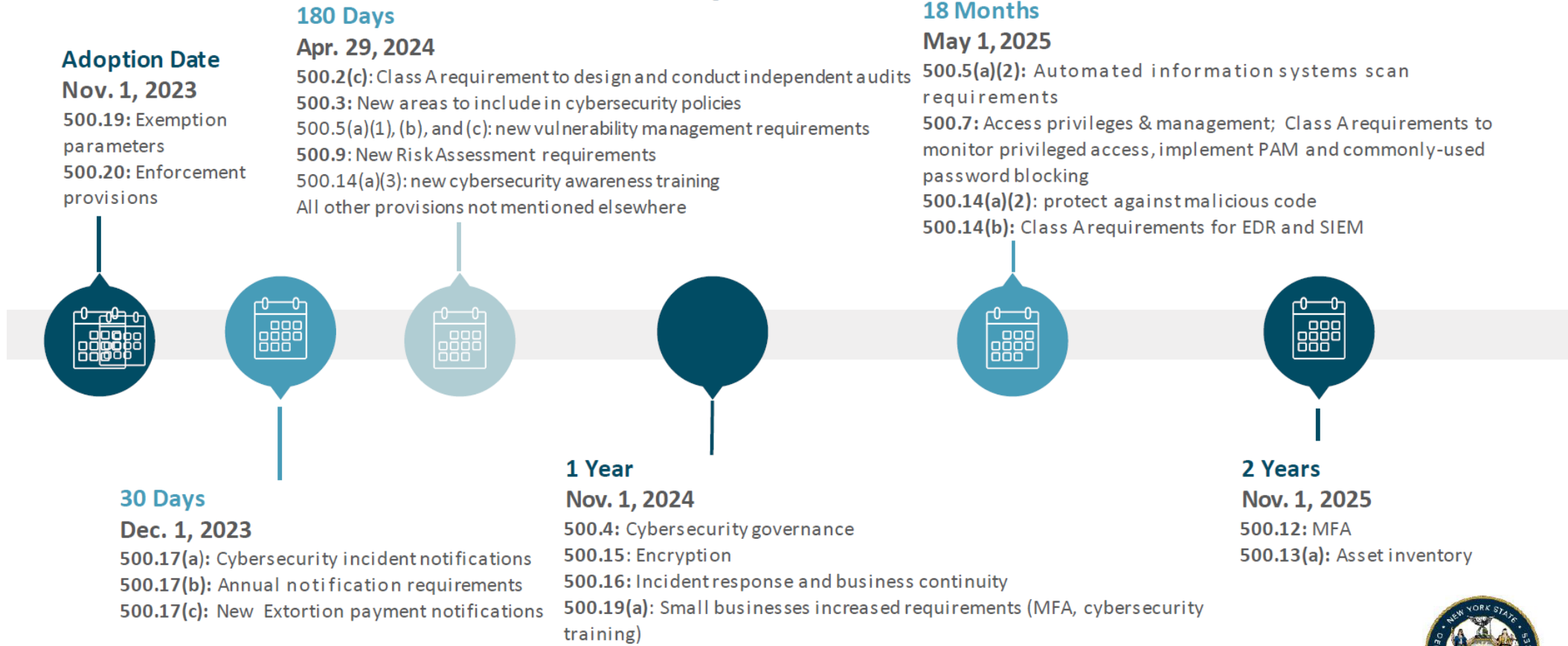
GRC SOLUTIONS (E.G., BUCKLER): HOW WE KEEP UP WITH WHAT TO DO AND ASSESS RISKS?

- Maps Policies, Processes, and Controls to the Applicable Regulation
- Guides Your Cyber Program and Guides Your Risk Assessments

The screenshot displays the Security Basecamp GRC solution interface. On the left, a navigation sidebar lists various categories: Policies, Evidence, Open VRM, Contacts, Locations, and Settings. The main content area is titled 'Policies' and shows a list of 'All Policies' (240 total). A modal window is open, displaying 'Policy Details' for 'CYBERSECURITY PROGRAM MANAGEMENT'. This modal includes an 'Insights' section with a lightbulb icon and text: 'This is exactly why you use Buckler! -- See "Nonpublic Information (NPI) Definition" for details on NPI.' The main content area also features a 'Regulation Policy Match' section listing various regulatory references such as FINRA - Cybersecurity Report 2018, HIPAA, and NYDFS - 3/1/2017 23 NYCRR 500. A table on the right side of the interface shows columns for 'DATES', 'OWNER', and 'DELEGATED TO', with entries for 'CISO (Chief Information Security Officer)'. The top right corner of the interface shows 'Security Basecamp LLC' and buttons for 'Download' and 'Add Policy'.

