GreyCastle SECURITY

NEW DRAFT AMENDMENTS FOR NYS DFS PART 500 CYBERSECURITY RULES

greycastlesecurity.com

185 Jordan Road, Suite 3
Troy, NY 12180

(800) 403-8350

MORE NOTIFICATION OBLIGATIONS

- Requiring notification to DFS within 72 hours of unauthorized access to privileged accounts or the deployment of ransomware within a material part of the company's information systems. These are in addition to the existing requirements to notify DFS within 72 hours of any cybersecurity events that require notice to a supervisory body or that have a reasonable likelihood of materially harming a material part of the company's normal operations. Notably, these newly proposed requirements would significantly lower the notification threshold, as they could be triggered before any sign of actual data compromise or exfiltration.
- A new 24-hour notification obligation in the event a ransom payment is made, and a 30-day requirement to provide a written description of why the payment was necessary, alternatives to payment that were considered, and all sanctions diligence conducted.

NEW REQUIREMENTS FOR LARGER "CLASS A" COMPANIES

- These "Class A" companies are defined as entities with over 2,000 employees or over $1 billion in gross annual revenue average over the last three years from all business operations of the company and its affiliates. They must:
  - Conduct weekly systematic scans or reviews reasonably designed to identify publicly known cybersecurity vulnerabilities, and document and report any material gaps in testing to the board and senior management;
  - Implement an endpoint detection and response solution to monitor anomalous activity and a solution that centralizes logging and security event alerting;
  - Monitor access activity and implement a password vaulting solution for privileged accounts and an automated method of blocking commonly used passwords;
  - Conduct an annual, independent audit of their cybersecurity programs; and
  - Use external experts to conduct a risk assessment at least once every three years.

MORE OBLIGATIONS ON COMPANY GOVERNING BODIES

- To ensure the boards of covered entities have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cyber risk;
- To provide the CISO with adequate independence and authority to appropriately manage cyber risks;
- That the CISO will provide the board with additional detailed annual reporting on plans for remediating issues and material cybersecurity issues or events;
- That the CISO will annually review the feasibility of encryption and the effectiveness of any compensating controls for any unencrypted nonpublic information;
- That covered entities' cybersecurity policies must be approved by the board on an annual basis; and
- That add significantly to the annual certification requirements, requiring covered entities to not only certify to their compliance or acknowledge any noncompliance, but also provide sufficient data and documentation to accurately determine and demonstrate compliance, and have such certification or acknowledgment of noncompliance be signed by both the CEO and the CISO.

NEW REQUIREMENTS FOR OPERATIONAL RESILIENCY & IR

- Identifying business components essential to continued operations (documents, data, facilities, personnel, and competencies) and personnel responsible for implementation of the BCDR plans;
- Preparing communications plans to ensure continuity of communications with various stakeholders (leadership, employees, third parties, regulatory authorities, others essential to continuity);
- Maintaining procedures for the back-up of infrastructure and data; and
- Identifying third parties necessary to continued operations.

ENHANCED TECHNOLOGY & POLICY REQUIREMENTS

- Clarify the definition of "privileged accounts" as covering any account that can be used to perform security-relevant functions that ordinary users are not authorized to perform, or affect a material change to technical or business operations. Under the proposals, privileged accounts must:
    - Have multi-factor authentication (with exceptions for certain service accounts); and
    - Be limited in both number and access functions to only those necessary to perform the user's job;
    - Be limited in use to only when performing functions requiring their use of such access;
- Require stricter access management, including periodic review of all user access privileges and removal of accounts and access that are no longer necessary, as well as disabling or securely configuring all protocols that permit remote control of devices;
- Require that emails are monitored and filtered to block malicious content from reaching authorized users;
- Mandate penetration testing be conducted by an independent party at least annually, and also adjust the required frequency of vulnerability assessments from bi-annually to "regular[ly]," with Class A companies conducting weekly scans as noted above;
- Require the use of strong, unique passwords—and Class A companies have additional requirements, as discussed above, relating to passwords and monitoring of access activity;
- Require multi-factor authentication for remote access to the network and enterprise and third-party applications that access nonpublic information; and
- Mandate that covered entities must maintain backups isolated from network connections.
- Implement written policies and procedures to ensure a complete and documented asset inventory for all information systems and their components (e.g., hardware, operating systems, applications, infrastructure devices, APIs, and cloud services); and
- Have asset inventory that must, at a minimum, track each asset's key information (e.g., owner, location, classification or sensitivity, support expiration date, and recovery time requirements).

INCREASED REQUIREMENTS FOR RISK & IMPACT ASSESSMENTS

- Tailored to consider the “specific circumstances” of the covered entity, including size, staffing, governance, businesses, services, products, operations, customers, counterparties, service providers, vendors, other relations and their locations, as well as the geographies and locations of its operations and business relations; and
- Updated at least annually.

CLARIFIED ENFORCEMENT CONSIDERATIONS

- A violation occurs by committing any act prohibited by the regulations or failing to satisfy a required obligation. This includes the failure to comply for more than 24 hours with any part of the regulations or the failure to prevent unauthorized access to nonpublic information due to noncompliance with the regulations.
- DFS may consider certain aggravating and mitigating factors when assessing the severity of penalties, including cooperation, good faith, intentionality, prior violations, number or pattern of violations, gravity of violation, provision of false or misleading information, harm to customers, accuracy and timeliness of customer disclosures, participation of senior management, penalties by other regulators, and business size.