

April 7, 2022

Via email to rule-comments@sec.gov

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

Re: **Proposed Rule: Cybersecurity Risk Management for Investment Advisers,
Registered Investment Companies, and Business Development Companies
File Number S7-04-22**

Dear Ms. Countryman,

Thank you for the opportunity to provide comments to the Securities and Exchange Commission (“SEC”) on the Proposed Rules for advisors regarding cybersecurity requirements. We may have additional comments on the proposal related to Funds.

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 95 percent of industry assets in the United States.

Executive Summary

ACLI member companies appreciate the opportunity to share comments regarding the Proposed Rule. Our members are most concerned about the following aspects of the proposal: alignment and consistency with existing cybersecurity frameworks, the definitions proffered, and the notice requirements, specifically as they relate to materiality and harm. Our members have also provided direct responses to the questions posed throughout the proposal. Please see Appendix A for further detail.

Alignment and Consistency with Existing Frameworks

ACLI members believe that overall, any cybersecurity proposals generated by the SEC should be aligned and consistent with existing cybersecurity frameworks, particularly the NY DFS framework. Harmonization with existing frameworks will be extremely helpful in reducing unnecessary compliance burden. Our members would recommend that overall, the policies and procedures

proposed should be less prescriptive and allow flexibility to account for the multiple existing cybersecurity frameworks and various regulatory requirements to which organizations are already subjected. For example, removing references to inventories and required components within risk assessments is appropriate. Additional flexibility in service provider requirements would also be helpful. We note that some entities are trying to develop holistic programs that meet all their various regulatory requirements, as well as are appropriate for the size and the risks of the entity, and this is made much easier by harmonization and flexibility. Our members would also urge the SEC not to prescribe one cybersecurity framework over another, as that would be unduly burdensome to entities subject to differing requirements.

Consistent with the above points, we also specifically urge that advisors employed by a larger parent entity need not create their own protocols. New York Regulation 500 provides such an exception in subsection 500.19(b) that states: An employee, agent, representative or designee of a covered entity, who is itself a covered entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the covered entity.

Definitions

ACLI members have concerns with a few of the definitions provided in the proposal. Specifically, they feel that certain key definitions are overly broad. ACLI members believe that the definition of personal information provided is overly broad and would recommend that definition be changed to reflect the definition of personal information in existing cybersecurity frameworks. They also believe that the definition of cybersecurity incident is overly broad and would note that the inclusion of the word “jeopardizes” reads as subjective. We recommend editing that definition to remove the reference to “jeopardizes” and to reflect more closely existing definitions in other cyber frameworks. For example, there are existing privacy notification requirements that define personal information within the NAIC Cybersecurity model. There likely are other appropriate references that can be incorporated.

Fund Information as defined includes *any electronic information related to the funds business, including personal information, received, maintained, created, or processed by the fund*; this requirement would be onerous given the current definition of personal information as well as this definition including any electronic information related to the funds business. In addition, Fund information systems is defined extremely broadly also including *any information resources owned or used by the fund, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the fund information to maintain or support the fund’s operations*. As applied to policies and procedures requirements and risk assessments, it is unreasonable to apply requirements to the scope of these definitions and inventory all these components and information. The risk assessment should be determined by the entity based on the size, business model, and sensitivity of the data in scope. The rule should be amended to require a periodic risk assessment of cybersecurity risks and should consider the entities business operations, information collected and stored, and effectiveness of controls in such policies and procedures.

Service Providers & Contract Requirements

We believe it is important that any framework allows for reasonable flexibility with respect to service provider contractual language. Companies may use hundreds or even thousands of third-party vendors to provide supporting services. The extent to which a company has the ability to negotiate specific terms will vary based on the respective sizes of the entities, market conditions and other

factors. Companies should not be precluded from obtaining essential services because of an inability to effectuate mandated contractual language. A related point is that companies commonly rely on third parties to perform certain cybersecurity risk-related tasks. Here too, a recognition of reasonable flexibility in contractual arrangements is desirable.

Notification Requirements

Our members' primary concern is with the proposed guidelines regarding notification to the Commission. Our members have concerns with the timing of the requirements, as well as regarding the materiality aspect. We again urge tying in requirements that exist in current laws and frameworks.

Regarding the timing, we would request a longer notification deadline. A 48-hour deadline would single out Advisors as having the most aggressive reporting deadline we have yet encountered, and our members do not believe that those entities are uniquely exposed to any specific increased cybersecurity risks that would warrant them having such an aggressive deadline. We believe this deadline should be extended to allow for internal determinations to be made, and for remediation efforts, and our members are concerned that a focus on fast reporting takes time away from remediation efforts. This deadline also conflicts with the deadline proposed for public companies in the Commission's recent proposed rules for public companies. We request that the notice requirements here be aligned with other notice requirements. For reference, New York DFS has a 72-hour reporting requirement after the covered entity has determined a cybersecurity event occurred. Our members also have concerns with the fact that the report would require updating within 48 hours of every material update, as well as within 48 hours of conclusion of the investigation. We believe that repeated updates are challenging within that time frame to the level of detail currently requested. These repeated updates also take away from the important response and activities during the event that should be the primary concern of entities.

Beyond that, ACLI members feel that the required reporting of incidents from the past two fiscal years, prior to the promulgation of the proposed rules, is unduly burdensome. They note that any risk assessment requirement will take into consideration prior cybersecurity incidents and will list remediation efforts made by the firm to address vulnerabilities. Our members do not understand why this requirement is necessary and seek additional clarification on how the SEC would use this information.

We note that the reporting timeframe is tied to the concept of materiality, or whether the cybersecurity incident is "significant". Our members do not believe that 48 hours is likely to be enough time to determine the impact of a cybersecurity incident, including materiality or whether or not the incident may be "significant" for a company. Particularly for more significant incidents, the investigation can be complicated. It is unlikely that a company would have the information that the SEC is asking for on Form ADV-C within only 48 hours – such as the nature and scope of the incident; actions to recover from the incident; etc.

Our members believe there should be a clear requirement that an incident should be reported when it is definitely occurring or has definitely occurred. We note that to report an incident when there is no definitive conclusion that there is an incident could lead to many false reports to the Commission, which would have to be rescinded upon further investigation. That would create unnecessary burden for all parties involved due to the influx of unnecessary filings. Any reporting requirement should be tied to cybersecurity events that have been determined to have occurred, and the time period for reporting should not be triggered until that determination has occurred.

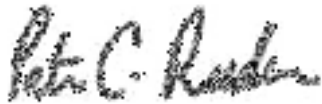
Responses to Specific Questions- See Appendix A

Please see the attached chart with responses to specific questions set forth in the proposal.

