omega systems
technology managed

KEY TAKEAWAYS

SEC Cybersecurity Rules for Investment Advisers and Funds

Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (SEC Release No. 11208)

FEB 2022 — SEC proposed Cyber Risk Management rule for registered investment advisers & funds

APR 2022 — Initial public comment period ends; significant feedback provided to Commission

JAN 2023 — SEC releases final vote schedule, indicating Cybersecurity will be slated for April

MAR 2023 — Commission re-opens public comment period through May 22, delaying final vote

OCT 2023 — FINAL VOTE expected by SEC

Since the SEC's Division of Enforcement first established a Cyber Unit in 2017, the Commission's focus on the topic has increased steadily. General market consensus is that the current rules related to cybersecurity are not enough. But do the SEC's proposed rules go too far?

"The [proposed] rules are consistent with the SEC's view that market forces are not going to be enough to force firms to employ good cybersecurity policies. They have to be required to do it." **— Jan M. Folena, former SEC enforcement litigator**

What's Driving Regulatory Action?

- Recent high-profile breaches
- Continued evolution of cyber threats
- Service provider reliance & accompanying risk
- Deterrence to future neglect/wrongdoing

In particular, the increasing reliance on third-party service providers — who are often given significant capabilities to access, store and manage sensitive information — indicates a need for funds and advisers to take action to reduce potential vendor risk and establish/enhance processes to safeguard investor assets.

Key Rule Provisions *(as appear in proposed rules)*

The SEC's proposed cybersecurity rules can be easily divided into four critical categories:

Risk Management Policies & Procedures

- Annual review of written policies & procedures
- Completion & documentation of a "periodic" risk assessment
- Access controls & threat monitoring
- Incident response roles & responsibilities
- Identification of service providers / vendor management & oversight
- Board review, approval & oversight of policies/procedures & incident documentation

Incident Reporting (to SEC)

- Report cybersecurity incidents to the SEC via IARD system and Form ADV-C within 48 hours
- Amend and update the Form as new information is uncovered and as necessary

Disclosure should occur when adviser or fund has "a reasonable basis to conclude that a 'significant' incident has occurred or is occurring."

Incident Disclosure (to Advisers/Investors)

- Disclose all cybersecurity risks that could "materially affect" advisory services
- Disclose security incidents from previous two (2) fiscal years
- Include within Form ADV's Part 2A narrative section

Recordkeeping Requirements

- Maintain copies of policies & procedures (in effect or from previous 5 years)
- Written report/annual review (5 years)
- Completed ADV-C (5 years)
- Documented cyber incidents (5 years)
- Risk assessment documentation (5 years)

What advisers should expect:

The SEC *will* pass a version of these rules through a final vote. It's possible we may see substantive changes following the completion of the second public comment period, but this Commission looks certain to finalize rules on cybersecurity risk management sometime in October 2023.

SEC Compliance Readiness Services

The time to act is now. To get ahead of the SEC's final vote, we recommend scheduling an initial risk assessment & establishing a thorough compliance management process.

Reach out to your existing Omega rep or get in touch with us today:

+ omegasystemscorp.com
+ (610) 678-7002
+ connect@omegasystemscorp.com