>>>FAIRVIEW FLASH REPORT <<<

Cybersecurity Guidance

WHAT IS HAPPENING?	Yesterday, the SEC released additional cybersecurity guidance, highlighting the importance of the issue and providing ways in which funds and advisers may address cybersecurity risks. Funds and advisers are encouraged to consider adding the following measures to their compliance programs.
PERIODIC ASSESSMENTS	First, funds and advisers should periodically assess: • The type and sensitivity of data collected by the firm and the technology systems in place; • The internal and external cybersecurity threats posed to the firm's sensitive information and technology systems, and the priority of each threat; • The current cybersecurity processes and governance structure in place, and its effectiveness of managing cybersecurity risk; and • The potential effects of a cybersecurity breach.
DEVELOP A STRATEGY	Second, funds and advisers should develop a strategy reflective of the periodic assessment. The strategy should be designed to "prevent, detect and respond to cybersecurity threats" and may include: • Regulating access to sensitive data by methods such as user authentication, firewalls, and network segregation; • Encrypting sensitive data; • Restricting the use of removable storage media; • Utilizing software to monitor technology systems for unusual events, such as unauthorized use or exfiltration of sensitive data; • Data backup and retrieval; and • Creating an incident response plan. Additionally, funds and advisers should consider whether it is possible to implement cybersecurity procedures that also address federal securities laws. For example, a fund or adviser "could address cybersecurity risk as it relates to identity theft, data protection, fraud, and business

	continuity, as well as other disruptions in service that could affect, for instance, a fund's ability to process shareholder transactions."
IMPLEMENT POLICIES AND PROCEDURES	Lastly, funds and advisers should implement the strategy through written policies and procedures. Periodic training should be conducted to ensure officers and employees of the firm are prepared to prevent, detect and respond to cybersecurity threats. Firms may also wish to provide information to clients and investors to assist in limiting their exposure to cybersecurity threats. Fairview can support clients in formulating and assessing the firm's cybersecurity procedures and in developing and implementing a customized strategy.

Source: SEC Cybersecurity Guidance, April 28, 2015