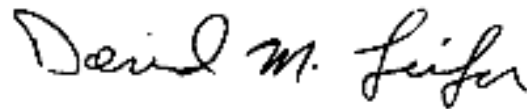
Conclusion

ACLI Member companies continue to digest the impact of these proposed cybersecurity rules, as well as the cybersecurity rules proposed for publicly traded companies. We appreciate the specific questions raised in this proposal. Our members welcome the opportunity to continue with a discussion to make sure that the operations of our members are fully considered.

Very truly yours,



Patrick C. Reeder
Deputy General Counsel



David Leifer
Senior Associate General Counsel

SEC Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies – Responses to Questions for Comment

4/5/22

Key Issues Overview

1. The Rules must limit or include exceptions to disclosures of current or ongoing incidents where such disclosures could: (1) impede cooperation with law enforcement; or (2) create a security risk or adversely affect incident response efforts by the impacted organization.
2. Disclosures of vulnerabilities must be narrowly tailored in such a way as to mitigate the risk of vulnerabilities being exploited by threat actors (especially against other organizations not related to the disclosing organization); this should include a reasonable opportunity to notify the company the provider of the software or device with the vulnerability and for that company to provide an update or patch. This is particularly relevant for zero-day vulnerabilities.
3. Board requirements are too onerous and veer into company management and strategy. Requiring reporting to a board of directors on cybersecurity matters and, even, approval of an overall cybersecurity program, is not uncommon. However, board requirements should not extend further into day-to-day management.
4. Requiring specific cybersecurity credentials or expertise for board members, or even for certain roles within organizations, risks creating an environment of general non-compliance without any discernable benefit to investors. There is a shortage of cybersecurity talent, and specific requirements relating to credentials and expertise will exacerbate that problem. Instead, companies should only be required to provide regular cybersecurity training to staff (and board members) that is appropriate to their particular roles and responsibilities.
5. Rules should leave companies more flexibility to manage their cybersecurity programs in line with their particular business/industry, risks, risk tolerance, and other factors.
6. Vendor and third-party management and disclosures should remain flexible. The level of due diligence that organizations are required to perform on third parties must be reasonable and should permit a risk-based approach in order to be practicable, especially for large organizations with thousands of vendors. Organizations must also retain flexibility with respect to contract terms with vendors and third parties—this is only one way to manage cybersecurity risks. For example, an organization may have little negotiating leverage with respect to a cloud services agreement and may be forced to choose between non-compliance with specific contract terms or foregoing the use of essential technology. However, even without ideal contract terms, the organization could implement other compensating measures to protect against cyber incidents in relation to the cloud services provider. Requiring customer to choose a less dominant provider who may be more agreeable to required contract terms is also likely to result in a less secure platform.
7. Incident reporting and disclosures requirements should be flexible with respect to incidents that directly impact vendors or other third parties. If an incident involves a vendor or other third party, an organization might not have the information that must be disclosed and might be largely dependent on the vendor or third party to provide the relevant information. This will vary on a case-by-case basis depending on the size and sophistication of the vendor or third party, the nature of the incident, and numerous other factors. Allowing for direct impacted vendor reporting would be even more efficient.
8. There is a risk of over disclosure under the proposed rules and a risk that consumers are not equipped to understand disclosures. This could potentially create undue panic among investors that would affect

situations that would likely otherwise be handled in a routine manner (e.g., a widespread vulnerability, like Log4j, that a company identifies and addresses but which is contained and is not exploited).

Responses to Questions for Comment

1	Should we exempt certain types of advisers or funds from these proposed cybersecurity risk management rules? If so, which ones, and why? For example, is there a subset of funds or advisers with operations so limited or staffs so small that the adoption of cybersecurity risk management programs is not beneficial?	
2	Should we scale the proposed requirements based on the size of the adviser or fund? If so, which of the elements described below should not be required for smaller advisers or funds? How would we define such smaller advisers or funds? For example, should we define such advisers and funds based on the thresholds that the Commission uses for purposes of the Regulatory Flexibility Act? Would using different thresholds based on assets under management, such as \$150 million or \$200 million, be appropriate? Would another threshold be more suitable, such as one based on an adviser’s or fund’s limited operations, staffing, revenues or management?	Requirements for the cybersecurity program should be flexible and should be based on several factors, such as the size of the adviser’s and fund’s assets under management, the nature of the operations, staffing, revenue, risk profile, etc. There should not be a one-size-fits-all requirement. This is common in other cybersecurity laws such as insurance data security laws enacted by many states.
3	Are the proposed elements of the cybersecurity policies and procedures appropriate? Should we modify or delete any of the proposed elements? Why or why not? For example, should advisers and funds be required, as proposed, to conduct a risk assessment as part of their cybersecurity policies and procedures? Should we require that a risk assessment include specific components (e.g., identification and documentation of vulnerabilities and threats, identification of the business effect of threats and likelihood of incidents occurring, identification and prioritization of responses), or require written documentation for risk assessments? Should the rules require policies and procedures related to user security and access, as well as information protection?	<p>The proposed high-level elements for policies and procedures are sufficient but should leave flexibility each organization flexibility to address the elements as appropriate.</p> <p>Required components, if any, that would form part of risk assessments should be limited so that organizations maintain flexibility to address cybersecurity risks unique to that organization. For example, a fund that relies on third-party IT infrastructure may have more elements focusing on third-party due diligence and assurances than an adviser that primarily operates its own IT infrastructure. In addition, flexibility is needed such that covered advisers or funds may rely on the cybersecurity programs of parent companies.</p> <p>Risk Assessment policy requirements should be less prescriptive and more flexible and should allow for flexibility with other regulatory requirements.</p> <p>The implicit asset/data inventory concepts should be removed.</p> <p>Regarding service providers, should acknowledge bargaining position differences in requirements.</p> <p>Regarding written documentation, documentation about smaller events is going to be different than “significant”. We seek clarification on that point and that there will not be</p>

