CRINDATA™

www.CRINDATA.com

April 11, 2022

Secretary
U.S. Securities and Exchange Commission
100 F Street NE,
Washington, DC 20549–1090

Submitted through the SEC's website portal
To rule-comments@sec.gov,
Subject: File Number S7–04–22

Comment Letter to Proposed Rule

Cybersecurity Risk Management

for Investment Advisers, Registered Investment Companies, and Business Development Companies

SEC RINs: 3235-AL61 ; 3235-AL42
File Number S7–04–22

Dear Sir or Madam:

We write in support of the purpose and the direction of, while also providing specific comments and further recommendations with respect to, the abovementioned Proposed rulemakings (i) to require registered investment advisers and investment companies to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks; and (ii) report significant cybersecurity incidents affecting the adviser; and other requirements, as published in 87 Federal Register 13,524, dated March 9, 2022 (the "**Proposed Rules**") by the Securities and Exchange Commission, for which comments are requested by April 11, 2022.

I. Preliminary Comment and Focus in Support of the Proposed Rules

We write in overall support of the Proposed Rules, with more detailed comments on specific aspects which could make the final rules more efficient and effective for the SEC and industry in support of the SEC's objectives. Requiring cybersecurity policies and procedures and cybersecurity incident reporting are reasonable in light of the SEC's goals in promoting investor protection and in reducing systemic risk.

While cybersecurity risks are relevant to advisers and funds, they are not in any way unique to them. Rather, the cybersecurity risks are one component of operational risks that could lead to disruption at advisers or funds, as well as exposure of personal information. Hence, cybersecurity reporting for funds and advisers should be required as part of broader operational event reporting; and harmonized with other increasing governmental incident reporting rules.

A. Relation among risk mitigation policies, and incident reporting

We also support the SEC proposing the combination of distinct, yet complementary elements of requiring:

- the adoption of policies and procedures on the basis of a risk assessment
- reporting of significant incidents; and
- related recordkeeping requirements.

These together are recognized elements of many compliance requirements implementing policy objectives for the broader financial services sector. The disclosures of risks and past incidents are somewhat different.

For current, high-level purposes, we wish to focus on the different temporal nature of these elements of a broader compliance program for the Proposed Rules:

- Policies and procedures are *proactive, ex ante* measures aimed at increasing risk awareness, and where possible risk mitigation. It must be noted, however, that while cybersecurity risks may be mitigated through a reasonably designed and implemented program, they cannot be totally eliminated.
- Reporting of incidents is by definition *ex post*, and preparing a structured way for such reporting recognizes that cybersecurity risks may be mitigated but cannot be eliminated. **Timely reporting of incidents is critical to allow the SEC to identify and where possible to act with respect to potential systemic risks.** Moreover, prompt initial reporting of operational incidents or events may require reporting before the cause is identified, be it *either* due to an "unauthorized occurrence" and hence falling under the proposed cybersecurity incident definition, *or* some other source of operational failure (e.g., other human error, coding error, hardware failure or natural cause).
- Recordkeeping requirements are good corporate practices generally, and support both an entity and its oversight and supervisory authorities to review over time whether a program appears reasonably designed and implemented to mitigate risks and meet regulatory requirements.
- Disclosures to clients and investors are consistent with investor protection and fiduciary duties; past incidents provide some indication of the reasonableness or effectiveness of an entity's risk mitigation measures, but are not conclusive. An analogy can be made to the principles in the securities industry and related disclosures that risk-taking is correlated with returns (and that additional controls or risk mitigation measures come at costs); as well as that historical return (or historical incidents) are not necessarily indicative of future returns (or incidents).

This comment letter will focus most on elements relevant to the second arrowpoint above with respect to the timely and effective reporting of incidents for the purpose of systemic risk mitigation. **It would be prudent and consistent with the SEC's systemic risk mitigation goals not only to adopt cybersecurity risk mitigation program requirements, but also a**

broader definition of operations events and incidents reporting than under the proposed more narrow definition of cybersecurity incidents.

B. Reporting disclosure of operational incidents, versus more narrow disclosure requirements with respect to unauthorized access to personal information

We support the goals of the SEC in proposing **incident reporting to the Commission**, not only to address individual incidents, but also to address potential systemic risks. As stated in the proposal,

> This reporting would help us in our efforts to protect investors in connection with cybersecurity incidents by providing prompt notice of these incidents. We believe this proposed reporting would allow the Commission and its staff to understand the nature and extent of a particular cybersecurity incident and the firm's response to the incident. As stated above, this reporting would not only help the Commission monitor and evaluate the effects of the cybersecurity incident on an adviser and its clients or a fund and its investors, but also assess the potential systemic risks affecting financial markets more broadly. For example, these reports could assist the Commission in identifying patterns and trends across registrants, including widespread cybersecurity incidents affecting multiple advisers and funds.[1]

Throughout this comment letter, we note that the SEC's goals of assessing potential systemic risks more broadly, would be better served by requiring incident reporting with respect to operations disruptions. Prompt reporting will further the SEC's ability to more quickly act in light of potential systemic risks, and a reporting adviser or fund can be expected in many instances to more quickly be able to identify the ***effect*** of operational disruption than to discern the ***cause*** as a cybersecurity incident of unauthorized access.

We also support the general direction of a separate proposal of the SEC that there should be some **public disclosure of cybersecurity events** to allow assessments by clients and investors. This comment letter does not provide detailed observations on those aspects of the Proposed Rules. We nonetheless note that such transparency and reporting, if adopted along the lines of the proposal, are most relevant to the ***effect*** of a given incident and an understanding of the risks, moreso than a specific cause.

We respectfully suggest that our comments are intended to promote the SEC's purposes and goals, and where practical to focus on the most relevant effects of incidents and promoting early ability of individual affected entities, as well as the SEC, to address them.

[1] 87 Fed. Reg, at 13,536.

II. Summary of Conclusion and General Comments

We write in overall support of the proposed rules. This comment letter will provide more detailed comments on the following aspects, which are meant to help the SEC craft rules that will more efficiently and effectively support its objectives.

Requiring cybersecurity policies and procedures and cybersecurity incident reporting are reasonable in light of the SEC's goals in promoting investor protection and in reducing systemic risk.