NYDFS CYBERSECURITY: PHASED COMPLIANCE DATES

Phased Compliance Deadlines



DEEP DIVE ON KEY DATE FOR '23 – '24

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



NOTABLE ITEMS FOR ALL COMPANIES

- All Required to do Annual (previously Periodic) Risk Assessments
- Policies must be reviewed annually, and most companies must address all elements of the law
- Training MUST address Social Engineering


General Overview: Amended Cybersecurity Regulation

Key Dates

Joanne Berman

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.	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.	Section 500.14(a)(3) Cybersecurity awareness training for all personnel must now include social engineering and must be provided at least annually.
Limited-Exempt Companies Standard Companies Class A Companies	Small Business Limited-Exempt Companies Standard Companies Class A Companies	Standard Companies Class A Companies



“As report by the DHS, FBI, and the NSA, more than 90% of all cyber attacks begin with phishing.” Joanne Berman, NYDFS

DEEP DIVE ON KEY DATE FOR '23 – '24

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



DEEP DIVE ON KEY DATE FOR '23 – '24

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



VULNERABILITY MANAGEMENT (500.5)

A vulnerability is a weakness in an information system or other valuable asset that can be exploited by a bad actor. Remediate. Patch. Address

- Your Annual Risk Assessment should “incorporate threat and vulnerability analyses”. (500.9)
- Policies for companies of all sizes should address vulnerability management (500.3)
- Vulnerabilities are usually published (i.e., known to both good and bad actors). Have a monitoring process in place. Prioritize and remediate vulnerabilities.
- **Remediate and PATCH!!**

DEEP DIVE ON KEY DATE FOR '23 – '24

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



DEEP DIVE ON KEY DATE FOR '23 – '24

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



NEW RISK ASSESSMENT REQUIREMENTS

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))



CYBERSECURITY POLICIES: AREAS TO ADDRESS

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



MULTI-FACTOR AUTHENTICATION

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.



VULNERABILITY MANAGEMENT & PENETRATION TESTING

An Area of
Potential
Confusion

Use
Professionals

Electronic
Truth

Timely
Remediation

500.5 Vulnerability management.

Each covered entity shall, in accordance with its risk assessment, develop and implement written policies and procedures for vulnerability management that are designed to assess and maintain the effectiveness of its cybersecurity program. These policies and procedures shall be designed to ensure that covered entities:

(a) conduct, at a minimum:

(1) penetration testing of their information systems from both inside and outside the information systems' boundaries by a qualified internal or external party at least annually; and

(2) automated scans of information systems, and a manual review of systems not covered by such scans, for the purpose of discovering, analyzing and reporting vulnerabilities at a frequency determined by the risk assessment, and promptly after any material system changes;

(b) are promptly informed of new security vulnerabilities by having a monitoring process in place; and

(c) timely remediate vulnerabilities, giving priority to vulnerabilities based on the risk they pose to the covered entity.

VULNERABILITY MANAGEMENT & PENETRATION TESTING

- Understand the test types that exists.
- Remember both compliance and security.
- “Vulnerability Management is Your Friend”
- “Automated scans for information systems, and a manual review of systems not covered by such scans”
- Your risk assessment sets the frequency.

Type	Description	Scope	Key Traits	Common Tools
Network Penetration Test	Manual tests that <u>attempts</u> to exploit network vulnerabilities identified.	Same as Network Vulnerability Scan	<p>Key aspect to any penetration test is the manual component. <u>Pentests</u> often incorporate automated vulnerability scans initially to identify vulnerabilities on in-scope systems, but the tester will manually attempt to exploit those vulnerabilities to compromise the systems. The objective of any penetration test is to prove that the vulnerabilities are real and exploitable – it is often difficult and rare for a <u>pentester</u> to exploit every vulnerability identified.</p> <p>In a <u>pentest</u> report, you'll often see screenshots of the <u>pentester</u> and their successful exploit attempts of different vulnerabilities. It is also common for <u>pentest</u> reports to include other vulnerabilities identified that have not been exploited, thereby making the results very similar to typical vulnerability scan reports.</p> <p>Since a <u>pentest</u> requires specialized skills to manually exploit vulnerabilities, most companies will hire an external security firm, such as Protiviti, to conduct these tests.</p>	Qualys Nessus Nexpose Kali Nmap <u>Nikto</u> <u>DirBuster</u> Metasploit
Dynamic Application Security Test	Automated scans that identify application-level vulnerabilities while the application is in its compiled and operating mode.	Web Applications (Internal and External) often indicated as URLs instead of IP addresses.	<p>A dynamic application security test is <u>most commonly referred</u> to as application vulnerability scans. It relies on automated scans that are scheduled, and identifies known vulnerabilities based on the application in its operating mode.</p> <p>It is important to run these scans on every page of the web application instead of just the home page that many companies will focus on. To do so, authentication may be required based on the function of the web application.</p> <p>Vulnerabilities identified will focus on application-layer vulnerabilities such as ones published by OWASP.</p>	Veracode <u>WhiteHat</u> <u>BurpSuite</u> <u>AppSpider</u> <u>WebInspect</u> <u>AppScan</u>

