DINSMORE COMPLIANCE SERVICES

AN AFFILIATE OF DINSMORE & SHOHL LLP

SEC Proposes Cybersecurity Risk Management Rules

February 2022

On Feb. 9, 2022 the SEC proposed rules related to cybersecurity risk management for investment advisers and registered investment companies, as well as amendments to certain rules that govern adviser and fund disclosures. The proposed rules would:

- Require advisers and funds to adopt and implement policies and procedures designed to address cybersecurity risks;
- Require advisers to report significant cybersecurity incidents to the SEC on proposed Form ADV-C;
- Enhance adviser and fund disclosures related to cybersecurity risks and incidents; and
- Require advisers and funds to maintain, make and retain certain cybersecurity-related books and records.

Proposed new Advisers Act Rule 206(4)-9 and Investment Company Act Rule 38a-2 require advisers and funds to adopt policies and procedures designed to address cybersecurity risk. The proposed Rule 206(4)-9 and Rule 38a-2 list general elements that advisers and funds are required to address in their cybersecurity policies and procedures. The general elements include the following –

- Risk Assessments
  - Periodic risk assessments to categorize, prioritize and draft written documentation of cybersecurity risks and the information maintained within the systems of advisers and funds.
- User and Security Access
  - Controls designed to minimize user-related risks and prevent the unauthorized access to information and systems. The policies and procedures must include the following:

NEXT

©2022 Dinsmore Compliance Services, LLC. All rights reserved.

    - Requiring standards of behavior for individuals authorized to access information systems, such as an acceptable use policy;
    - Identifying and authenticating individual users, including dual-factor authentication;
    - Procedures for the timely distribution, replacement and revocation of passwords;
    - Limiting access for individuals to the information necessary for such individuals to perform their job tasks; and
    - Securing remote-access technologies.
- Information Protection
    - Monitor information systems to protect information from unauthorized access or use, based on periodic assessments of the information systems and the information that resides on the systems.
- Threat and Vulnerability Management
    - Detect, mitigate and remediate cybersecurity threats and vulnerabilities.
- Cybersecurity Incident Response and Recovery
    - Measures to detect, respond to, and recover from a cybersecurity incident, including policies and procedures designed to ensure:
        - Continued operations of the fund or adviser;
        - The protection of information systems and the information residing on those systems;
        - External and internal cybersecurity incident information sharing and communications; and
        - Reporting of significant cybersecurity incidents to the SEC – Form ADV-C.

In addition, the proposed rules require advisers and funds to review their cybersecurity policies and procedures at least annually. Pursuant to this proposed requirement, funds and advisers must, at least annually:

- Review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk over the time period covered by the review; and
- Prepare a written report – which, at a minimum:
    - Describes the annual review, assessment and any control tests performed;
    - Explains the results for the foregoing;
    - Documents any cybersecurity incident that occurred since the date of the last report; and
    - Discusses any material changes to the policies and procedures since the date of the last report.

In regards to recordkeeping, Advisers Act rule 204-2 would be amended to require advisers to maintain:

- A copy of their cybersecurity policies and procedures that are in effect, or at any time within the past five years were in effect;
- A copy of the adviser's written report documenting

©2022 Dinsmore Compliance Services, LLC. All rights reserved.

the annual review of its cybersecurity policies and procedures for the last five years;

- A copy of any Form ADV-C filed by the adviser in the last five years;
- Records documenting any cybersecurity incident in the last five years; and
- Records documenting an adviser's cybersecurity risk assessments for the last five years.

The proposed Rule and rule amendments is subject to a public comment period for a period of at least 60 days from Feb. 9, 2022

BACK

Questions? Contact the DCS Team

Dinsmore Compliance Services (DCS), an affiliate of Dinsmore & Shohl LLP, offers compliance solutions for investment managers and municipal advisers. DCS will help you develop and maintain high-quality compliance programs customized to your particular business demands and operational realities. We offer these services, all as an affiliate of a coast-to-coast, full-service law firm.

Kevin Woodard
President
(513) 977-8646
kevin.woodard@dinsmorecomplianceservices.com

Jeff Chapman
Director of Client Relations
(513) 977-8647
jeff.chapman@dinsmorecomplianceservices.com

dinsmorecomplianceservices.com

©2022 Dinsmore Compliance Services, LLC. All rights reserved.