Cybersecurity is one of the greatest risks facing not only investment advisers and funds, but our modern economy more generally. That being said, cybersecurity is (i) one component of the broader category of operational risk (i.e., as opposed to more traditional financial sector risks such as credit, market or liquidity risks); and (ii) cybersecurity risks are driven not only by growing cybersecurity threats, but by the exposure created by the increasing reliance on IT and communications, AND, (iii) increasing reliance on third-party service providers including subcontractors. Taking all of the foregoing into consideration, the cybersecurity risk management policies and procedures, and cybersecurity incident reportings should:

- Continue to be part of an overall operational risk management framework and resilience from disruptions leading to a similar negative effect even if not caused by a defined "cybersecurity" incident involving unauthorized access; too narrow or prescriptive cybersecurity rules will lead to a check-the-box approach not consistent with the broader goals and purposes
- Must take into consideration and therefore integrate practices for third party service provider oversight, not just limited to "named service providers" which comprise only a portion of the cybersecurity and operational risk exposures to advisers and funds
    - Include further expectations for understanding and due diligence of further sub-contracting and further service provider dependency chains
- The requirements for prompt, initial incident reporting should be expanded to apply to operations events beyond just what are initially identified as cybersecurity incidents; otherwise, the SEC will receive an underreporting of the desired incident information potentially indicative of systemic risks beyond the reporting entity
- To be effective, entities directly regulated by the SEC and subject to incident reporting requirements will need to obtain, at least as contractually agreed, timely incident notifications from their service providers, including through subcontractor chains
- Continue to seek harmonization with reporting of cybersecurity and operational risk incident reporting increasing mandated by the SEC and other government authorities for parties other than advisers or funds; especially taking into consideration that many relevant third party service providers have broader support relationships than just for advisers and funds
- Support the ability of advisers and funds, including smaller entities to rely on industry shared solutions and specialized service providers, both for their oversight of risks—in

particular reliance on third party service providers, and in incident reporting. Shared solutions are appropriate and can be viable, effective, and efficient not only at the level of due diligence and risk assessment, but throughout the risk management life cycle, and in reporting among counterparts, or on behalf of regulated entities directly to the SEC or other regulator.

III. About the Commenters

This comment is submitted by **CRINDATA**, LLC, (www.CRINDATA.com) which offers solutions to financial institutions for managing operational risk in their reliance on third party service providers. Underlying many aspects of the Proposed Amendments is the structural framework under which an adviser and a fund rely on a range of distinct service providers in order to operate.

CRINDATA offers unique cloud-based solutions to financial institutions who must pro-actively manage their critical third-party relationships (including their indirect relationships with subcontractors) and must prepare for and mitigate business disruptions management and cybersecurity events originating anywhere in the chain of service providers and subcontractors. Concurrently, CRINDATA helps third party service providers like cloud providers, custodians, core systems, payments providers, and transaction motoring solutions, by substantially simplifying the due diligence interactions with financial service companies and by providing a compliant, common platform and communications to manage business disruptions and cybersecurity events when they occur. The platform serves needs across multiple jurisdictions applying similar, evolving risk management principles. The authors of this comment letter are CRINDATA's co-founders, Mark Stetler and James H. Freis, Jr. Mr. Freis as the primary author draws upon his experience working together with the SEC while serving as Director of the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), and in a range of other roles on behalf of government and private sector groups including SEC-regulated entities.

IV. Trend towards operational incident reporting and opportunity to promote further harmonization

While cybersecurity risks are relevant to advisers and funds, they are not in any way unique to them. Rather, the cybersecurity risks are one component of operational risks that could lead to disruption at advisers or funds, as well as exposure of personal information. Hence, cybersecurity reporting for funds and advisers should be required as part of broader operational event reporting; and harmonized with other increasing governmental incident reporting rules.

Operational events, including cybersecurity incidents, can have both investor protection implications in terms of the potential for exposure of personal information. Operational events, including cybersecurity incidents, can also have systemic risk implications, to a limited extent if impacting a discrete adviser or fund, but moreso if impacting a critical third party service provider to multiple advisers, funds, or broader actors within the financial services industry.

Prudent regulations to manage and address these risks have the potential for benefits that outweigh the costs to imposing them.

As to relevant operational risks being broader than cybersecurity incidents, while the SEC should move forward with the Proposed Rules with some amendments, such efforts should be pursued in the broader context of broader operational risk management efforts, including reporting of operational risk incidents beyond cybersecurity incidents. Such broader reporting would be similar to the operational incident reporting that would be required under the SEC's proposed rulemaking to amend Form PF, the confidential reporting form for certain SEC-registered investment advisers to private funds to require current reporting upon the occurrence of key events and other requirements for advisers to certain types of funds, as published in 87 Federal Register 9106, dated February 17, 2022, for which CRINDATA filed a comment letter on March 21, 2022. A copy of CRINDATA's earlier comment letter is attached and hereby incorporated by reference, as many of CRINDATA's comments are similar in their applicability here to advisers and funds, as well as there to private funds. One element that should be understood across the two comment letters is that while we believe the SEC should require the reporting of operations events beyond cybersecurity incidents, we do not believe that such reporting should be incorporated within a broader informational report such as directly on Form ADV, or the proposed amendments to Form PF. Rather, preferable are separate and complementary reporting of operational events including cybersecurity incidents along the lines of the confidential reporting proposed in Form ADV-C with the specific additional observations in this comment letter. Specifically, the SEC could adopt a separate yet analogous reporting format for operational events beyond but including cybersecurity incidents, that would apply to advisers, funds, and private funds (which would also address that some advisers support both public and private funds). A more consistent reporting across advisers and fund types would be easier for the industry, and its service providers to implement, while also better supporting the SEC's systemic risk interests in helping identify risks that might affect broader parts of the industry.

A significant portion of SEC-registered investment advisers are also registered as broker-dealers, while other advisers traditionally have a related person that is a broker-dealer; additionally, a large portion of investment adviser representatives are also registered representatives of broker-dealers. These inter-relationships also are reflected in a large portion of shared reliance on common outsourcings and third party service providers, which in turn means interconnected (and potentially indicative of systemic) risks in the areas of the current rule's concerns with respect to cybersecurity, incident reporting, and broader operational risk management.

Reporting of broader operational events including cybersecurity incidents also would be consistent with other SEC initiatives. Reference is made to the notification requirements under the SEC's Regulation Systems Compliance and Integrity (Regulation SCI) which was developed, *inter alia*, in light of the dependency of the securities markets on evolving technology and vulnerabilities to outages including in connection with cyberattacks.[2] Notably, a covered entity is

[2] See SEC Final Rule, Systems Compliance and Integrity, 79 Fed. Reg. 72,252 (December 5, 2014), as implemented in particular in 17 CFR § 242.1002--.1007, available at 2014-27767.pdf (govinfo.gov). The primary author of this

required both to make an "immediate" notification to its Federal regulator of an incident; followed within 24 hours on a "good faith, best efforts basis" by a notification of event and assessment to the extent available at that time; and at later times more detailed impact assessments.[3] More recently, the SEC has published for comment a proposed rule that would enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies.[4]

Particularly instructive for the SEC, and essential for efforts of the Financial Stability Oversight Council to monitor potential systemic risks, should be the new reporting requirement by the U.S. Federal Banking Agencies – the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation.[5] That final rule will require a banking organization to notify its primary Federal regulator of any ''computer-security incident'' that rises to the level of a ''notification incident,'' as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. The final rule also requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours. Regulated entities as well as their service providers are currently preparing for implementation of that new rule with compliance date of May 1, 2022. Notably, the Federal Banking Agencies require incident reporting broader than cybersecurity incidents and more akin to the SEC policy's concern underlying the proposed operations events reporting on funds PF. This is made clear in the background explanation of the final rule of the Federal Banking Agencies, but is equally relevant to the SEC's policy objectives underlying the Proposed Rules for advisers and funds: "Computer-security incidents can result from destructive malware or malicious software (cyberattacks), as well as non-malicious failure of hardware and software, personnel errors, and other causes."[6]

The trend to require additional reporting of incidents or operations events will only continue. After the publication of the Proposed Rules, on March 15, 2022 the President signed into law the Consolidated Appropriations Act, 2022.[7] That appropriations law also contains the ''Cyber Incident Reporting for Critical Infrastructure Act of 2022" which authorizes rulemaking for incident reporting across a broad range of actors (including components of the financial sector) and calls for coordination with any analogous reporting requirements by other government agencies. Other jurisdictions are following analogous paths to mandate incident reporting. One

comment letter previously had oversight responsibility for the implementation of Regulation SCI by SEC regulated exchanges.