THE NEXT TWO CALLS

- Tuesday, March 12 at 1pm PST / 4pm EST:
 - **Effective Incident Response: Identifying, Mitigating, Managing, and Reporting Cybersecurity Incidents**
- Tuesday, April 9th at 1pm PST / 4 pm EST:
 - **Third Party Risk Management / Vendor Risk Assessments**

GETTING INTO ACTION: RECOMMENDED NEXT STEPS

1. Determine the Size of Your Company.
2. Review the NYDFS Cybersecurity Implementation Timeline for Your Company.
3. Use the NYDFS Resource Center. Listen to the NYDFS Video. Sign up for Alerts.
4. Develop a Plan of Actions and Milestones (POA&M).
5. Conduct a Risk Assessment. All, but Fully Exempt, must complete them annually (vs. the previous requirement of “periodically”).
6. Update Your Policies and Procedures based Upon the Risk Assessment.
 1. Ensure Your Policies Address Each of the Required Areas.
 2. Keep in mind, even for small companies (i.e., Exempt), that includes most every area of the law including vulnerability management.
7. Submit either a Certification of Material Compliance or Acknowledgement of Non-Compliance for Calendar Year 2023 (by April 15th, 2024).
8. Focus first on Being Secure, and then use the tools and resources of the NYDFS / Regulators to Ensure You are Being Compliant.

QUESTIONS & ANSWERS

John Cooney

The Law Office of John J. Cooney
(631) 949-2626
jcooney@jcooneylaw.com

Paul Osterberg

Security Basecamp
(949) 330-0899
paul@securitybasecamp.com

Vincent Guyaux

Buckler
(646) 315-4161
vincent@buckler.app

Scott Smith

Buckler / Security Basecamp
(612) 805-8400
scott@buckler.app
ssmith@securitybasecamp.com



This Photo by Unknown Author is licensed under [CC BY-ND](https://creativecommons.org/licenses/by-nd/4.0/)



NYDFS CYBERSECURITY: SUMMARY OF KEY CHANGES IN THE AMENDED LAW FOR THIS YEAR (NOV 23 – NOV 24)

- Tailored Requirements to Better Fit Different Sizes and Type of Entities – More Businesses Now Qualify for Full and Limited Exemptions
- Phased Compliance Deadlines – Notable Items:
 - December 1, 2023: Updates to Notification Requirements
 - April 29, 2024:
 - Class A Requirements to **Design / Conduct Independent Audits**
 - **New Areas** to Include in Cybersecurity Policies
 - **New Vulnerability Management Requirements** (i.e., Conduct At Least Annual Penetration Testing from Inside and Outside the Systems' Boundaries; Detect and Remediate Vulnerabilities)
 - November 1, 2024:
 - Cybersecurity Governance
 - Encryption
 - Incident Response and Business Continuity
 - **Small Business Increased Requirements (MFA, Cybersecurity Training)**

Sign Up for Alerts on the NYDFS Resource Center.



YOUR NEW OBLIGATIONS UNDER THE NYDFS AMENDED CYBERSECURITY REGULATIONS



INFO@SECURITYBASECAMP.COM



[HTTP://WWW.SECURITYBASECAMP.COM/](http://www.securitybasecamp.com/)



(949) 330-0899

KEY CONTACTS: IF YOU HAVE QUESTIONS, REACH OUT TO:

John Cooney

The Law Office of John J. Cooney
(631) 949-2626
jcooney@jcooneylaw.com

Paul Osterberg

Security Basecamp
(949) 330-0899
paul@securitybasecamp.com

Vincent Guyaux

Buckler
(646) 315-4161
vincent@buckler.app

Scott Smith

Buckler / Security Basecamp
(612) 805-8400
scott@buckler.app
ssmith@securitybasecamp.com



