BIG I | NEW YORK

BIG I NEW YORK
SUMMARY OF 2ND AMENDMENT TO 23 NYCRR 500
CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

CHANGE	DEADLINE FOR COMPLIANCE

Changes to Exemptions
• Limited exemption applies to entities with:
  ○ Fewer than 20 employees and independent contractors of entity and its affiliates.
NOTE: "AFFILIATE" IS SOMEONE WHO CONTROLS THE ENTITY, THAT THE ENTITY CONTROLS, OR IS UNDER COMMON CONTROL WITH SOMEONE ELSE.
  ○ Less than $7.5 million in gross annual revenue in each of last 3 fiscal years from all of entity's business operations and New York operations of its affiliates.
  ○ Less than $15 million in year-end total assets including affiliates' assets.
• Individual licensed insurance brokers who qualify for an exemption because they do not use information systems or nonpublic information are exempt from the regulation's requirements if they:
  ○ Have not acted as an insurance broker for compensation for at least 1 year, and
  ○ Do not otherwise qualify as covered entities.
• Notices of Exemption must be filed electronically using form on DFS website.
• Regulation's requirements do not apply to:
  ○ Reciprocal jurisdiction reinsurers.
  ○ Licensed insurance agents whose licenses are in inactive status.
  ○ Licensed mortgage loan originators whose licenses are in inactive status.
	Nov. 1, 2023

Changes to Enforcement
• Violation of the regulation defined as:
  ○ Committing a single prohibited act.
  ○ Failing to act to satisfy any of the requirements.
• Violations include without limitation:
  ○ Failure to secure or prevent unauthorized access to nonpublic information due to noncompliance with any of regulation's sections.
  ○ Material failure to comply with any of regulation's sections for any 24-hour period.
• DFS will consider 16 listed factors or more when assessing penalties for violations.
	Nov. 1, 2023

CHANGE	DEADLINE FOR COMPLIANCE

Exemptions From Electronic Filing and Submission Requirements
• Filers required to make electronic filings or submissions under the regulation can apply to DFS for exemption from electronic filing in writing at least 30 days before submitting the filing.
• Request must:
  ○ Provide filer's license number or other identifying number.
  ○ Identify specific filing for which exemption is requested.
  ○ Specify whether filer is making request based on undue hardship, impracticability, or good cause.
  ○ Provide detailed explanation for reason DFS should approve it.
  ○ Specify whether request extends to future filings as well.
• Filer must provide DFS with additional information upon request.
• Filer is exempt from electronic filing if DFS grants exemption with a determination specifying the basis for it.
• Any non-electronic filing must be in form and manner acceptable to DFS.
	Nov. 1, 2023

New Notice of Cybersecurity Incident Requirement
• Must report electronically using the form on the DFS website within 72 hours after determining that a cybersecurity incident has occurred at entity's business, those of its affiliates, or that of a third-party service provider.
 	
NOTE: "CYBERSECURITY INCIDENT" IS A CYBERSECURITY EVENT:
• IMPACTING THE ENTITY AND REQUIRING ENTITY TO NOTIFY AUTHORITIES
• REASONABLY LIKELY TO MATERIALLY HARM A MATERIAL PART OF ENTITY'S NORMAL OPERATIONS, OR
• RESULTS IN RANSOMWARE DEPLOYMENT IN MATERIAL PARTY OF ENTITY'S INFORMATION SYSTEMS
 	
• Entity must
  ○ Promptly provide any information DFS may request regarding the incident.
  ○ Update DFS with any material changes or new information previously unavailable.
	Dec. 1, 2023

CHANGE	DEADLINE FOR COMPLIANCE
Changes to Certification of Compliance Requirement Must submit electronically using form on DFS website by April 15 each year one of the following: • Written certification stating that covered entity materially complied with the regulation's requirements during the prior calendar year. Certification must be based on data and documentation sufficient to accurately determine and demonstrate material compliance. • Written acknowledgment that covered entity did not materially comply with all of the regulation's requirements during the prior calendar year. Must identify all sections of the regulation that the entity has not materially complied with and describe the nature and extent of non-compliance. Must provide either a remediation timeline or confirmation that remediation has been completed. Either statement must be signed by the entity's • Highest-ranking executive and its • Chief information security officer (CISO.) If the entity does not have a CISO, statement must be signed by • Highest-ranking executive and • Senior officer responsible for the entity's cybersecurity program.	Dec. 1, 2023