[3] See 17 CFR § 242.1002(b).

[4] See 87 Fed. Reg. 16,590 (March 23, 2022). Comments on that proposed rulemaking may be submitted separately.

[5] See 86 Fed. Reg. 66,424 (November 23, 2021).

[6] See id. at 66,425 (emphasis added).

[7] Public Law No: 117-103 (March 15, 2022).

prominent example is the European Union's proposed Digital Operations Resilience Act (DORA),[8] for which a revised proposal after a round of public consultation is expected soon.

This broader context should be understood as strong support for the policy goal of the SEC requiring additional reporting of relevant operations events including cybersecurity incidents, and in moving forward with additional reporting requirements without delay. That notwithstanding, the broader trend towards such reporting also emphasizes the need for the SEC to take an approach more consistent across the SEC's own various new reporting proposals. The broader trend also suggests that the SEC should attempt to act increasingly consistently with other governmental authorities for which there is not a differing policy goal or interest. Many underlying entities impacted by the reporting requirements—in particular third party service providers—support multiple different regulated entities. Analogous goals requiring nonetheless different prescriptive reporting methods, formats, data fields and timing would make more difficult the goals sought by the SEC and a range of other government entities to obtain and be able to share information about incidents and potential indicators of systemic risks; it would also raise the complexity and costs, and make more difficult for the regulated industry to timely notify reportable incidents. Again, a relevant consideration is that the parties involved in reportable incidents often will include broader IT service providers and sub-contractors that are not specifically focused on the Proposed Rules at issue here for advisers and funds; rather an operations event or incident affecting an entity such as a cloud services provider could in the future trigger directly or indirectly through affected chains of customers, reporting to a broad range of government entities.

Part of that harmonization, increased effectiveness towards the systemic risk mitigation goals of the SEC and other governmental authorities, and achieving these goals in a more efficient, effective, and less costly way for regulated entities including advisers and funds would be to allow operational risk mitigation information sharing and incident reporting on behalf of those regulated entities by specialized service providers acting on behalf of the regulated entities. Thus, the SEC should consider allowing incident reporting either in different formats, or in parallel to its existing portal for reporting by advisers.

V. Specific Comments and Responses to Request for Comment Questions

The following responds in more detail to some of the specific items on which comments were requested in connection with the proposed rules.

8. 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 the proposed terms too broad or too narrow? Are there other terms that we should define?

[8] See Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, available at EUR-Lex - 52020PC0595 - EN - EUR-Lex (europa.eu).

While the definitions of "cybersecurity threat" and related terms appear largely sufficient for the purpose of the proposal to adopt cybersecurity policies and procedures, the term "cybersecurity incident" is too narrow for the incident reporting requirement. Rather, the SEC should introduce a broader definition of reportable operations events or incidents including cybersecurity-related incidents.

The cybersecurity incident reporting under proposed § 275.204-6 incorporates by reference the definition of "cybersecurity incident" of proposed rule 206(4)-9:

> Cybersecurity incident means an unauthorized occurrence on or conducted through an adviser's information systems that jeopardizes the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.

Thus, a reportable incident would be one that involves an "unauthorized occurrence." In practice, many "unauthorized occurrences" such as malware or trojans may go undetected for some time after being introduced, or, it may take time for the source of a disruption event to be detected and identified as to whether it was caused by an "unauthorized occurrence." Various other aspects of the definitions and the preamble to the Proposed Rules make clear that the systemic risk mitigation purpose of the proposed incident reporting should not be limited to the cybersecurity *cause*, but rather that the concerns are with respect to the *effects* an incident could have on "confidentiality, integrity, or availability." Thus, the SEC, should wish reporting to include disruptions which appear likely to affect "confidentiality, integrity, or availability."

It is suggested that the SEC adopt for the purposes of a new incident reporting requirement a definition of a reportable Operations Event that would be the same as that which it adopts in connection with its pending proposal, mentioned above, for reporting by private funds: that the reporting fund or adviser experiences a significant disruption or degradation of the reporting entity's key operations, whether as a result of an event at a service provider to the reporting fund, the reporting fund, or the adviser.[9] It would be more efficient to adopt this broader reporting requirement sooner, rather than first the more narrow reporting based on the definition of cybersecurity incident, including because of the overlap of advisers to public as well as private funds, and the broader trend toward incident reporting and implications for common service providers mentioned above.

In conclusion, whatever the final definition of a reportable incident, it is in the interest of the SEC and its goals of identifying potential systemic risks to have more operations incidents

[9] See 87 Fed. Reg. at 9230. See also id. at 9115, n.40, in which the SEC itself recognized the relation among these proposals. ("We recognize that the SEC currently does not require registered investment advisers and registered investment companies to report operational events. We are also considering recommending that the Commission propose rules to enhance fund and investment adviser disclosures and governance relating to cybersecurity risks. *See* Securities and Exchange Commission, Agency Rule List (Fall 2021), *available at* Agency Rule List—Fall 2021 (*reginfo.gov*).").

reported, rather than risking more narrow reporting based on whether the reporting entity has timely identified a more narrow causation involving an "unauthorized occurrence."

9. 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?

Measures with respect to oversight of, and requiring incident reporting from, third party service providers, as well as their subcontractors, are an evolving best practice. They are also essential to effective risk management in light of the increasing reliance on third party service providers.[10]

12. Other than what is required to be reported under proposed rule 204-6, should we require any specific measures within an adviser's policies and procedures with respect to cybersecurity incident response and recovery?

While not wanting to be overly prescriptive in the rule itself, it is nonetheless prudent to expect that with respect to cybersecurity incidents that turn out to be material, that there be a fuller report of incident that would better be an attachment or further documentation in support of the theme of proposed questions 12 to 14 on proposed Form ADV-C. See also the response to question 46.

13. Should we require that advisers and funds respond to cybersecurity incidents within a specific timeframe? If so, what would be an appropriate timeframe?

A "response" to a cybersecurity incident may differ in each case based on what is understood with respect to the incident, what business continuity plans are available, and what if any action can be taken. This it is difficult to "require that advisers and funds respond." The most important and consistent aspect of any response is to require prompt incident reporting.