APPENDICES

BONUS MATERIAL

4 STEPS

TO KEEP YOU CYBER SAFE



1



TURN ON MULTI-FACTOR
AUTHENTICATION

2

UPDATE YOUR
SOFTWARE



3

THINK BEFORE
YOU CLICK



4

USE STRONG
PASSWORDS



CISA.GOV



MITRE ATT&CK® AND DEFEND® FRAMEWORKS: EFFECTIVELY USING CYBERSECURITY RESOURCES

- [MITRE ATT&CK® Framework](#)
- Globally-Accessible Knowledge Base of Adversary Tactics and Techniques
- Understand Mitigations that Can Be Employed to Prevent Attacks.
- [MITRE DEFEND® Framework](#)

ATT&CK®

Getting Started Take a Tour

Contribute

Blog [↗](#)

FAQ

Random Page | ▾

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world – by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.



ATT&CK v14 has been released.
We hope everyone will enjoy our latest treats!

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (2)	Drive-by Compromise	Command and Scripting Interpreter (2)	BITS Jobs	Access Token Manipulation (2)	Access Token Manipulation (2)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (2)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (2)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Gather Victim Network Information (2)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (2)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (2)	Debugger Evasion	Forceful Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Data Obfuscation (2)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (2)	Phishing (4)	Inter-Process Communication (2)	Compromise Client Software Binary	Boot or Logon Initialization Scripts (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Storage Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (2)	Replication Through Removable Media	Native API	Create Account (2)	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Endpoint Denial of Service (4)	Financial Theft
Search Open Technical Databases (3)	Stage Capabilities (4)	Supply Chain Compromise (2)	Scheduled Task/Job (2)	Create or Modify	Domain Policy	Direct Volume Access	Modify	Container and Resource Discovery	Taint Shared Content	Data from Configuration	Ingress Tool Transfer	Firmware Corruption	



CISA: EFFECTIVELY USING CYBERSECURITY RESOURCES

- Access Insights Into Threat Intelligence & See the Future of Cybersecurity Tech in Action.
- Subscribe to Alerts and Guidance
- [Cybersecurity & Infrastructure Security Agency \(CISA\)](#)
- [Resources & Tools | CISA](#)
- [CISA Tabletop Exercise Packages | CISA](#)
- [Zero Trust Maturity Model Version 2.0 \(cisa.gov\)](#)



The screenshot shows the CISA website homepage. At the top left is the CISA logo and the text "CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY" and "AMERICA'S CYBER DEFENSE AGENCY". To the right is a search bar. Below the header is a navigation menu with "Topics", "Spotlight", "Resources & Tools", "News & Events", "Careers", and "About". A red "REPORT A CYBER ISSUE" button is on the right. Below the navigation is a "Home" link and social media share icons for Facebook, Twitter, LinkedIn, and Email. The main content area has a dark red background with the text "SHIELDS UP!" and "As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyberattacks." A large blue shield icon with a white upward arrow is on the right. At the bottom, there is another "REPORT A CYBER ISSUE" button and the text "Organizations should report anomalous cyber activity and or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870."



NYDFS CYBERSECURITY REGULATION: BREAKING DOWN WHAT WAS REQUIRED 2017 – NOV 2023

Under the DFS 23 NYCRR 500, a firm licensed in NY may be classified as a “Limited Exempt” entity. Under this designation, many of the controls within the DFS framework are considered “not-applicable.”

The “Limited Exempt” status can be assigned to any NY State financial or insurance institution that meets any one of the following criteria.

- Fewer than 10 employees including any independent contractors, **(changed to 20)** OR
- Less than \$5M in gross annual revenue **(changed to < \$7.5M)** in NYS each of the last 3 fiscal years, OR
- Less than \$10M in year-end total assets **(changed to < \$15M)**

CORE TO ALL - Cyber Program Elements:

#	Targeted Requirement Area(s)
500.02	Cybersecurity Program
500.03	Cybersecurity Policies
500.07	Limit User Access
500.09	Risk Assessment
500.11	Third-Party Service Providers
500.13	Data Retention Policies
500.17	Notification to DFS

Non-Exempt Must Also Complete

#	Targeted Requirement Area(s)
500.04	Employ a Chief Information Security Officer
500.05	Conduct Penetration Testing and Vulnerability Assessments
500.06	Implement Audit Trails
500.10	Employ Cybersecurity Personnel
500.12	Use of Multifactor Authentication (becoming effective for Small Companies)
500.14	Cybersecurity Awareness Training (becoming effective for Small Companies)
500.15	Encryption of NPI
500.16	Incident Response Plan
500.08	Application Security Procedures (if applicable)

REPORTING CYBERSECURITY INCIDENTS

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

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.

