September 17, 2015

OCIE Issues Additional Information on Cybersecurity Examination Initiative

The SEC's Office of Compliance Inspections and Examinations ("OCIE") recently published[1] additional information on the areas of focus for OCIE's second round of cybersecurity examinations of registered investment advisers and registered broker-dealers. SEC examiners will gather information on cybersecurity-related controls and procedures and will also test to assess implementation of certain firm controls and procedures, focusing on the following areas:

- Governance and Risk Assessment – generally, policies and procedures related to the protection of client records/information and patch management practices (i.e., the development of a systematic and controlled process to update or "patch" vulnerabilities in existing software systems and applications); cybersecurity risk assessment processes; cybersecurity incident response planning.
- Access Rights and Controls – generally, policies and procedures designed to prevent unauthorized access to firm network resources and devices; restrictions on access to certain systems and data via management of user credential, authentication and authorization methods.
- Data Loss Prevention – generally, policies and procedures related to enterprise data loss prevention, data classification, monitoring the transfer of sensitive information outside of the firm (whether authorized or unauthorized).
- Vendor Management – generally, policies and procedures related to the use of third-party vendors; due diligence with regard to vendor selection, monitoring, oversight, contract terms and contingency plans.
- Training – training provided to employees and third-party vendors regarding information security and risks.
- Incident Response – generally, policies and procedures addressing mitigation of the effects of a cybersecurity attack; testing of an incident response plan; records of any cyber incidents.

OCIE included in the risk alert a sample request for information and documents that examiners will be using as part of the Cybersecurity Examination Initiative.

* * *

[1] National Exam Program Risk Alert "OCIE's 2015 Cybersecurity Examination Initiative" (Sept. 15, 2015), see http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Yvonne Y.F. Chan
212-373-3255
ychan@paulweiss.com

Udi Grofman
212-373-3918
ugrofman@paulweiss.com

Michael S. Hong
212-373-3788
mhong@paulweiss.com

Amran Hussein
212-373-3580
ahussein@paulweiss.com

Marco Masotti
212-373-3034
mmasotti@paulweiss.com

Phillip A. Heimowitz
212-373-3518
pheimowitz@paulweiss.com

Stephanie McCavitt
212-373-3558
smccavitt@paulweiss.com

Jyoti Sharma
212-373-3712
jsharma@paulweiss.com

Aubry D. Smith
212-373-3276
ausmith@paulweiss.com

Richard C. Tarlowe
212-373-3035
rtarlowe@paulweiss.com

Lindsey L. Wiersma
212-373-3777
lwiersma@paulweiss.com

Gitanjali Workman
212-373-3201
gworkman@paulweiss.com