		<p>an expectation of consistent documentation for every event, given their inherent differences.</p>
4	<p>Should there be additional or more specific requirements for who would implement an adviser's or fund's cybersecurity program? For example, should we require an adviser or fund to specify an individual, such as a chief information security officer, or group of individuals as responsible for implementing the program or parts thereof? Why or why not? If so, should such an individual or group of individuals be required to have certain qualifications or experience related to cybersecurity, and if so, what type of qualifications or experience should be required?</p>	<p>Although it is not uncommon for regulations to require companies to designate a role responsible for overseeing a cybersecurity program, requirements should not be included as to who must implement a cybersecurity program. For example, small organizations may have a CIO or CTO who oversees the cybersecurity program and may not have someone with the designated title of CISO. Focusing on a title rather than the function would not further the objective of cybersecurity program oversight.</p> <p>Similarly, the experience requirement should be broad and should only require (at most) that the individual be knowledgeable in cybersecurity. There is currently a severe cybersecurity skills shortage in the U.S. (and across the globe) and requiring specific qualifications or experience risks creating a situation where companies simply cannot hire enough individuals to meet the relevant criteria.</p> <p>Similarly, the experience requirement should be broad and should only require (at most) that the individual be knowledgeable in the area of cybersecurity. There is currently a severe cybersecurity skills shortage in the U.S. (and across the globe) and requiring specific qualifications or experience risks creating a situation where companies simply cannot hire enough individuals to meet the relevant criteria. Such a requirement would also discriminate against many senior-level cybersecurity professionals who may have started their careers in information technology and gained experience through practical work without obtaining qualifications or degrees (which were not widely available until a few years ago and which many competent cybersecurity professionals still do not have).</p> <p>We believe that it would be prudent to require an adviser or fund to specify an individual, such as a chief information security officer as responsible for implementing the program. Some existing cybersecurity laws, such as the New York Department of Financial Services cybersecurity law (23 NYCRR Part 500) and the National Association of Insurance Commissioners model cybersecurity law require the appointment of a chief information security officer who is responsible for the cybersecurity program. Many large financial services companies already have chief information security officers.</p>

5	<p>The Investment Company Act compliance rule prohibits the fund’s officers, directors, employees, adviser, principal underwriter, or any person acting under the direction of these persons, from directly or indirectly taking any action to coerce, manipulate, mislead or fraudulently influence the fund’s chief compliance officer in the performance of her responsibilities under the rule in order to protect the chief compliance officer from undue influence by those seeking to conceal non-compliance with the Federal securities laws. Should we adopt a similar prohibition for those administering a fund’s or adviser’s cybersecurity policies and procedures? Why or why not?</p>	<p>It is important for cybersecurity professionals to have independence to carry out their functions. However, based on experience so far with cybersecurity regulations such as the New York Department of Financial Services Cybersecurity Regulations, the prohibition is not necessary for cybersecurity professionals to be able to carry out their functions. Such a prohibition might lead to outcomes where officer, directors, and others do not question actions taken by the CISO or equivalent.</p>
6	<p>Would advisers and funds expect to use sub-advisers or other third parties to administer their cybersecurity programs? If so, to what extent and in what manner? Should there be additional or specific requirements for advisers and funds that delegate cybersecurity management responsibilities to a sub-adviser or third party? If so, what requirements and why?</p>	<p>Most, if not all, funds and advisers will rely on third parties to administer at least some component of their cybersecurity program, even if only to provide certain security tools and training related to those tools. This is not uncommon throughout the industry, and no additional or specific rules should be promulgated in that respect. Whether an organization outsources some or all of its cybersecurity program, requirements for and practical aspects of due diligence and oversight related to third parties should be the same.</p> <p>Advisers and funds might use third parties to administer their cybersecurity programs. For example, some large financial services companies use an affiliate to administer their cybersecurity program. While we do not believe specific requirements regarding third party administration of a cybersecurity program are necessary, we believe it would make sense for the Rules to contemplate the possibility of third-party management since it is a common practice.</p>
7	<p>Should we include any other cybersecurity program administration requirements? If so, what? For example, should we include a requirement for training staff responsible for day-to-day management of the program? If we require such training, should that involve setting minimum qualifications for staff responsible for carrying out the requirements of the program? Why or why not?</p>	<p>No minimum qualifications for staff should be established. This risks creating a situation where advisers and funds cannot hire to fill roles and satisfy requirements, given the ongoing cybersecurity skills shortage, even though competent individuals may be available who do not possess the requisite qualifications established under the rules. As such, a requirement related to training should only state that individuals responsible for administering components of the cybersecurity program should have or be provided appropriate training tailored to their roles and responsibilities..</p>
8	<p>Are the proposed rules’ definitions appropriate and clear? If not, how could these definitions be clarified within the context of the proposed rules? Should any be modified or eliminated? Are any of them proposed terms too broad or too narrow? Are there other terms that we should define?</p>	<p>The definitions of information systems should explicitly exclude third party information systems, which should be addressed separately.</p> <p>The definition is overbroad for purposes of the reporting obligation and should exclude publicly available information.</p>

9	<p>What are best practices that commenters have developed or are aware of with respect to the types of measures that must be implemented as part of the proposed cybersecurity risk management rules or, alternatively, are there any measures that commenters have found to be ineffective or relatively less effective?</p>	<p>Best practices that are effective should be tailored to the organization and the information or information systems being protected but generally include, at a minimum: appropriate cybersecurity training; use of strong passwords or passphrases; implementation of multifactor authentication for system and application access outside of a defined network; and encryption (as appropriate) based on the sensitivity of information; regular patch management (updating software); deployment of anti-malware software on endpoints; and regular back-ups and business continuity planning.</p>
10	<p>What user measures do advisers currently have for using mobile devices or other ways to access adviser or fund information systems remotely? Should we require advisers and funds to implement specific measures to secure remote access technologies?</p>	<p>Certain best practices, such as strong passwords/passphrases, use of VPNs for access from outside of a corporate network, use of anti-malware software, use of multi-factor authentication, and secure back-ups are common measures to used to protect mobile devices and/or connect to information systems remotely. Because of the rapidly changing nature of technology, specific requirements should not be mandated, because they would quickly become outdated. Instead, a requirement to have a processes and procedures would satisfy this need, along with publication of best practices companies can choose to adopt based on their particular circumstances.</p> <p>We do not believe it would be productive to require advisers and funds to implement specific measures to secure remote access technologies. Advisers and funds use a wide variety of remote access technologies in different ways, depending on a variety of business models. Being prescriptive about securing remote access technologies would most likely be counterproductive.</p>
11	<p>Do advisers and funds currently conduct periodic assessments of their information systems to monitor and protect information from unauthorized use? If so, how often do advisers and funds conduct such assessments? Should the proposed rules specify a minimum assessment frequency, and if so, what should that frequency be?</p>	<p>At a minimum, advisers and funds that are part of larger organization (or group of companies) will typically conduct assessments of information systems as part of the organization's overall cybersecurity program. As such, the rules should only require periodic risk assessments, and any other requirement should only serve as a minimum baseline (e.g., annually or bi-annually). In any case, the requirements should leave enough flexibility so that where assessments may be required under other laws, such assessments will satisfy requirements under these rules.</p> <p>We believe that the correct time frame for advisers and funds to assess their information systems to monitor and protect information from unauthorized use is annually. Such a time frame would align with the proposed requirement of an annual risk assessment.</p>
12	<p>Other than what is required to be reported under proposed rule 204-6, should we require any specific</p>	<p>The policies and procedures will vary by company, but a key requirement will be that the policies and procedures are</p>