New Requirement to Report Extortion Payments
Must report electronically using form on DFS website regarding an extortion payment made in connection with a cybersecurity event involving covered entity:
• Notice of the payment within 24 hours
• Within 30 days:
  ○ Written description of the reasons payment was necessary.
  ○ Description of alternatives that were considered.
  ○ All diligence performed to find alternatives.
  ○ All diligence performed to ensure compliance with applicable rules and regulations.
	Dec. 1, 2023

Changes to Cybersecurity Program Requirements • Program must be designed to protect confidentiality, integrity and availability of both entity's information systems and nonpublic information stored on them. • Program documentation and information that must be provided to DFS upon request includes provisions of a cybersecurity program maintained by entity's affiliate (e.g., a bank that owns the agency) and that the entity has adopted. NOTE: THE NEXT ITEM APPLIES ONLY TO COMPANIES WITH REVENUES GREATER THAN $20 MILLION AND EITHER MORE THAN 2,000 EMPLOYEES OR MORE THAN $1 BILLION IN REVENUE. • Must design and conduct independent audits of cybersecurity program based on risk assessment.	April 29, 2024

CHANGE	DEADLINE FOR COMPLIANCE

Changes to Cybersecurity Policies and Procedures Requirement
• Must be approved at least annually by a senior officer or entity's senior governing body.
• Procedures must be developed, documented, and implemented in accordance with the written policy or policies.
• To extent they apply to entity's operations, new items the policy must address include:
  ○ Data retention
  ○ End of life management of information system assets and devices.
  ○ Monitoring of systems security.
  ○ Security awareness and training.
  ○ Systems and application security.
  ○ Third-party service provider management.
  ○ Incident notification.
  ○ Vulnerability management.
	April 29, 2024

NOTE: THESE ITEMS DO NOT APPLY TO ENTITIES THAT QUALIFY FOR LIMITED EXEMPTION
Changes to Vulnerability Management
• Must develop and implement written policies and procedures for vulnerability management designed to assess and maintain cybersecurity program's effectiveness.
• Policies and procedures must ensure that entities:
  ○ Conduct at minimum internal and external penetration testing at least annually.
  ○ Have a monitoring process in place to inform entity of new security vulnerabilities.
  ○ Remediate vulnerabilities promptly and address the most serious risks first.
	April 29, 2024

NOTE: THIS ITEM DOES NOT APPLY TO ENTITIES THAT QUALIFY FOR LIMITED EXEMPTION **Changes to Application Security Requirements** • Procedures, guidelines, and standards for ensuring secure development of in-house developed applications the entity uses must be reviewed, assessed, and updated at least annually.	April 29, 2024
Changes to Risk Assessment • Risk assessment must be reviewed and updated at a minimum annually and whenever a change in the business or technology causes a material change to entity's cyber risk.	April 29, 2024
NOTE: THIS ITEM DOES NOT APPLY TO ENTITIES THAT QUALIFY FOR LIMITED EXEMPTION **Changes to Cybersecurity Personnel and Intelligence** • Choice of affiliate or qualified third-party service provider to assist in complying with regulation's requirements subject CISO requirements.	April 29, 2024

CHANGE	DEADLINE FOR COMPLIANCE
Changes to Third-Party Service Provider Requirements • Limited exception for employees, representatives, agents, and designees of a covered entity who are covered by that entity's third-party service provider policy is deleted because it repeats an exemption stated elsewhere in the regulation.	April 29, 2024
Changes to Monitoring and Training Requirements • Entity must provide all personnel with cybersecurity awareness training that includes social engineering at least annually. • Training must be updated to reflect risks identified in entity's risk assessment.	April 29, 2024
Changes to Exemptions • Entity's wholly owned subsidiary is exempt from the regulation's requirements if it is covered by entity's cybersecurity program. • Subsidiary must file Notice of Exemption.	April 29, 2024