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?

Advisers and funds should assess the compliance of all service providers for which a disruption of services – whether due to a cybersecurity-related issue or other cause – would have a significant impact on the operations of the adviser or fund. The above language appears to be more skewed to the one policy aspect of unauthorized access to fund information, rather than the SEC's broader concern of disruption to operations (for example, a DDOS attack could lead to an operational disruption without necessarily exposing adviser or fund information).

[10] For support for the proposition of growing risks in connection with reliance on third party service providers, see the preamble to the Proposed Rules, 87 Fed. Reg. at 13,530; see also the SEC's proposed cybersecurity reporting for public companies describing risks in connection with third party service providers, 87 Fed. Reg. at 16,592-93.

Any fund should have a risk assessment as to its dependencies upon service providers. This goes beyond "named service providers" as described earlier in the preamble and which definition should not be applied for the purpose of service provider compliance assessment.

> Similarly, 17 CFR 270.38a-1 ("Investment Company compliance rule") requires funds to adopt and implement written policies and procedures reasonably designed to prevent violations of the Federal securities laws by the fund, including policies and procedures that provide for the oversight of compliance by each investment adviser, principal underwriter, administrator, and transfer agent of the fund (**"named service providers"**). We understand that funds take into account the specific risks they face, often including any specific cybersecurity risks, when developing their compliance policies and procedures under the Investment Company compliance rule.[11]

We agree with the SEC's analysis elsewhere in connection with the Proposed Rules.

> Narrowing the scope of the types of service providers affected by the proposal could lower costs for registrants, especially smaller registrants who rely on generic service providers and would have difficulty effecting changes in contractual terms with such service providers. However, given that in the current technological context, cybersecurity risk exposure of registrants is unlikely to be limited to (or even concentrated in) certain named service providers, narrowing the scope of service providers would likely lead to lower costs only insofar as it reduces effectiveness of the regulation. In other words, absent a written contractual arrangement with a service provider relating to the provider's cybersecurity practices, it is unlikely that registrants could satisfy their overarching obligations under the proposed rules.
>
> Alternatively, maintaining the proposed scope but only requiring a standard, recognized, certification in lieu of a written contract could also lead to cost savings for registrants. However, we preliminarily believe that it would be difficult to prescribe a set of characteristics for such a "standard" certification that would sufficiently address the varied types of advisers and funds and their respective service providers.[12]

We propose that narrowing the types of service providers should be based on a risk assessment of the materiality of the service provider to the operations of the adviser or fund (operations generally and not only with respect to cybersecurity risks). Such an approach would be preferable to either of the options considered by the SEC in the foregoing excerpt, of using the overly narrow definition of named service providers, or somewhat blindly relying on a certification without which no one would use the service provider, which would take time to implement, and would not necessarily address the different needs or risks for various advisers or funds.

[11] 87 Fed. Reg. at 13,526 (footnote omitted).
[12] 87 Fed. Reg. at 13,557 (footnotes omitted).

Such risk assessment should also take into consideration whether the third party has critical dependencies on underlying sub-contractors or other service providers, in which case such underlying parties should also be included in the risk assessment.

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?

Due diligence on service providers, the disruption of which services could have a material impact on the operations of an adviser or fund, including further subcontractors ("fourth parties"), is the primary way to mitigate operational risks (including potential cybersecurity incidents). Oversight and monitoring must be continuous, not only at the time of entering into a service party relationship.

Once a security incident occurs, it is not always possible to prevent the cybersecurity incident transferring from a service provider or a fourth party to an adviser. Some types of cybersecurity incident, such as intrusion into a service provider IT systems might be avoid spreading to an adviser's systems through various firewalls and detection systems. But "transferring" is not the only risk; an operational disruption at a third or fourth party, if material, might prevent or have negative consequences for the operation of an adviser or fund.

Please also see the discussion on page 2 of this comment letter regarding the interrelationship of the various components of the Proposed Rules, and their different temporal nature.

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?

One of the most important provisions for effective risk assessment and oversight of service providers for operational risk management (including, but not limited to cybersecurity risks), is for the adviser or fund to have transparency with respect to material dependencies of the service provider on further subcontractors or other service providers to the service providers (also sometimes referred referred to as fourth parties). Because, by definition, there is no contractual privity between the adviser or fund and a "fourth party," there is a reliance on the third party to oversee and provide information with respect to the fourth party, including changes to the use of different material fourth parties.

As related to incident reporting, if a significant incident impacts a fourth party, there must be not only contractual agreements in place, but also structured reporting mechanisms, to allow the reporting of relevant incident information:

- from the fourth party (or further chain of subcontractors up the chain) to the third party
- from the third party to the adviser or fund
- from the regulated adviser or fund to the SEC as regulator, as well as any other applicable authority.

Understanding and assessing risks, and getting notification of incidents in timely fashion, from fourth parties or other third party service provider chains are among the greatest challenges faced throughout the financial services industry. These challenges cannot be overcome individually by each adviser or fund, which generally do not have the comparative market size to change practices of service providers. A shared solution or type of utility serving multiple advisers, funds, and other financial industry participants lends itself well to sharing costs and more efficiently leveraging risk management solutions. CRINDATA is a provider of one such shared solution.

It is suggested that the SEC not be prescriptive, but rather raise awareness such as in guidance on best practices about the importance of understanding exposure and addressing information needs on third party providers and their subcontractors or fourth parties. Analogous approaches have been expected for years by the Federal Banking Agencies, and revisions to guidance on oversight of outsourcing to third parties have recently been published for public consultation.[13]

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?

Review of service providers' insurance policies, including the extent of coverage for the benefit of the contracting entity as additional insured, is a common aspect of overall due diligence on service providers, including exposure to operational risk generally (if not necessarily cybersecurity specifically). That is a proactive measure. Ex post review of insurance policy coverage might be relevant for some types of losses, including possibly shifting some monetary losses from a contracting entity to the service provider. Insurance cannot help other aspects of losses from incidents, including data exposure or reputational impact.

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?

Review of service providers' cybersecurity policies, and in particular whether a service provider has an independent review or certification, such as ISO 27001 Information Security Management

[13] See Proposed Interagency Guidance as published in 86 Federal Register 38,183 (July 19, 2021).

System, is a common aspect of overall due diligence on service providers, including exposure to operational risk generally.

As stated above in response to question 17, it is more challenging to obtain relevant information with respect to further underlying subcontractors or service providers (fourth parties).

There is nonetheless limited ability beyond identifying service providers with certain audits, reviews or certifications, to assess the information that is provided in terms of the effectiveness of implementation.

26. 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?

Taking as an assumption that cybersecurity generally is a significant risk to an adviser or fund (something that would in any case be part of the proposed disclosures if adopted), then it would be appropriate for a board to approve a cybersecurity policy. This should be considered as part of the decision of risk tolerance of the board, and similar to the approach to approving other significant policies. It would generally not be expected that a board (and in particular independent directors) review and approve more detailed operational procedures, which should be left to management and be updated or changed whenever necessary.

