April 19, 2022

Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, DC 20549-1090

Re: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (File No. S7-04-22)

Dear Ms. Countryman:

Intercontinental Exchange, Inc. ("ICE"), on behalf of itself and its subsidiaries, appreciates the opportunity to comment on the U.S. Securities and Exchange Commission's ("Commission" or "SEC") Proposed Rule on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies ("Proposal").[1]

ICE provides market infrastructure, data services and technology solutions to a broad range of customers including financial institutions, corporations, and government entities. Through its Fixed Income and Data Services segment, ICE provides, among other things, fixed income pricing, reference data, and corporate actions information designed to support financial institutions' and investment funds' pricing activities, securities operations, research, and portfolio management. We produce daily evaluations for approximately three million fixed income securities spanning approximately 150 countries and 80 currencies, including sovereign, corporate and municipal bonds, mortgage, and asset-backed securities as well as leveraged loans. ICE's reference data complements its evaluated pricing by providing our clients a broad range of descriptive information, covering millions of financial instruments. A U.S. subsidiary of ICE, ICE Data Pricing & Reference Data, LLC, is registered with the SEC under the Investment Advisers Act of 1940 ("Investment Advisers Act"), for its evaluated pricing and other advisory services.

ICE maintains the physical and digital security of its markets, clearing houses, mortgage technology, and data through industry-leading security technology and processes. ICE's Information Security Department consists of diverse and skilled teams that work to protect confidential data from unauthorized access, misuse, disclosure, destruction, modification or disruption.

<u>The Proposal Should not be Based on the Anti-Fraud Provisions in Section 206 of the Investment Advisers Act</u>

ICE generally supports the Commission's initiative to enhance cybersecurity preparedness to improve investor confidence in the resiliency of advisers and funds against cybersecurity threats and attacks. However, we believe that grounding the Proposal in Section 206 of the Investment Advisers Act is misplaced.

[1] https://www.sec.gov/rules/proposed/2022/33-11028.pdf

Section 206(4) states that it is unlawful for an adviser "to engage in any act, practice, or course of business which is fraudulent, deceptive, or manipulative." As it relates to cybersecurity, the fraudulent, deceptive, or manipulative acts are not acts conducted by the adviser but rather by an external party attempting to cause harm to the adviser and the adviser's clients. As stated by Commissioner Peirce in her statement on the Proposal "there is no apparent logical connection between the effectiveness of an adviser's cybersecurity policies and the soundness of its investment advice."[2] ICE believes it would be more appropriate for the Commission to use alternative sources of authority that do not frame potential deficiencies in cybersecurity risk management as a fraudulent activity.

Proposal's Definitions

The SEC asks commenters whether the Proposal's definitions are appropriate and clear and, if not, how these definitions could be clarified within the context of the Proposal. Under the Proposal, an adviser's requirement to report significant cybersecurity incidents to the SEC extends to significant cybersecurity incidents at an adviser's "covered client." Covered client is defined as "a client that is a registered investment company or business development company, or a private fund."[3] ICE believes that the SEC should clarify that the inclusion of "covered client" in the reporting requirement only pertains to the investment adviser of the "covered client", not other service providers of the covered client, whether or not these service providers are registered as advisers or acting under a contract. Such a clarification would be similar to that provided by the Commission in the adopting release for Rule 2a-5 under the Investment Company Act of 1940.

Annual review of the design and effectiveness of the cybersecurity policies and procedures

The SEC asks for comment on whether there should be additional, fewer, or more specific requirements for the annual review or written report. ICE believes the Proposal creates uncertainty as to what would be deemed reasonable and effective policies and procedures. The Proposal is detailed and not entirely consistent with existing, widely-accepted cybersecurity best practices. For example, the proposed specific contract requirements for oversight of third-party providers are more prescriptive than those included in widely-accepted and risk-based cybersecurity best practices and could needlessly limit an adviser's ability to contract with certain service providers. The emphasis on inventory as part of the annual risk assessment, as described in "Categorize and prioritize cybersecurity risks *based* on an inventory of the components" (italics added), diverges from the spirit of the widely-accepted NIST CSF that does not base the risk "Identify" function primarily on inventory but instead includes asset management as one of many areas, alongside understanding those assets in the context of the critical workflows and the overall business environment. In addition, the Proposal does not explicitly acknowledge these widely-accepted cybersecurity best practices. The combination of detailed requirements with no general references to existing widely-accepted cybersecurity standards and frameworks as a "safe harbor," introduces uncertainty as to whether following industry best practices would satisfy the requirements in the Proposal.