NOTE: THESE ITEMS DO NOT APPLY TO ENTITIES THAT QUALIFY FOR LIMITED EXEMPTION
Changes to Cybersecurity Governance
• CISO's report on entity's cybersecurity program to entity's senior governing body must include plans for remediating material inadequacies.
• CISO must timely report to senior governing body or senior officer on material cybersecurity issues (significant cybersecurity events, significant changes to entity's cybersecurity program, etc.)
• Senior governing body must oversee entity's cybersecurity risk management, including by:
  ○ Having sufficient understanding of cybersecurity matters.
  ○ Requiring entity's executive management to develop, implement, and maintain entity's cybersecurity program.
  ○ Regularly receiving and reviewing management's reports on cybersecurity.
  ○ Confirming that entity's management as allocated sufficient resources for effective cybersecurity.
	Nov. 1, 2024

NOTE: THESE ITEMS DO NOT APPLY TO ENTITIES THAT QUALIFY FOR LIMITED EXEMPTION **Changes to Encryption Requirements** • Entity must implement written policy requiring encryption meeting industry standards. • If encryption of nonpublic information at rest is not feasible, entity may use effective alternative compensating controls that CISO has reviewed and approved in writing. CISO must review feasibility of encryption and effectiveness of alternative controls at least annually.	Nov. 1, 2024

NOTE: THESE ITEMS DO NOT APPLY TO ENTITIES THAT QUALIFY FOR LIMITED EXEMPTION
Changes to Incident Response and Business Continuity Management
• Entity must establish written plans containing proactive measures to investigate and mitigate cybersecurity events and to ensure operational resilience. Must include at least:
  ○ Incident response plans reasonably designed to enable prompt response to and recovery from cybersecurity events materially affecting:
  ▪ Confidentiality, integrity or availability of the covered entity's information systems.
  ▪ Continuing functionality of any aspect of the covered entity's business or operations.
  ○ Incident response plans must address, with respect to different types of cybersecurity events including disruptive events such as ransomware incidents, these areas in addition to the ones already listed:
  ▪ Recovery from backups.
  ▪ Preparation of root cause analysis describing:
  ▪ How and why event occurred.
  ▪ Event's business impact.
  ▪ What will be done to prevent reoccurrence.
  ▪ Updating of plans as necessary.
  ○ Business continuity and disaster recovery plan BCDR plan) reasonably designed to:
  ▪ Ensure availability and functionality of entity's information systems and material services.
  ▪ Protect entity's personnel, assets, and nonpublic information in event of a cybersecurity-related disruption to normal business activities.
  ○ BCDR plan must at minimum:
  ▪ Identify documents, data, facilities, infrastructure, services, personnel, and competencies essential to continuing operations.
  ▪ Identify supervisors responsible for implementing each part of the plan.
  ▪ Include communications plan for contacting essential persons should a cybersecurity-related event disrupt operations.
  ▪ Include procedures for timely recovery of critical data and information systems and prompt resumption of operations after a disruptive cybersecurity event.
  ▪ Include procedures for regularly backing up and copying essential data backup and copying and storing it offsite.
  ▪ Identify third parties necessary to entity's information systems continued operation.
• Entities must ensure that current copies of plans are accessible to all employees responsible for implementing them.
• Entities must train all employees responsible for implementing plans.
• Entity must at least annually test its:
  ○ Incident response and BCDR plans with relevant staff and management and revise them as necessary.
	Nov. 1, 2024