27. 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?

Fund boards should not be required to approve the cybersecurity policies and procedures of service providers – these documents are not under the control of the board and, especially for a service provider serving multiple unrelated funds, it should not be assumed that the board has any ability to influence or change the content of such policies and procedures.

A board should consider relevant aspects of the costs, benefits, and risks (of which cybersecurity is only one) as part of a broader operational risk decision with respect to the most important service provider relationships. The board would not generally be expected to conduct detailed reviews of all relevant underlying policies and procedures, but could reasonably rely on review and summary information provided by management, the investment adviser, or third party experts.

28. 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?

A board, or designated subcomponent, should have oversight, understand, and be comfortable with the risk assessments of service providers. Banking regulators require the board to approve material outsourcings to service providers.

29. Should the Commission require boards to base their approval of cybersecurity policies and procedures on any particular finding, for example, that 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?

The standard should be that policies meet the regulatory requirement, and are consistent with the individual entity's risk assessment and risk tolerance of the board. It would not seem prudent to impose a standard for board approval solely with respect to cybersecurity singled out from oversight of other material classes of risk for the entity.

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?

Annual review by the board of a report is prudent and consistent with practices for other material risks to the entity. Other items that would be expected to come before the board are findings from an audit or review suggesting deficiencies; as well as material incidents having a negative impact on the entity, which should not necessarily wait until an annual reporting cycle.

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?

See response to question 26.

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?

We strongly support the SEC requirement that advisers report significant security incidents of the adviser and covered clients with the Commission. As stated throughout this comment letter, we believe this would support both investor protection and potential systemic risk mitigation goals. We believe that reporting should also apply to each of private funds and BDCs, as detailed in our comment letter in response to the proposed operations events reporting requirements on Form PF, which comment letter is mentioned above, attached and incorporated by reference.

As described elsewhere in this comment letter and that comment letter with respect to proposed changes to Form PF, we believe that incident reporting should be for broader operations events (not limited to cybersecurity), and in a harmonized way facilitating prompt incident reporting,

not otherwise integrated as part of broader descriptive and financial information on Form ADV or Form PF.

38. At what point would one conclude that there has been a significant adviser cybersecurity incident or significant fund cybersecurity incident? Would it be after some reasonable period of assessment or some other point?

See the response to question 8. As described therein and elsewhere in this comment letter, it might be difficult to assess the cause of a incident, or there could be a time delay in determining that a cybersecurity incident has occurred. In contrast, a disruption in operations at the adviser, or at a material service provider to the adviser or fund, may be observable at an earlier stage, even if the cause (including if a cybersecurity nature) has yet to be determined.

Based on the foregoing, we recommend that it would better serve the SEC's goals to require prompt reporting of operations events or incidents. Future updates or clarifications of the incident at later stages can provide any assessment or determination that the incident is of a cybersecurity or other nature.

39. 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?

This question contain multiple different elements.

With respect to the definition of cybersecurity incident, please see the response to question 8 that we believe for the purpose of prompt incident *reporting to the SEC* it would be better to adopt a broader definition of operational events or incidents. This would not preclude a more narrow *public reporting* of cybersecurity incidents after more thorough assessment.

We believe that the critical operations for advisers and funds should be considered to include the operations mentioned above: investment, trading, valuation, reporting, and risk management, as well as operations necessary to be in compliance with applicable securities laws and regulations. While the activities of advisers and funds are somewhat discrete in comparison to corporate entities generally or certain other financial services companies, it is not necessary that the rule contain an exclusive list, which rather could be suggested through guidance examples, or subject to a determination of materiality to the specific adviser or fund.

With respect to materiality, we do not believe that a quantitative threshold is advisable or practicable. The concept of materiality could nonetheless include the components that an

incident (i) impairs the operation of the fund, including the risk of operational loss; (ii) negatively impairs investors in a fund (for example, an operational incident that prevents withdrawal might not impact the fund itself but nonetheless have a negative liquidity impact on an investor; this is in addition to the investor protection aspects of the Proposed Rules related to disclosures of personal information or transparency to clients and investors with regard to past incidents); and (iii) or causes the failure to meet regulatory requirements such as ongoing risk management monitoring (regardless of whether a risk materializes, this may include the absence of a risk mitigation tool).

We further draw to your attention and incorporate by reference the comments on the proposed amendments to Form PF in the attachment, in particular the response to question number 41.

40. 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?

With respect to "substantial harm", the SEC might wish to review the significant public comments to the Federal Banking Agencies on the new incident reporting requirement referenced *infra* on page 6.

We do not believe the term "inconvenience" is appropriate as a standard, particularly if hoped to provide greater clarity in regulatory expectations.

41. 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?

As reasoned throughout this comment letter, we believe it would be more purposeful to require reporting on the basis of an operational disruption, event, or incident. The initial reporting obligation could be triggered by a materiality determination as described in response to question 39. More objective for service providers would be the failure to provide the services as agreed for a minimum period of time. Since a service availability is a common aspect of a Service Level Agreement, availability is commonly measured and monitored.

The conclusion as to the cause of such an incident, cybersecurity or otherwise, should be reported at such later time when the cause has been assessed. Delaying the reporting for an assessment of cause, or including a "reasonable basis" or similar standard, will not serve the SEC's potential systemic risk mitigation goals requiring prompt notification.

With respect to the amount of time from the trigger to the report being required to be filed with the SEC, we believe it prudent to require at least 24 hours – a time period under Regulation SCI, which nonetheless might suggest a longer period for funds or advisers than for exchanges.

Rather than 48 hours, we recommend harmonization at 36 hours with the new reporting rule of the Federal Banking Agencies described on page 6. Harmonization of reporting timing, together with information sharing among government authorities, would further promote efforts to address systemic risks.

42. 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?

We believe that SEC should allow for specialized service providers to report incidents on behalf of advisers and funds; this would include the essential information provided on proposed Form ADV-C. Such reporting would be more efficient in the event that the operations event or incident happens not at the adviser but rather a service provider to the adviser or fund. A given service provider may have multiple notification requirements to effected entities, which in turn trigger reporting requirements to the SEC or other government authorities.

43. 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 events 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?

As per the comments we filed in response to the proposed changes to Form PF, attached and hereby incorporated by reference, we do not believe that Form PF is an appropriate or useful means to report operations events. We believe that there should be a distinct reporting for operations events (separate from broader identifying and financial information reporting). As distinct from the proposed changes to Form PF for operations event reporting, the proposed for a distinct Form ADV-C approach is preferable. These views reflect practical observations on the expected processes and involved persons for preparing timely reporting, as well as how the report components would be used by the SEC or other recipients where applicable.

44. 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?