	measures within an adviser’s policies and procedures with respect to cybersecurity incident response and recovery?	documented and periodically reviewed and updated, as appropriate, by the relevant company.
13	Should we require that advisers and funds respond to cybersecurity incidents within a specific timeframe? If so, what would be an appropriate timeframe?	<p>No, a specific timeframe for response is not advisable. The timeframe is fact specific and should be reasonable and appropriate under the circumstances. In many cases, threat actors have been found to have been inside companies’ networks for months before discovery. Upon discovery of a cybersecurity incident, companies react quickly because it is in their best interest to do so from an operational, legal, and reputational standpoint. The response (and response time) will vary based on the particular company and its capabilities. For example, large companies often triage and prioritize incidents based on severity, which impacts response times. Imposing a specific response time could force companies to respond to less significant incidents to meet legal requirements at the expense of dedicating resources to incidents that should take more priority.</p> <p>Each cybersecurity incident presents its own facts and circumstances. Depending on the facts and circumstances of a cybersecurity incident, timeframes can vary significantly. Therefore, we believe it would be counterproductive to require advisers and funds to respond to cybersecurity incidents within a specific timeframe.</p> <p>Firms, particularly those with limited resources, may choose a risk-based approach to applying timeframes to incident response. Prescribed timeframe requirements may inadvertently draw resources away from more severe incidents to ensure less severe incidents are receiving an initial response within required timeframes.</p>
14	Should we require advisers and funds to assess the compliance of all service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access adviser or fund information systems and any adviser or fund information residing therein, with these proposed cybersecurity risk management rules? Should we expand or narrow this set of service providers? For example, with respect to funds, should this requirement only apply to “named service providers” as discussed above?	<p>No, the rules should not require advisers and funds to assess the compliance of all service providers, because such a requirement is not practical given the number of service providers companies rely on for everything from email to contract management to cyber defense.</p> <p>We should note there should be a materiality provision to service providers and not just all named service providers. In addition, affiliates should be exempt from such definition, as well as UIT separate accounts and their underlying funds, or any entities or parties that are under the compliance of the entities’ cybersecurity program and policies.</p>
15	How do advisers and funds currently consider cybersecurity risks when choosing third-party service providers? What due diligence with respect to cybersecurity is involved in selecting a service provider?	Third party cybersecurity risk is typically assessed along with and in addition to other third-party compliance risks (e.g., financial condition, sanctions and anti-money laundering requirements, privacy risks, etc.). Cybersecurity risk is generally assessed taking a risk-based approach to the relationship with a third-party service provider, considering for example, whether any network connections will be established with the third-party service provider, the nature

		and sensitivity of any data the service provider would handle, the legal regime under which the third-party service provider operates, etc.).
16	How do advisers and funds reduce the risk of a cybersecurity incident transferring from the service provider (or a fourth party (i.e., a service provider used by one of an adviser's or fund's service providers)) to the adviser today?	Third party service provider risks are typically managed through appropriate due diligence based on the nature of the services and data being handled by the service provider; through contractual requirements imposed on the service provider and its service providers; and through ongoing engagements with and oversight of the service provider.
17	Should we require advisers' and funds' cybersecurity policies and procedures to require oversight of certain service providers, including that such service providers implement and maintain appropriate measures designed to protect a fund's or an adviser's information and information systems pursuant to written contract? Do advisers and funds currently include specific cybersecurity and data protection provisions in their agreements with service providers? If so, what provisions are the most important? Do they address potential cybersecurity risks that could result from a cybersecurity incident occurring at a fourth party? Should any contractual provisions be specifically required as part of these rules? Should this requirement apply to a more limited subset of service providers? If so, which service providers? For example, should we require funds to include such provisions in their agreements with advisers that would be subject to proposed rule 206(4)-9? Are there other ways we should require protective actions by service providers?	<p>Companies must retain flexibility to contract with and maintain oversight of third-party service providers as appropriate based on the nature of each service provider relationship. Prescriptive requirements on how to manage these relationships are not advisable. In some cases, such as with SaaS providers or cloud-hosting providers, companies may not have the leverage to impose certain contractual terms and conditions on the service providers, so imposing strict contractual requirements will put companies in the position of choosing to either forego necessary services, choose a less secure but more contractually accommodating service provider, or to enter contracts that do not comply with the rules. Instead, in those cases where specific contractual terms are not feasible, a company could choose to manage the cybersecurity risk with a third-party service provider in other ways, such as due diligence and ongoing assessments, through cyber risk insurance, or through other means.</p> <p>Contractual requirements should only require companies to maintain and carry out policies and procedures to oversee cybersecurity risks related to third party service providers as appropriate based on the nature of the relationship, the services provided, and the potential resulting cyber risk.</p>
18	Do advisers or funds currently consider their or their service providers' insurance policies, if any, when responding to cybersecurity incidents? Why or why not?	This consideration will vary depending on the nature and severity of the incident, as well as contractual obligations between a company and its services providers and customers.
19	Are advisers and funds currently able to obtain information from or about their service providers' cybersecurity practices (e.g., policies, procedures, and controls) to effectively assess them? What, if any, challenges do advisers and funds currently have in obtaining such information? Are certain advisers or funds (e.g., smaller or larger firms) more easily able to obtain such information?	<p>Third party service providers are generally willing to provide information about their cybersecurity practices and procedures. However, the quality and level of detail of information varies widely. The level of detail able to be obtained often ties to the power dynamic in the relationship.</p> <p>Yes. Advisers and funds currently can obtain information from or about service providers' cybersecurity practices to enable them to adequately assess their service providers' cybersecurity programs.</p>
20	Should there be additional, fewer, or more specific requirements for the annual review or written report? Why or why not?	No, additional requirements for an annual review or written report should be imposed; organizations should have a large degree of flexibility to address to the cyber risks specific to