CHANGE	DEADLINE FOR COMPLIANCE
○ Ability to restore critical data and information systems from backups. • Entity must maintain backups necessary to restore material operations and adequately protect them from unauthorized changes or destruction.	
Changes to Exemptions • Entities that qualify for limited exemption will not be exempt from: ○ Multi-factor authentication requirements ○ Requirement to provide annual cybersecurity awareness training, updated to reflect the entity's risks including training on social engineering, for all personnel.	Nov. 1, 2024
NOTE: THESE ITEMS DO NOT APPLY TO ENTITIES THAT QUALIFY FOR LIMITED EXEMPTION **Changes to Vulnerability Management** • Entity's vulnerability management policies and procedures must ensure that it conducts: ○ Automated scans of information systems ○ Manual review of systems not covered by scans. • Purpose is to discover, analyze, and report vulnerabilities. • Frequency of scans determined by risk assessment. Must be done promptly after material system changes.	May 1, 2025

CHANGE	DEADLINE FOR COMPLIANCE

Changes to Access Privileges and Management
• Entity must:
  ○ Limit user access privileges to systems providing access to nonpublic information to only those necessary to perform user's job.
  ○ Limit number of privileged accounts.
NOTE: "PRIVILEGED ACCOUNT" IS AN AUTHORIZED USER ACCOUNT OR SERVICE ACCOUNT THAT PERMITS PERFORMING SECURITY-RELATED FUNCTIONS THAT ORDINARY USERS ARE NOT AUTHORIZED TO PERFORM. AN EXAMPLE IS A SYSTEM ADMINISTRATOR'S ACCOUNT.
  ○ Limit privileged accounts' access functions to only those necessary to perform user's job.
  ○ Limit privileged accounts' use to only when performing functions that require such access.
  ○ Annually review all user access privileges. Remove or disable unnecessary accounts and access.
  ○ Disable or securely configure all protocols permitting remote control of devices.
  ○ Promptly terminate users' access privileges following departures.
  ○ Implement written password policy meeting industry standards.
NOTE: THIS NEXT ITEM APPLIES ONLY TO COMPANIES WITH REVENUES GREATER THAN $20 MILLION AND EITHER MORE THAN 2,000 EMPLOYEES OR MORE THAN $1 BILLION IN REVENUE.
• Monitor privileged access activity and implement:
  ○ Privileged access management solution.
  ○ Automated method of blocking commonly used passwords for all accounts on systems owned or controlled by entity and wherever feasible for other accounts.
	May 1, 2025

NOTE: THESE ITEMS DO NOT APPLY TO ENTITIES THAT QUALIFY FOR LIMITED EXEMPTION
Changes to Monitoring and Training Requirements
• Entity must implement risk-based controls designed to protect against malicious code.
NOTE: THIS NEXT ITEM APPLIES ONLY TO COMPANIES WITH REVENUES GREATER THAN $20 MILLION AND EITHER MORE THAN 2,000 EMPLOYEES OR MORE THAN $1 BILLION IN REVENUE.
• Unless CISO approves use of controls reasonably equivalent or more secure, entity must implement:
  ○ Endpoint detection and response solution.
  ○ Centralized logging and security event alerting solution.
	May 1, 2025

CHANGE	DEADLINE FOR COMPLIANCE

Changes to Multi-Factor Authentication (MFA) Requirements
• Entities that qualify for limited exemption must use MFA for:
  ○ Remote access to entity's information systems.
  ○ Remote access to third-party applications (cloud-based or not) from which users can access nonpublic information.
  ○ All privileged accounts (other than service accounts that prohibit interactive login.)
• Entities that do not qualify for limited exemption must use MFA for any individual accessing any of entity's information systems.
• If entity has a CISO, CISO may approve controls that are reasonably equivalent or more secure. CISO must review these controls at least annually.
	Nov. 1, 2025

Changes to Asset Management Requirements
• Entity must implement written policies and procedures for producing and maintaining an asset inventory of its information systems.
• Policies and procedures must include:
  ○ Method to track information on each asset, including:
  ▪ Owner
  ▪ Location
  ▪ Classification or sensitivity
  ▪ Support expiration date
  ▪ Recovery time objectives.
  ○ Frequency required to update and validate the inventory.
	Nov. 1, 2025