Chanda Brady
Associate Director, ACLI
202-624-2314 t
chandabrady@acli.com

Via email to rule-comments@sec.gov

Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

May 22, 2023

Re: Proposed Rule: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period
File Number S7-04-22

Dear Ms. Countryman,

Thank you for the opportunity to provide additional comments to the Securities and Exchange Commission ("SEC") on the reopened "Investment Management Cybersecurity Release" ("release").[1] The American Council of Life Insurers (ACLI)[2] recognizes the threat cyber incidents pose to consumers and the United States financial market. The ACLI supports national, uniform, and risk-based cybersecurity standards to combat this threat.

The ACLI commented on the release when it was initially proposed last year.[3] We ask that the SEC consider our initial comments in its ongoing assessment of the release. In light of the SEC's recently proposed cybersecurity rules, as well as the broader state and federal cybersecurity regulatory landscape, the ACLI's original comments on the release remain unchanged. However, our members' concerns about the release's alignment with existing cybersecurity frameworks and pending proposals have grown.

[1] https://www.federalregister.gov/documents/2023/03/21/2023-05766/cybersecurity-risk-management-for-investment-advisers-registered-investment-companies-and-business

[2] The American Council of Life Insurers (ACLI) is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 280 member companies represent 94 percent of industry assets in the United States.

[3] https://www.sec.gov/comments/s7-04-22/s70422-20123086-279413.pdf

Regarding the overlapping SEC cybersecurity proposals recently released for public comment, we echo Commissioner Mark T. Uyeda's statement[4] that,

> "[T]he Commission has provided little analysis as to how the proposals interact with each other or how, as a group, they mitigate cybersecurity risks in the most efficient manner. The lack of an integrated regulatory structure may even weaken cybersecurity protection by diverting attention to satisfy multiple overlapping regulatory regimes rather than focusing on the real threat of cyber intrusions and other malfeasance."

We urge the SEC to both align its cybersecurity proposals with each other, as well as existing federal and state regulatory frameworks[5], to eliminate unnecessary, duplicative, and expensive requirements that would confuse consumers and divert regulated entities from a strong, proactive cybersecurity posture. Targeted, coordinated SEC cybersecurity requirements will help investment advisers and investment companies to focus their resources on preventing and mitigating cyber incidents.

Much work has gone into studying the elements of an effective cybersecurity framework. We recommend that the SEC make use of this work in developing and harmonizing its own rulemaking. The National Institute of Standards and Technology (NIST)'s cybersecurity framework[6] is well-regarded and widely used. The SEC should consider aligning its proposed cybersecurity requirements with the best practices delineated in the NIST framework.

The Financial Stability Board (FSB)'s consultative document, "Achieving Greater Convergence in Cyber Incident Reporting" is another example of recently developed guidance.[7] The FSB document explains the concept of a common format for incident reporting exchange (FIRE).[8] The FSB's

---

[4] https://www.sec.gov/news/statement/uyeda-statement-regulation-sp-031523

[5] For example, in November 2021, the Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) published a rule imposing notification requirement on banking organizations and bank service providers not later than 36 hours after certain "computer-security incidents" that may materially and adversely impact the banking organization. Notification requirements include those related to a non-bank affiliate insurer.

Further, many of ACLI's member companies sell vision, dental, and long-term care insurance, and may be subject to HIPAA's federal cybersecurity reporting requirement. HIPAA mandates that if a data breach occurs which exposes the personal health information of more than 500 individuals, the Department of Health and Human Services' Office for Civil Rights must be notified "without unreasonable delay," and certainly within 60 days of the discovery of the breach.

Many businesses also report under the Payment Card Industry Data Security Standard (PCI DSS), which establishes cybersecurity controls and business practices that any company that accepts credit card payments must implement. Per the PCI DSS, merchants have an obligation to notify their payment processor of any breach.

When the Cybersecurity and Infrastructure Security Agency (CISA) completes its rule-making process under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), covered entities will be required to report covered cyber incidents to CISA within 72 hours and ransomware payments within 24 hours.

Additionally, all 50 states and DC have data security breach notification requirements.

[6] https://www.nist.gov/cybersecurity

[7] https://www.fsb.org/2023/04/achieving-greater-convergence-in-cyber-incident-reporting-overview-of-responses-to-consultative-document/

[8] https://www.fsb.org/wp-content/uploads/P171022.pdf (pg. 24)

document also offers multiple specific recommendations, including one pertaining to overlapping cyber incident reporting processes. It states:

> Potential approaches include implementing unified cyber incident reporting to all relevant authorities or designating a lead reporting authority to receive reports and disseminate this information to other authorities as appropriate. Authorities in such cases should seek to use common reporting formats for the dissemination of information, which can additionally support the delivery of individual report instances to multiple authority recipients.[9]

Though it speaks specifically to the insurance industry, the International Association of Insurance Supervisors' Global Insurance Market Report on Cyber expresses some of the benefits harmonization would provide. The Report states:

> Continue to support efforts to harmonize cybersecurity standards applicable to insurers so that comparisons can be made within and across jurisdictions. Such harmonization would help insurers' micro- and macroprudential supervision and reduce the regulatory burden on insurers, especially those that are internationally active.[10]

This assessment is equally applicable to the SEC. Ultimately, harmonization would ease and support the SEC's supervisory work and further its long-standing three-part mission—to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.[11]

Though cybersecurity incidents have increased in recent years, rapidly layering cybersecurity compliance requirements onto regulated entities is unlikely to be an effective solution. The SEC should slow its rule-making process to allow sufficient time to engage with other government agencies and stakeholders. Coordination will help the SEC to construct a framework that will effectively address cybersecurity threats well into the future.

Thank you for considering both our initial and supplemental comments on the proposed Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies rule.

Sincerely,

Chanda Brady
Associate Director and Cybersecurity Working Group Lead, ACLI

[9] https://www.fsb.org/wp-content/uploads/P171022.pdf (pg. 12)
[10] https://www.iaisweb.org/uploads/2023/04/GIMAR-2023-special-topic-edition-on-cyber.pdf (pg. 42)
[11] https://www.sec.gov/our-goals