		<p>that organization.</p> <p>Our members seek clarification on how the annual review differs from the risk assessment requirement under the policies and procedures question. The two concepts seem very intertwined and potentially duplicative.</p>
21	Is the proposed requirement for advisers and funds to review their cybersecurity policies and procedures at least annually appropriate? Is this minimum review period too long or too short? Why or why not?	The requirement to review policies and procedures at least annually is not unreasonable, so long as the requirement is limited to this.
22	Should the annual review include whether the cybersecurity policies and procedures reflect changes in cybersecurity risk over the time period covered by the review? Why or why not?	This requirement would be best addressed in guidance issued related to the annual review requirement.
23	Should management, a cybersecurity officer, or a centralized committee be designated to conduct the annual review and prepare the report? Would additional specificity promote accountability and adequate resources? Should relevant expertise be required? Why or why not?	<p>Because of cybersecurity staff shortages, specific requirements that certain individuals or committees conduct the annual review should be avoided. As an example, there is no reason a competent third party, such as a law firm or cybersecurity consultant could not conduct a thorough annual review and provide findings and recommendations, particularly for smaller companies that may not have dedicated cybersecurity staff. Specific expertise should similarly not be required, because it will be overly restrictive and will likely raise the cost significantly of conducting annual reviews of policies and procedures.</p> <p>We believe it would not be productive to require a certain designee to conduct the annual review and prepare the report. Each organization subject to the rule has its own business practices and internal structure and different approaches will be appropriate for different organizations. Therefore, additional specificity would most likely be counterproductive.</p> <p>The provisions drafted for the board oversight are too prescriptive. Board Oversight provision appears to be management and not oversight. The board should not approve policies and procedures and be provided annually a report detailing material cybersecurity risks, overall effectiveness of the program including policies and procedures, and material cybersecurity events during the reporting period.</p>
24	Would the proposed annual review raise any particular challenges for smaller or different types of advisers or funds? If so, what could we do to help mitigate these challenges?	
25	Are there any conflicts of interest if the same adviser or fund officers implement the cybersecurity program and also conduct the annual review? How can those conflicts be mitigated or eliminated? Should advisers and funds be required to have their cybersecurity policies and	While conflicts of interest could be presented if the same adviser or officers implement the cybersecurity program and conduct the annual review, the likelihood of the conflicts materializing or impacting the review should be low. In most cases, from a practical perspective, the

	<p>procedures periodically audited by an independent third party to assess their design and effectiveness? Why or why not? If so, are there particular cybersecurity-focused audits or assessments that should be required, and should any such audits or assessments be required to be performed by particular professionals (e.g., certified public accountants)? Would there be any challenges in obtaining such audits, particularly for smaller advisers or funds?</p>	<p>individual(s) overseeing the cybersecurity program will not be the same individual(s) conducting the annual review, even though they would likely be involved in the annual review. That fact will mitigate some of the risk of conflicts of interest.</p> <p>Cybersecurity audits may be conducted by an audit function or by more specialized IT security or consulting firms. As such, the rules should not require specific assessments or audits, except to the extent the rules outline baseline components of the cybersecurity program that should be reviewed (e.g., access controls, incident response plans, implementation of multifactor authentication). Large organizations in particular are likely to have the resources and expertise in-house to conduct the annual review, so requiring that it be conducted by an independent third party will increase costs without providing a clear benefit.</p> <p>We do not believe that it would be an added value to require cybersecurity programs, policies and procedures to be audited by an independent third party to assess their design and effectiveness. Having learned from other contexts in which independent third-party reviews are required, the costs of an independent third-party review are high while the benefit received by such a review is minimal.</p>
26	<p>Should the Commission require a fund's board, including a majority of its independent directors, initially to approve the cybersecurity policies and procedures, as proposed? As an alternative, should the Commission require approval by the board, but not specify that this approval also must include approval by a majority of the fund's directors who are not interested persons of the fund? Why or why not?</p>	<p>Specifically requiring approval of the cybersecurity policies and procedures by a majority of independent directors should not be a requirement under the rules. Existing laws and regulations require approval and/or oversight of cybersecurity programs (including policies and procedures) by boards of directors. There is no evidence to show that such requirements have resulted in less rigorous board oversight or weaker cybersecurity postures than if the existing obligations were imposed on a majority of the independent directors.</p>
27	<p>As part of their oversight function, should fund boards also be required to approve the cybersecurity policies and procedures of certain of the fund's service providers (e.g., its investment adviser, principal underwriter, administrator, and transfer agent)? Why or why not? If so, which service providers should be included and why?</p>	<p>No, a company's board of directors should not be required to approve the cybersecurity policies and procedures of its service providers. This would go beyond reasonable (or even best practices) with respect to third party due diligence without providing any clear benefit in improving cybersecurity.</p> <p>Companies should have a process to review the cybersecurity practices of their service providers. The board of directors should approve that process. However, the board should not be involved in reviewing, let alone approving, the cybersecurity policies and procedures of every separate legal entity which provides products or services to the company. Instead, such reviews (not approvals) should fall to the experts engaged by the adviser or fund (internal or external) to carry out these processes. If</p>

		<p>a particular business arrangement represents an unusual risk from a cybersecurity standpoint, then it can be escalated to the board through normal channels if and as appropriate.</p> <p>No. Requiring fund boards to approve the cybersecurity policies and procedures of the fund's service providers would impose an undue burden on fund boards as well as service providers. It would be particularly challenging in situations in which a service provider provides services to many different funds.</p> <p>Regarding Boards of Directors, recall the NAIC proposed several changes to the financial conditions examine for cybersecurity experts to be a part of Board of Directors. ACLI may be able to reference previous industry discussion on this piece.</p> <p>The requirement that the Board participate in the approval of the cybersecurity policies and procedures of third-party service providers, and review their contracts and risk assessments, appears to take the function of the Board from oversight to management. Oversight over the firm's cybersecurity program is one thing but extending this to third-party service providers seems problematic.</p>
28	<p>Should a fund's board, or some designee such as a sub-committee or cybersecurity expert, have oversight over the fund's risk assessments of service providers? Why or why not?</p>	<p>Cybersecurity risk is part of a company's overall risk profile, so the board or a specific committee does not need direct oversight of all risk assessments of service providers. That should be managed as part of the day-to-day business operations by the experts engaged by the adviser or fund to carry out these tasks. Particularly, given the volume of service providers that a typical company engages, this would be an unreasonable requirement that would take time that the board could otherwise devote to more high value strategic considerations (regarding cybersecurity and other matters).</p> <p>If a particular business arrangement represents an unusual risk from a cybersecurity standpoint, then it can be escalated to the board through normal channels.</p> <p>We believe that different funds will have different approaches to overseeing the fund's risk assessments of service providers and that many different approaches can be effective. Therefore, we do not think it would be productive to try to dictate which function should have oversight of the fund's risk assessments of service providers.</p>

