ELANY
EXCESS LINE ASSOCIATION
OF NEW YORK

BULLETIN

120 Wall Street, 24th Floor
New York, New York 10005

Bulletin No. 2025-22

November 7, 2025

RE: FINAL PHASE OF DFS CYBERSECURITY REGULATION – NOVEMBER 1, 2025 REQUIREMENTS

On November 1, 2025, the final set of New York Department of Financial Services (DFS) revise Cybersecurity Regulation (23 NYCRR 500) requirements went into effect. Here is what brokers need to know:

---

1. **All non-exempt brokers must** utilize MFA for *any* individual accessing *any* information system of the broker's enterprise according to Section 500.12.

   If the broker utilizes a CISO, the CISO may approve in writing the use of reasonably equivalent or more secure compensating controls and such controls shall be reviewed periodically but at a minimum annually.

2. **Brokers that have filed for limited exemption under Section 500.19(a) (Small Businesses) must** use Multi-Factor Authentication (MFA) for all remote access to their information systems, remote access to third-party applications (including but not limited to those applications that are cloud based and from which nonpublic information is accessible), and all privileged accounts other than service accounts that prohibit interactive login.

3. **Additionally, under Section 500.13(a) all brokers must** implement written policies and procedures to maintain a complete, accurate, and documented asset inventory of their information systems that includes, among other things, tracking ownership and location.

   At a minimum, such policies and procedures shall include:
   - A method to track key information for each asset, including, as applicable the following:
     - Owner;
     - Location;
       - Classification or sensitivity;
       - Support expiration date; and
       - Recovery time objectives; and
     - The frequency required to update and validate the covered entity's asset inventory.

The previous phase of Cybersecurity Regulations that went into effect on May 1, 2025 are presented in ELANY's Bulletin No. 2025-09 accessible on our website here.

As of the May 1, 2025 deadline, non-exempt brokers as per Section 500.5(a)(2), must implement written vulnerability management policies and procedures based on their risk assessment that include automated scans of information systems as well as manual reviews of systems not covered by said scans.

Also as of the May 1, 2025 deadline, under Section 500.7, brokers must also implement enhanced requirements regarding limiting user access privileges, including privileged account access, review access privileges and remove or 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, and implement a reasonable written password policy to the extent passwords are used. Section 500.19(a) exempt brokers must comply only with the Section 500.7 requirements. Additionally, Section 500.14(a)(2) requires brokers to implement controls to protect against malicious code.

Class A Brokers must comply with Sections 500.5(a)(2), 500.7, 500.14(a)(2), and 500.14(b).

Should you have any questions regarding the content of this bulletin, please direct them to elanyinfo@elany.org.