---

[2] https://www.sec.gov/news/statement/peirce-statement-cybersecurity-risk-management-020922

[3] See https://www.sec.gov/rules/proposed/2022/33-11028.pdf p.41

The Proposal implies that widely-accepted cybersecurity best practices align with the Proposal by stating in the accompanying text that "Registrants that have already implemented cybersecurity policies and procedures that adhere to best practices and are consistent with the proposed rules are not expected to undertake material changes to their existing policies and procedures, in which instance the proposed rules would have limited added benefits."[4] However, the proposed rule text does not include such language regarding adherence to best practices.

Incorporating a reference to widely accepted cybersecurity standards and frameworks would be consistent with other SEC regulations, such as Regulation SCI, which specifically states that:

> "For purposes of this paragraph (a), such policies and procedures shall be deemed to be reasonably designed if they are consistent with current SCI industry standards, which shall be comprised of information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization. Compliance with such current SCI industry standards, however, shall not be the exclusive means to comply with the requirements of this paragraph (a)"[5]

In its cybersecurity management, ICE relies heavily on technology, reviews a variety of different standards and frameworks or best practices, and then adopts a derivative of multiple standards, customizing them for the systems at issue and any applicable regulatory requirements. ICE is of the opinion that reasonable policies and procedures should be forward-looking, and sufficiently nimble to respond dynamically to changes and threats as they arise, which may not be achieved if a rule is too prescriptive or refers to a specific standard. For this reason, ICE recommends including language similar to that in Reg SCI 1001(a)(4), which would support the ability of companies to be consistent in the development and implementation of cybersecurity programs across the enterprise, while allowing enough flexibility to update the program as best practices or circumstances evolve.

The SEC also asks whether advisers and funds should be required to have their cybersecurity policies and procedures periodically audited by an independent third party to assess their design and effectiveness, whether there are particular cybersecurity-focused audits or assessments that should be required, and whether any such audits or assessments should be required to be performed by particular professionals (*e.g.,* certified public accountants).

As discussed above, the lack of a general reference to existing widely-accepted cybersecurity standards and frameworks in the proposed rule text creates uncertainty in the implementation and assessment of the effectiveness of such implementation. Without such clarity, auditing any cybersecurity program's compliance with rule requirements by an independent third-party would be extremely challenging. Even if the proposed rule is amended to make such references, ICE believes that a third-party audit should not be required, but instead provide that an adviser could choose whether the review is done by an internal audit group, a third party or a combination of the two based on the adviser's risk assessment.

---

[4] See https://www.sec.gov/rules/proposed/2022/33-11028.pdf p.86

[5] See Rule 1001(a)(4)

Finally, ICE suggests that the SEC clarify that the written report required under the Proposal be an internal, confidential report. Given the proposed scope of the report, it could include sensitive information about the state of the adviser's cybersecurity program, the effectiveness or weaknesses of specific controls, and, potentially, details about cyber incidents. All of this information, if disclosed, could provide malicious actors with information about possible weaknesses in the adviser's cybersecurity control framework. Therefore, ICE believes that it is imperative that the sharing of such report with a regulator, if required, be on a confidential basis.

* * * * *

ICE appreciates the opportunity to present its perspective and views on the Commission's Proposal. Should any questions arise about the content of this letter, please do not hesitate to contact me.

Respectfully submitted,

Sigal Lewkowicz

Sigal Lewkowicz
Interim Chief Compliance Officer
ICE Data Pricing & Reference Data, LLC