		<p>Board Oversight (funds)- Feels like management rather than oversight- very granular and detailed report out and approval. What happens if Board doesn't approve? What happens if they don't have the expertise to approve?</p> <p>Reporting is overly prescriptive. Leaves a CISO with a rigid framework of what to cover, rather than options to convey key messages. Getting into control tests, results, any cyber incident and material changes feels too granular for board reporting.</p>
29	Should the Commission require boards to base their approval of cybersecurity policies and procedures on any particular finding, for example, that they are reasonably designed to prevent violations of the Federal securities laws or reasonably designed to address the fund's cybersecurity risks? Why or why not?	Board approval should not be based on a specific finding. Such a requirement could lead to a focus that is too narrow. Instead, the approval should be based on a broader set of requirements that each company is subject to and that are specific to that company.
30	Does the release provide adequate guidance to funds' boards regarding their initial approval of the cybersecurity policies and procedures? Why or why not? Should the Commission provide any additional guidance in this regard? If so, what guidance would assist boards in their approval process? For example, should the Commission provide additional guidance on documentation provided to the board with respect to the initial approval?	No guidance needed.
31	Is the proposed requirement for fund boards to review the required written reports appropriate? The proposed rules would require these reports to be prepared at least annually, and a fund's board would be required to review each such report that is prepared. Should the Commission instead require periodic reviews of a report on the fund's cybersecurity risk management policies and procedures, or specify a shorter or longer frequency for review of such a report? Why or why not?	The annual requirement for the board of directors to review the report is sufficient. A shorter time period would risk diverting time and resources of the board away from other strategic matters.
32	Should the Commission require boards to approve any material changes to the fund's cybersecurity policies and procedures instead of reviewing a written report that discusses such changes? Why or why not?	<p>Requirements for the board to review, rather than approve, material changes are sufficient to ensure the board has appropriate visibility over such changes. This is only a baseline, and boards of individual companies can decide to take on different processes based on their risk profile.</p> <p>We believe it is not necessary to require boards to approve any material changes to the fund's cybersecurity policies and procedures instead of reviewing information discussing the changes. Boards may not have the necessary subject-matter expertise to approve material changes and requiring board approval adds an additional layer of approvals that would delay the implementation of changes.</p>
33	Are the records that we propose to require advisers and funds to keep relating to the proposed cybersecurity risk management rules appropriate? Why or why not? Should	The recordkeeping requirements impose an administrative burden that outweighs the cybersecurity benefit. The time period for retaining certain records (such as policies and

	advisers and funds have to keep any additional or fewer records, and if so, what records?	procedures) should be shortened to a period less than 5 years. The only purpose of the recordkeeping requirement is to ensure compliance, and that can be accomplished through other means at less cost, such as compliance certifications. Re Record Keeping- Records related to response and recovery- if requested be produced how would they be protected?
34	Do advisers or funds have concerns it will be difficult to retain any of documents? Could this place an undue burden on smaller advisers or funds?	Increased document retention means increased costs and administrative burdens. Companies should not be required to keep all documents relating to their cybersecurity program for 5 years. For example, there is little to no benefit, from a cybersecurity perspective to retaining policies and procedures for 5 years.
35	Should we require advisers to report significant cybersecurity incidents of the adviser and covered clients with the Commission? Why or why not? Alternatively, should we exclude incidents that affect private fund clients of an adviser? Should we exclude registered funds and BDCs as covered clients? If so, should we require them to report to the Commission in another manner? How should the Commission address funds that are internally managed? Should we require a separate reporting requirement under the Investment Company Act for such funds? If so, should it be substantially similar to the proposed reporting requirements under rule 204-6?	Independent advisers should not be required to report significant cybersecurity incidents of covered clients. Such a requirement assumes that an adviser will be made aware of such incidents in a timely manner. It also imposes additional obligations on the adviser where the adviser's information and information systems may not be affected in any way and where the adviser is in compliance with the rules. With respect to internally managed funds, incident reporting should be captured under the proposed rules, because from a practical standpoint, IT and information resources are typically shared within an organization. The definition of cybersecurity incident and significant cybersecurity incident are too broad given the definitions of personal information, fund information, and information systems. The requirement to report and fulfill disclosure requirements on individual client incidents is overburdensome and should require a materiality provision.
36	Should we require advisers to report on significant cybersecurity incidents of other pooled investment vehicle clients? For example, should we require advisers to report on significant cybersecurity incidents of pooled investment vehicles that rely on the exemption from the definition of "investment company" in section 3(c)(5)(C) of that Act?	
37	Who should be responsible for having a reasonable basis to conclude that there has been a significant adviser cybersecurity incident or significant fund cybersecurity incident or that one is occurring? Should the Commission require a person or role be designated to be the one responsible for gathering relevant information about the incident and having a reasonable basis to conclude that such an incident occurred?	Each organization should determine and define in its own policies and procedures who will be responsible for concluding that a significant cybersecurity incident has occurred. This will vary based on an organization's size and structure, and there is no one right way for this to be done. As such, the Commission should leave flexibility for organizations to determine the appropriate person(s) or role for reaching this conclusion.
38	At what point would one conclude that there has been a significant adviser cybersecurity incident or significant fund	This will vary case-by-case. However, some reasonable period of assessment will be necessary to determine to assess the nature and (potential) impacts of a cybersecurity

	<p>cybersecurity incident? Would it be after some reasonable period of assessment or some other point?</p>	<p>incident.</p> <p>Companies should have a defined process for identifying incidents and would use the process to determine whether an incident has occurred. The point at which one would conclude an incident has or is occurring is based on executing an incident detection and identification process. The time necessary to complete the process is based on many factors, some outside of company control.</p>
39	<p>Are the proposed definitions of significant adviser cybersecurity incident and significant fund cybersecurity incident appropriate and clear? If not, how could they be made clearer? Should the term critical operations be defined for advisers and funds, and if so what adviser and fund operations should be considered critical? For example, should critical operations include the investment, trading, valuation, reporting, and risk management of the adviser or fund as well as the operation of the adviser or fund in accordance with the Federal securities laws? Alternatively, should there be a quantitative threshold at which operations must be impaired by a cybersecurity incident before an adviser’s or fund’s obligation to report is triggered (for example, maintaining operations at minimally 80% of current levels on any function)? If so, what should that threshold be and how should an adviser or fund measure its operational capacity to determine whether that threshold has been crossed?</p>	<p>The definitions of significant adviser cybersecurity incident and significant fund cybersecurity incident could be clearer. For example, substantial harm to a client, or an investor in a private fund, whose information was accessed is too broad, would be impractical to implement, and should be removed.</p> <p>“Critical operations” should not be defined. Although there may be many common elements, to some extent, what is considered critical will vary across organizations, so this term should allow for that flexibility. Similarly, no quantitative amount should be established as a threshold because it would result in arbitrary decisions.</p> <p>There is no easy way to establish whether a firm is operating at 75% or 80% of operations (as compared with measuring output a firm that manufactures physical products).</p> <p>We believe that the term “critical operations” should be left to the particular adviser or fund to define, because each adviser or fund may operate differently and therefore may have different critical operations.</p>
40	<p>Is the proposed “substantial harm” threshold under the definition of significant adviser and fund cybersecurity incident appropriate? Should we also include “inconvenience” as a threshold with respect to shareholders, clients and investors? In other words, should we also require reporting if the unauthorized access or use of such information results in substantial harm or inconvenience to a shareholder, client, or an investor in a private fund, whose information was accessed?</p>	<p>Substantial harm is appropriate. “Inconvenience” would introduce more ambiguity and too low of a threshold—it is the opposite of substantial harm. For example, if a DDoS attack causes a website to be inaccessible for a few minutes, it might be an inconvenience but would not result in substantial harm.</p> <p>We believe that the term “inconvenience” is unclear and would set an unreasonably low threshold for reporting. No other cybersecurity regulation or law has such a low threshold.</p>
41	<p>Do commenters believe requiring the report 48 hours after having a reasonable basis to conclude that there has been a significant adviser cybersecurity incident or significant fund cybersecurity incident or that one is occurring is appropriate? If not, is it too long or too short? Should we require a specific time frame at all? Do commenters believe that “a reasonable basis” is a clear standard? If not, what other standard should we use?</p>	<p>The reasonable basis standard is clear. Rather than requiring the report within 48 hours after establishing a reasonable basis, requiring the report as soon as reasonably possible would be preferable. The rapidly increasing number of time-bound reporting requirements across regulatory agencies, means that organizations are increasingly spending time during essential periods of incident response, working on multiple (and often</p>