We believe that there should be ongoing reporting about unresolved significant cybersecurity incidents. These requirements should continue to be harmonized with other SEC and government authority incident reporting requirements. Suggested timeframes are: within 36 hours (similar to response to question 41) of a significant change of the nature of risks previously reported. This would not require an update to any component of the form generally, but something that would change the assessment of the materiality. Examples would be a change as to whether the incident is ongoing, or if there had been identified a personal information disclosure not previously reported. Separate from such a major change, it is proposed that an update be required 7 days (one week) after the initial incident notification, which timing is under consultation in the European Union with DORA as described on page 8. Thereafter, ongoing incidents or their assessments should be updated on a monthly (30 day) basis, which is consistent with prudent reporting to management of a material incident (in the absence of major changes). Requiring reporting on a two frequent basis, including reporting of minor updates, would potentially distract the reporting entity and draw resources away from more important tasks of risk remediation or future-oriented risk mitigation.

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?

The Commission should allow filing on behalf of advisers and funds by specialized third party service providers. This would be consistent with increasing incident reporting requirements for other regulated entities. The data with respect to incident reporting would not generally be integrated with either Form ADV information, nor with other EDGAR filing information (and should not be made public). Rather, as relevant for potential system risks, it should be available for sharing with other government authorities consistent with the Cyber Incident Reporting for Critical Infrastructure Act of 2022, as noted on page 7 was passed into law after the issuance of this proposal. The SEC should focus on receiving and sharing of information in a way that could be done more easily than making changes to either the IARD or EDGAR systems which are primarily designed for other purposes.

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?

We believe that the SEC goals would best be served by prompt, standardized reporting of the initial operations event or incident. Initial notification of operations events should be factual, and provided in a structured way, which allows the SEC to assess risks to a fund or adviser, as well as potential broader systemic risks. Subsequent updates should be made, including noting when the incident is resolved, and to provide more detail through attachments.

Initial reportable items would consist primarily of the use of unique identifiers for the reporting entity, and indicate where applicable if the incident affected service provider(s), also uniquely identified. Date and time of each of the first occurrence, and discovery are common reporting elements. (Time of day might be relevant, for example if during trading hours.) A third date/time element should be included as to when the event or incident is materially mitigated, or otherwise indicate that it is considered ongoing. Finally, include a concise statement along the lines of proposed Form ADV-C question 11 as to the nature of incident and its possible effect. Broader information as to systems, vulnerabilities, and methods, or in response to proposed questions 12 through 15, will likely only be available at a later time. These are better addressed in an attachment report, rather than in prescribed questions on Form ADV-C.

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?

Initial incident reporting should be confidential and distinct from any aspects that are determined to require later public disclosure, such as whether the incident has resulted in potential exposure of personal information.

VI. Closing

Thank you for the opportunity to comment on the Proposed Rules, and in particular with respect to incident reporting that could better further the SEC's systemic risk goals if incorporated as part of a broader reporting of operations events or incidents.

Sincerely,

CRINDATA, LLC

By: *James H. Freis, Jr.*
James H. Freis, Jr.
Co-Founder & Chairman

Mark Stetler
Mark Stetler
Co-Founder & CEO

Attachment: March 21, 2022 CRINDATA Comment Letter on SEC Proposed Amendments to Form PF

ATTACHMENT

www.CRINDATA.com

March 21, 2022

Secretary
U.S. Securities and Exchange Commission
100 F Street NE,
Washington, DC 20549–1090

Submitted through the SEC's website portal
To rule-comments@sec.gov,
Subject: File Number S7–01–22

Comment Letter to Proposed
Amendments to Form PF
To Require Current Reporting and Amend Reporting Requirements for Large Private Equity Advisers and Large Liquidity Fund Advisers

SEC RIN 3235-AM75
File Number S7–01–22

Dear Sir or Madam:

We write in support of the purpose and the direction of, while also providing specific comments and further recommendations with respect to, the abovementioned Proposed rulemaking to amend Form PF, the confidential reporting form for certain SEC-registered investment advisers to private funds to require current reporting upon the occurrence of key events and other requirements for advisers to certain types of funds, as published in 87 Federal Register 9106, dated February 17, 2022 (the "**Proposed Amendments**") by the Securities and Exchange Commission, for which comments are requested by March 21, 2022.

I. Comments Focused on Proposed "Item H. Operations Event"

This comment letter focuses on the aspects of the Proposed Amendments which would require new and more timely reporting on events affecting the operation of the respective fund or its adviser, in particular in a new Item H regarding an Operations Event. In summary, **while we believe the SEC <u>should</u> require the reporting of this type of operations event, we do <u>not</u> believe that such reporting should be incorporated within the broader proposed amendments to Form PF**. Rather it would better further the policy interests of the SEC to require such incidents to be reported separately. Particularly to identify potential systemic risks, it would be better to align this reporting more with rapidly evolving incident reporting approaches for other SEC regulated entities, other U.S. financial services providers and critical infrastructure components, and under analogous regulatory requirements in other jurisdictions.

II. Summary of Conclusion and General Comments

We write in support of the revisions in the Proposed Guidance. This comment letter will provide more detailed comments on the following aspects.

1. Operations events should be the subject of reporting, including because they can have systemic risk implications.
2. The SEC as well as other financial regulators are working to increase and formalize reporting requirements for incidents and operations events in shorter time periods.
3. Such reporting requirements are part of broader emphasis on such reporting for U.S. critical infrastructure, as well as in foreign jurisdictions.
4. The reporting of operations events is unlike the broader categories of proposed expanded Form PF reporting in terms of content, time relevance, parties involved, etc.; and integration of this information within Form PF would complicate future efforts to harmonize aspects of reporting to better understand and react to potential systemic risks.
5. It is important to continue to emphasize that operations events go beyond cybersecurity incidents.
6. To be effective, entities directly regulated by the SEC and subject to reporting requirements will need to obtain, at least as contractually agreed, timely notifications from their service providers, including through subcontractor chains.
7. Shared solutions are appropriate and can be viable, effective, and efficient not only at the level of due diligence, but throughout the risk management life cycle, and in reporting among counterparts, or on behalf of regulated entities directly to the SEC or other regulator.

III. About the Commenters

This comment is submitted by **CRINDATA**, LLC, (www.CRINDATA.com) which offers solutions to financial institutions for managing operational risk in their reliance on third party service providers. Underlying many aspects of the Proposed Amendments is the structural framework under which a reporting fund must rely on an adviser as well as a range of distinct service providers in order to operate.

CRINDATA offers unique cloud-based solutions to financial institutions who must pro-actively manage their critical third-party relationships (including their indirect relationships with subcontractors) and must prepare for and mitigate business disruptions management and cybersecurity events originating anywhere in the chain of service providers and subcontractors. Concurrently, CRINDATA helps third party service providers like custodians, core systems, payments providers, and transaction motoring solutions, by substantially simplifying the due diligence interactions with financial service companies and by providing a complaint, common platform and communications to manage business disruptions and cybersecurity events when they occur. The platform serves needs across multiple jurisdictions applying similar, evolving risk management principles. The authors of this comment letter are CRINDATA's co-founders, Mark Stetler and James H. Freis, Jr. Mr. Freis as the primary author draws upon his experience working together with the SEC while serving as Director of the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), and in a range of other roles on behalf of government and private sector groups including SEC-regulated entities.

