SEC Releases New Guidance Related to Investment Funds and Cybersecurity Risks

On April 28, 2015, the SEC's Division of Investment Management released a Guidance Update titled Cybersecurity Guidance (the "Guidance"). The Guidance represents the latest evidence of the SEC's continued focus on cybersecurity issues as they relate to financial services firms, particularly investment funds and advisers. Due to this heightened focus, it is becoming increasingly important for such firms to adopt more advanced and up-to-date cybersecurity protections. Funds and advisers would be well-advised to review their cybersecurity programs and to consider how they might implement some of the recommendations offered by the Guidance.

The Guidance's recommendations to advisers fall into three broad categories, with detailed suggestions for the implementation of each:

- Conduct periodic assessments of the firm's cybersecurity practices.
- Develop a cybersecurity strategy for the firm that is designed to prevent, detect, and respond to cybersecurity threats.
- Implement the strategy through written policies, procedures, and training.

The Guidance notes that periodic assessments should consider: (i) the nature and location of information; (ii) the technology systems used; (iii) internal and external cybersecurity threats and system vulnerabilities; (iv) current security controls and processes; (v) the potential impact of data or system compromise; and (vi) the existing governance structure for managing cybersecurity risks. The Guidance also notes that funds and advisers that share a common network with affiliated entities should consider whether to assess the entire common network.

The Guidance provides specific examples of the kinds of technical safeguards firms should consider deploying as part of their cybersecurity programs, including user credentials management, tiered access to sensitive information and systems, network segmentation, firewalls or other perimeter defenses, and system hardening (e.g., removing non-essential software, unnecessary usernames and logins, and ensuring that software is continuously updated).

The Guidance also suggests that funds and advisers implement data encryption, restrict the removal of media on which sensitive data can be stored, deploy software to monitor and identify unusual events such as unauthorized data exfiltration, and incorporate data backup and retrieval techniques into their cybersecurity program. Firms are also encouraged to adopt an incident response plan to enable a quick and effective response to cyber attacks.

The Guidance further recommends that funds and advisers train their officers and employees regarding potential security threats and measures that can be taken on an individual level to help prevent, detect, and respond to such threats. This includes monitoring internal compliance with cybersecurity policies and procedures.

The Guidance advises funds and advisers to take into account their existing compliance obligations under federal securities laws related to the safeguarding of information in designing and implementing a cybersecurity program and suggests that a non-compliant cybersecurity program could result in violations of

federal securities laws. For example, the Guidance notes that a cyber attack that results in disruptions in service and delays in performing redemption transactions for a mutual fund may implicate section 22(e) of the Investment Company Act of 1940 (redemption requirements) or Rule 22c-1 (requirement to issue shares at NAV).

For further information about how this update may impact your interests, please contact your regular Ropes & Gray contact or a member of Ropes & Gray's leading privacy & data security team.