		<p>overlapping) regulatory reports.</p> <p>We believe that a more reasonable reporting requirement would be a time frame substantially longer than 48 hours. The information that emerges within the first 48 hours of a cybersecurity event is often incomplete and inaccurate. A 48-hour reporting requirement most likely will result in an influx of misinformation to the Commission and significant time spent by the Commission clarifying the misinformation received.</p>
42	<p>Should we provide for one or more exceptions to the reporting of significant cybersecurity incidents, for example for smaller advisers or funds? Are there ways, other than the filing of Form ADV-C, we should require advisers to notify the Commission regarding significant cybersecurity incidents?</p>	<p>Another option should be provided to report significant cybersecurity incidents, for example by phone. If an organization has limited or no network access, the organization should be able to file an initial report by phone with basic information and then provide a supplemental report at a later time.</p> <p>Also requiring certain content in other electronic means and not via a formal template Form ADV-C is preferable. Providing substantive notice to the Commission and investors in a reasonable manner under the circumstances is the goal.</p>
43	<p>The Commission recently proposed current reporting requirements that would require large hedge fund advisers to file a current report on Form PF within one business day of the occurrence of a reporting event at a qualifying hedge fund that they advise. The proposed reporting events include a significant disruption or degradation of the reporting fund's key operations, which could include a significant cybersecurity incident. If the amendments to Form PF are adopted, should the Commission provide an exception to the Form ADV-C filing requirements when an adviser has reported the incident as a current report on Form PF? Alternatively, should the Commission provide an exception to the Form PF current reporting requirements if the adviser filed a Form ADV-C in connection with the reporting event?</p>	<p>Yes, exceptions should be made such that a significant cybersecurity incident is only reported to the Commission once, whether on Form PF or on Form ADV-C or elsewhere. The desired outcome is that a significant cybersecurity incident is appropriately disclosed but requiring additional disclosures on different forms imposes an additional burden but does not further the purpose of providing notice to the Commission or to investors.</p>
44	<p>Should advisers be required to provide the Commission with ongoing reporting about significant cybersecurity incidents? If so, are the proposed requirements to amend Form ADV-C promptly, but in no event more than within 48 hours, sufficient for such reporting? Is this timeframe appropriate? Should we require a shorter or longer timeframe? Is the materiality threshold for ongoing reports appropriate? Should we require another mechanism be used for ongoing reporting? For example, should advisers instead be required to provide periodic reports about significant cybersecurity incidents that are ongoing? If so, how often should such reports be required (e.g., every 30 days) and what information should advisers be required to provide?</p>	<p>The nature and potential impact of every cybersecurity incident is distinct. As such, amendments should be required to be made promptly without a specific time frame. In some cases, the requirement of 48 hours may be too short. As an example, new, material information may arise that requires an adviser or fund to work with law enforcement, and law enforcement may want the fund or adviser to postpone disclosing certain information.</p> <p>The requirement of ongoing reporting about significant cybersecurity incidents is not present in other cybersecurity laws and regulations such as the New York Department of Financial Services Cybersecurity Rule (23 NYCRR 500) and the National Association of Insurance</p>

		Commissioners model cybersecurity law. We believe that the requirement for entities to retain documentation of cybersecurity events and remediation, combined with the Commission's right to access such documentation, is a sufficient control for ensuring that significant cybersecurity events are adequately resolved.
45	Is IARD the appropriate system for investment advisers to file Form ADV-C with the Commission? Instead of expanding the IARD system to receive Form ADV-C filings, should the Commission utilize some other system, such as the Electronic Data Gathering, Analysis, and Retrieval System (EDGAR)? If so, please explain. What would be the comparative advantages and disadvantages and costs and benefits of utilizing a system other than IARD? What other issues, if any, should the Commission consider in connection with electronic filing?	Regardless of the platform used, advisers should have the option to report certain initial information by phone, particularly in cases where a company's IT networks have been impacted.
46	Should we include any additional items or eliminate any of the items that we have proposed to include in Form ADV-C? For example, should advisers be required to disclose any technical information (e.g., about specific information systems, particular vulnerabilities exploited, or methods of exploitation) about significant cybersecurity incidents? Should we modify any of the proposed items? If so, how and why?	<p>Detailed information about the information systems impacted and vulnerabilities exploited should not be required as part of the report unless the form will be kept confidential and can be protected from public disclosure, including additional targeted attacks by bad actors. Particularly if the information will be publicly available, there is a risk that previously unknown or little-known exploits will become more widely known and used. In addition, some of the details listed may be subject to attorney-client privilege depending on how a company's investigation is structured.</p> <p>Additionally cyber insurance information should be eliminated as it can be used by bad actors to target companies in ransomware.</p>
47	Should Form ADV-C be confidential, as proposed? Alternatively, should we require public disclosure of some, or all of the information included in Form ADV-C?	<p>Yes, the information submitted as part of Form ADV-C should be confidential.</p> <p>We believe that requiring public disclosure of some or all of the information included in Form ADV-C would be counterproductive. It might lead to unnecessary confusion on the part of individuals whose information may have been compromised.</p>
48	Will the proposed cybersecurity disclosures in Item 20 of Form ADV Part 2A be helpful for clients and investors? Are there additional cybersecurity disclosures we should consider adding to Item 20? Should we modify or delete any of the proposed cybersecurity disclosures?	The proposed disclosures in Item 20 are similar to the requirements of public companies, and this would provide sufficient information to sophisticated investors. Additional disclosures should not be added.
49	Does the definition of significant adviser cybersecurity incident allow advisers to inform investors of cybersecurity risks arising from the incident while protecting the adviser and its clients from threat actors who might use that information for the current or future attacks? Does this definition allow for disclosures relevant to investors	<p>No, including in the definition impact of a single client will likely desensitize investors.</p> <p>Yes, the proposed definition of significant cybersecurity incident strikes a balance of appropriately informing investors without potentially requiring overreporting that would desensitize investors.</p>