IV. Operations Events – Trend towards incident reporting and opportunity to promote further harmonization; not to include in Form PF

We believe it a very important step for the SEC to require the concept underlying proposed section 5, Item H, for an adviser to report when the adviser or reporting fund experiences a significant disruption or degradation of the reporting fund's key operations, whether as a result of an event at the reporting fund, the adviser, or other service provider to the reporting fund. This would further the goals underlying the expansion of reporting following the Dodd-Frank Act, and the policy goals of investor protection and mitigation of systemic risks. To be clear, operational events can have systemic risk implications.

Such reporting would be consistent with other SEC initiatives. Reference is made to the notification requirements under the Securities and Exchange Commission's (SEC) Regulation Systems Compliance and Integrity (Regulation SCI) which was developed, *inter alia*, in light of the dependency of the securities markets on evolving technology and vulnerabilities to outages including in connection with cyberattacks.[1] Notably, a covered entity is required both to make an "immediate" notification to its Federal regulator of an incident; followed within 24 hours on a "good faith, best efforts basis" by a notification of event and assessment to the extent available at that time; and at later times more detailed impact assessments.[2] More recently, the SEC has published for comment a proposed rule that would include new reporting requirements for the subset of operations events that are significant cybersecurity incidents, by investment advisers, registered investment companies, and business development companies.[3]

Particularly instructive for the SEC, and essential for efforts of the Financial Stability Oversight Council to monitor potential systemic risks, should be the new reporting requirement by the U.S. Federal Banking Agencies – the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation.[4] That final rule will require a banking organization to notify its primary Federal regulator of any ''computer-security incident'' that rises to the level of a ''notification incident,'' as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. The final rule also requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours. Regulated entities as well as their service providers are currently preparing for implementation of that new rule with effective date of April 1, 2022 and compliance date of May 1, 2022.

The trend to require additional reporting of incidents or operations events will only continue. On March 15, 2022, the President signed into law the Consolidated Appropriations Act, 2022.[5] That broader

[1] See SEC Final Rule, Systems Compliance and Integrity, 79 Fed. Reg. 72,252 (December 5, 2014), as implemented in particular in 17 CFR § 242.1002--.1007, available at 2014-27767.pdf (govinfo.gov). The primary author of this comment letter previously had oversight responsibility for the implementation of Regulation SCI by SEC regulated exchanges.
[2] See 17 CFR § 242.1002(b).
[3] See 87 Fed. Reg. 13,524 (March 9, 2022). Comments on that proposed rulemaking may be submitted separately.
[4] See 86 Fed. Reg. 66,424 (November 23, 2021).
[5] Public Law No: 117-103 (March 15, 2022).

appropriations law also contains the ''Cyber Incident Reporting for Critical Infrastructure Act of 2022 which authorizes rulemaking for incident reporting across a broad range of actors (including components of the financial sector) and calls for coordination with any analogous reporting requirements by other government agencies. Other jurisdictions are following analogous paths to mandate incident reporting. One prominent example is the European Union's proposed Digital Operations Resilience Act (DORA),[6] for which a revised proposal after a round of public consultation is expected soon.

This broader context should be understood as strong support for the policy goal of the SEC requiring additional reporting of relevant operations events, and in moving forward with the rule without delay. That notwithstanding, the broader trend towards such reporting also emphasizes the difference between this aspect of reporting and the other financial and operational details that the SEC requires currently and would expand through the proposed amendments to Form PF. Implementing such changes as part of Form PF not only appears out of place, but would make more difficult the goals sought by the SEC and a range of other government entities to obtain and be able to share information about incidents and indicators of systemic risks; it would also raise the complexity, costs, and make more difficult for the regulated industry to timely notify reportable incidents. One of the reasons for this is that the parties involved in reportable incidents often will include broader IT service providers and sub-contractors that are not specifically focused on the regulations at broader issue in the Proposed Amendments to Form PF; rather an operations event or incident affecting an entity such as a cloud services provider could in the future trigger directly or indirectly through affected chains of customers, reporting to a broad range of government entities.

V. Specific Comments and Responses to Request for Comment Questions

The following provides specific comments on the proposed current report in section 5, Item H regarding a "Operations Event."

40. Will this proposed reporting requirement provide us with notice of operations events that may have serious implications for the fund, its investors, and financial stability?

Yes. Please see above regarding the importance of this type of reporting regarding operations events, but with a recommendation that it be required separate from Form PF.

41. Does the definition of ''operations event'' provide a clear, objective trigger for reporting? Would advisers be able to assess this during an operations event? We proposed a principles-based approach for reporting of an operations event that is a ''significant'' disruption or degradation of the adviser's operations and for operations that are reasonably measurable, we would view a 20 percent disruption of degradation of normal volume or capacity as ''significant.'' Are we correct that certain disruptions may not be quantifiable? Do commenters agree that a 20 percent disruption or degradation of normal volume or capacity indicates that an event is ''significant?'' Should the reporting event include a time frame to

[6] See Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, available at EUR-Lex - 52020PC0595 - EN - EUR-Lex (europa.eu).

measure a 20 percent disruption or degradation? If so, what time frame? Should it be over one business day or over one month? Do advisers' compliance programs typically include benchmarks that could be used to measure a 20 percent disruption or degradation? Are there other potential approaches for an operational events trigger?

The definition and this question include multiple different aspects as to the nature of an event requiring reporting, and also to a materiality threshold.

- With respect to operations event, we suggest that in addition to the definition it is useful to provide and continually update examples in guidance with respect to reportable incidents. That notwithstanding, a general principle should prevail in that it is an aspect that meets any of the following requirements: (i) impairs the operation of the fund, including the risk of operational loss—this is included in the first three boxes under proposed 5-29; (ii) negatively impairs investors in a fund (for example, an operational incident that prevents withdrawal might not impact the fund itself but has a negative liquidity impact on an investor) -- this is not included in proposed 5-29; (iii) or causes the failure to meet regulatory requirements such as ongoing risk management monitoring (regardless of whether a risk materializes, this may include the absence of a risk mitigation tool) -- this is included in the fourth box under proposed 5-29.
- As to materiality threshold, we agree that it is useful to require that the disruption be "material" or "significant". We do not, believe, however, that a numerical threshold such as 20% is useful for a fund or an adviser. In the nature of the business, an operations event such as the failure of a system is likely on/off, black/white, and it does not help, certainly not in terms of timely reporting of an incident, to expect a numerical threshold such as might be the case in other reporting areas such as a market value movement of certain assets by 20%. In a large broker-dealer, it might be possible that a threshold be applied, such as if a pandemic caused 20% of staffing in a control division to be unavailable, but this hardly appears relevant for a fund or adviser.
- Regarding timeliness, it is recommended that the SEC adopt a provision similar to that of the new rule by the Federal Banking Agencies that the operations event may last more than four hours (or alternatively a business day). The issue is that there is a disruption -- it is unlikely to be useful, and rather is counterproductive to timely reporting to try to project the timing for a longer period such as a month. Moreover, timely *initial* reporting of an operations event does not lend itself to a numerical percentage threshold.