	without providing so much information as to be desensitizing? Why or why not?	
50	Do the required disclosures provide investors with prompt access to important information that they need in connection with the decision to engage, or continue to engage, an adviser? Why or why not?	<p>The proposed disclosures provide too much information, which is more than necessary and sufficient for sophisticated investors to make determinations related to their investments or to raise additional questions with the adviser or fund.</p> <p>Yes, the proposed disclosures provide sufficient information that the sophisticated investors working with advisers and funds need to make determinations related to their investments or to raise additional questions with the adviser or fund.</p>
51	We propose to require advisers to update their cybersecurity disclosures in Item 20 promptly to the extent the disclosures become materially inaccurate. Do commenters agree that the lack of disclosure regarding certain cybersecurity risks and cybersecurity incidents would render an adviser's brochure materially inaccurate? Should we only require advisers to update their cybersecurity disclosures on an annual basis (rather than an ongoing basis, as proposed)?	If not on an annual basis, quarterly and not ongoing would be preferable and still should only be required to update Item 20 to the extent the disclosures become materially inaccurate, as described.
52	We propose to require advisers to deliver brochure amendments to existing clients if the adviser adds disclosure of an event, or materially revises information already disclosed about an event, that involves a cybersecurity incident in response to proposed Item 20. Is this delivery requirement appropriate? Why or why not? Are there other delivery or client-notification requirements that we should consider for advisers when updates to their cyber security disclosures are made?	
53	Should advisers also be specifically required to disclose if there has <i>not</i> been a significant cybersecurity incident in its last two fiscal years? Would this disclosure assist investors in their investment decision-making? Why or why not?	<p>Advisers should not be required to disclose if there has not been a significant cybersecurity incident in its last two fiscal years. This would impose additional reporting obligations even though the material event has not occurred.</p> <p>Instead, this should be a permissive option for advisers.</p>
54	Should the rule include a requirement to disclose whether a significant adviser cybersecurity incident is currently affecting the adviser? Why or why not? Is the look-back period of two fiscal years appropriate? Why or why not?	The proposed rule relating to delivery of interim brochure amendments should not include current cybersecurity incidents. Advisers should have sufficient time to respond to and manage risk relating to an ongoing cybersecurity incident before being required to make the disclosure in its interim brochure.
55	Should there be a prospectus disclosure requirement of significant fund cybersecurity incidents for all registered funds? If some types of funds should be exempt, have different disclosure requirements, or not be subject to the proposed structured data requirement, which and why?	
56	Will the proposed cybersecurity disclosures be helpful for shareholders and potential shareholders? Are there additional cybersecurity disclosures we should add? Should	The current proposed disclosures will be helpful for shareholders and potential shareholders.

	we modify or delete any of the proposed cybersecurity disclosures?	Additional cybersecurity disclosures should not be necessary.
57	Does the definition of significant fund cybersecurity incident allow funds to inform investors of cybersecurity risks arising from the incident while protecting the fund from threat actors who might use that information for the current or future attacks? Does this definition allow for disclosures relevant to investors without providing so much information as to be desensitizing? Why or why not?	<p>No, including in the definition impact of a single client will likely desensitize investors.</p> <p>Yes, the proposed definition of significant cybersecurity incident strikes a balance of appropriately informing investors without potentially requiring overreporting that would desensitize investors.</p> <p>We believe that the definition of significant fund cybersecurity incident is too broad. The definition includes “unauthorized access or use of fund information, where the unauthorized access or use of such information results in substantial harm . . . to an investor whose information was accessed.” If the goal is to inform investors of risks, the compromise of one account is not the correct standard to use. It will result in the reporting of numerous small events, which will not provide meaningful information about the state of security at a fund and most likely would lead to investors failing to pay attention to the disclosures.</p>
58	Should the rule include a requirement to disclose whether a significant fund cybersecurity incident is currently affecting the fund as proposed? Why or why not? How often should cybersecurity disclosure be updated? Is the lookback period of two fiscal years appropriate? Why or why not?	Apart from disclosure to the Commission, funds should not be required to otherwise disclose a significant cybersecurity incident that is currently affecting the fund. Such a real-time disclosure requirement risks diverting incident response resources to the disclosure and communications process. In addition, information disclosed initially may quickly become outdated as investigations continue, requiring funds to continually update the disclosure(s).
59	Should the rule include an instruction about significant fund cybersecurity incidents that may have occurred in the fund’s last two fiscal years but was discovered later? Why or why not? Should the Commission provide more specific guidance or requirements on when a fund should update its disclosure to provide information about a significant fund cybersecurity incident? Should the timing or information about a significant cybersecurity incident for updated disclosure match the prompt reporting requirement for advisers on Form ADV-C? Why or why not?	<p>Because the current proposed rule focuses on when a cybersecurity incident “occurred,” the proposed rule would capture situations where a significant fund cybersecurity incident occurred in the fund’s past two fiscal years subject to reporting requirements but was not discovered until later.</p> <p>Funds should be provided flexibility to update disclosures based on their determination of the materiality of the circumstances.</p> <p>The timing of disclosures should be balanced against potential security risks or the risk of creating undue investor panic.</p>
60	Are there other delivery or shareholder-notification requirements that we should consider for funds when updates to their cybersecurity disclosures are made? For example, should there be an alternate website disclosure regime, similar to how proxy voting records may be disclosed, for cybersecurity incidents? Why or why not? Or alternatively or additionally, should information about	Website disclosures are easily accessible, updateable, and can be used to quickly reach a large number of individuals. As such, the website disclosure regime as an option should be maintained and extended for cyber incidents. To the extent that additional channels of disclosure may be required, such requirements should be flexible enough to permit funds to refer back to the website disclosure.

	significant fund cybersecurity incidents be included in funds' annual reports to shareholders, filed on Form N-CSR, or reported on Form N-CEN?	
61	Should funds also be specifically required to disclose if there has not been a significant cybersecurity incident in its last two fiscal years? Would this disclosure assist investors in their investment decision-making? Why or why not?	Funds should not be required to disclose if there has not been a significant cybersecurity incident in its last two fiscal years. This would impose additional reporting obligations even though the material event has not occurred. Instead, this should be a permissive option for funds.
62	Should the Commission provide more specific guidance or requirements on when and what cybersecurity risk funds should disclose, including when cybersecurity risk would be considered a principal risk factor? Why or why not?	At this stage, the Commission should not provide additional requirements on when and what cybersecurity risks funds should disclose. Funds should be able to address the risks that are unique to their businesses. However, the Commission should consider publishing guidance that will aid funds in making those determinations.
63	Should we require all funds to tag significant fund cybersecurity incidents in Inline XBRL, as proposed? Why or why not?	
64	Should we require funds to use a different structured data language to tag significant fund cybersecurity incident disclosures? If so, what structured data language should we require?	