42. Are we correct in our understanding that many large hedge fund advisers maintain sophisticated back office operations or already engage service providers that would be reasonably able to measure whether an event has impaired their key operation beyond a 20 percent threshold? Are there any other objective measures gathered by advisers or their service providers that could be utilized as a trigger for this reporting event?

As per the response to question 41, it is unlikely that this would be effective. More objective for service providers would be the failure to provide the services as agreed for a minimum period of time. Since a service availability is a common aspect of a Service Level Agreement, this is commonly measures and monitored.

43. Will the checkboxes provided to describe the circumstances of the ''operations event'' provide us with sufficient detail regarding the operational issue and its potential severity? Should we amend, add, or remove any of the check boxes? Is the check box for force majeure events appropriate, or does it have the potential to cause numerous notifications during certain widely applicable disaster events like a pandemic or large hurricane?

The checkboxes proposed are similar to elements in other incident or operations event reporting of an *initial* report, but do not lend themselves to ongoing updates or more detailed reporting. Again, this suggests that it is not prudent to attempt to include this class of reporting within Form PF.

As to different aspects:

- Date and time of each of the first occurrence, and discovery are common reporting elements. (Time of day might be relevant, for example if during trading hours.) A third date/time element should be included as to when the event or incident is materially mitigated.
- The category of whether an event occurred internally, at a specific service provider (see also next question) or externally is important.
- Reporting of force majeure events is important. There is no reason to assume in the modern age that institutions would be affected similarly by all but the most calamitous force majeure events. For example, a flood might only impact a tenant having a computer system in a lower level, or not at all if the data is processed by a cloud provider.

44. Should we require an adviser to indicate whether the operations event is caused by a service provider and require the adviser to provide information regarding the service provider, as proposed? Should we define the term ''service provider'' for these purposes? Should we require reporting only for those service providers listed in Form ADV, Schedule D for the private fund? Are there some operations events that could be caused by a third party that is not a service provider to the reporting fund or adviser? If so, should we require an adviser to provide information regarding such a third party?

It is essential to include service providers in order to fulfil the purpose of such reporting. It appears to be less important to define "service provider" than to indicate that a negative impact on operations should be reported, regardless including if provided by a third party service provider.

It is not sufficient to include only the service providers in Form ADV, Schedule D (auditor, prime broker, custodian, administrator) for the private fund. The failure of other IT service providers of the fund or sub-contractors or sub-outsources of the Schedule D delineated entities could cause a material disruption.

One of the most important lessons which the SEC could draw from the new incident reporting rule of the Federal Banking Agencies, is that incident requirements should be implemented through the regulated entity to all relevant entities, including outsourcing or subcontractor chains, to any entity for which a disruption could have a material negative impact on the regulated entity. Even if the SEC does not have direct regulatory authority over such third party service providers (such as that granted to the Federal Banking Agencies under the Bank Service Company Act), the SEC could impose expectations that its regulated entities contractually agree with relevant service providers to inform them of incidents, disruptions or operations events likely to lead to reportable events. This is a longstanding best practice across regulated entities in multiple jurisdictions.

Finally, it is relevant as proposed that the reporting with respect to service providers include full legal name, a unique identifier such as LEI where available, and identify the class of effected services. This information is essential to the ability of the SEC to quickly identify potentially systemic risks, in terms of a service provider to multiple industry participants. Such reporting solutions are reasonably available, including offerings by CRINDATA, which can be seen at www.crindata.com.

45. Should we define ''key operations'' as proposed? Are there any activities that we should add or delete from the definition? For example should key operations also include the operation of the reporting fund in accordance with major contractual commitments to the reporting fund's investors and/or

counterparties? For example, should it be considered a significant disruption or degradation of key operations if an issue at a service provider degrades the fund's ability to measure its positions or communicate certain information to counterparties pursuant to contractual notice terms?

We suggest that the key operations should include servicing investors, as also mentioned in response to question 41.

46. As an alternative to defining ''operations event'', should we require current reporting by advisers whenever they initiate a business continuity plan? Would the initiation of a business continuity plan be a simpler trigger to apply? Would the initiation of a business continuity plan as a reporting event result in too many current reports about events that could not lead to investor harm or systemic risk? Would it miss important operations events that could lead to investor harm or systemic risk? Should we be concerned that advisers might delay initiating a business continuity plan so as to avoid reporting?

The triggering of a business continuity plan per se does not appear to be a good proxy for the information otherwise sought in the rule. Such trigger could be either under-inclusive or over-inclusive, such as whether successful operation of the business continuity plan mitigates the risk. It would be better to include the effect of a business continuity plan or other contingency measure in mitigating risks, where available in initial reporting, but also as part of reporting updates over time.

47. Should we require an adviser to indicate whether it has initiated a business continuity plan relating to the operations of the adviser or reporting fund, as proposed? Does the initiation of such a plan provide the Commission with indications of potential stress at the fund or its adviser?

See response to question 46.

Comments to other specific issues:

Item K. Explanatory Notes: This section of the proposed Form PF would allow for additional information helpful in understanding the information reported in response to any Item in section 5 of this form. It is nonetheless unlikely to be helpful if operations events require additional elaboration in Item K. Initial notification of operations events should be factual, and provided in a structured way, which allows the SEC to assess risks to a fund or adviser, as well as potential broader systemic risks. Subsequent updates should provide more detail, including when the event is resolve. This comment further illustrates why the proposed Form PF is not an appropriate vehicle for reporting operation events.

Fees. While we have no objections to fees in connection with filing reports generally, in particular quarterly or annual disclosures, it could be counterproductive for the SEC to require a fee to provider an indication of potential operations events about which the SEC wishes to be made aware on a timely basis, as well as updates as the situation changes. The reporting entity will likely have much higher costs (if nothing else in lost management time) when an incident occurs than the filing fee itself. Requiring an additional fee for an early report of an operational incident also appears contrary to the trend of other such required reporting. Again, this illustrates the reporting under proposed Item H, while important, does not fit in the broader context of the proposed changes to From PF.

Shared solutions. Shared solutions are appropriate and can be viable, effective, and efficient ways for service providers to report to their various counterparts, or on behalf of regulated entities directly to the SEC or other regulator. The SEC should encourage or allow such reporting on behalf of its regulated entities, just as other regulators are implementing.

VI. Closing

Thank you for the opportunity to comment on the Proposed Amendments, and in particular the importance of requiring notifications of an Operations Event as suggested in Item H, but ideally to be implemented outside of changes to Form PF.

Sincerely,

CRINDATA, LLC

By: *James H. Freis, Jr.*
James H. Freis, Jr.
Co-Founder & Chairman

Mark Stetler
Mark Stetler
Co-Founder & CEO