Martin Boer
Senior Director
Regulatory Affairs

December 19th, 2022

Mr. Rupert Thorne
Deputy Secretary General
Financial Stability Board (FSB)
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland
(Submitted electronically)

Re: FSB Consultative Document on Achieving Greater Convergence in Cyber Incident Reporting

Dear Mr. Thorne,

The Institute of International Finance (IIF)[1] and its members are pleased to respond to the Financial Stability Board (FSB) Consultative Document on "Achieving Greater Convergence in Cyber Incident Reporting."[2] We commend the FSB's long-standing leadership in promoting greater harmonization around cyber security and cyber risk practices, including in this case around incident reporting across financial institutions and reporting authorities around the world. Cyber incident reporting (CIR), when used effectively, can be a beneficial tool that helps protect the global financial system. Increased awareness, visibility, and incident exchange, including across jurisdictions, can help disrupt and stop adversaries and assist affected financial institutions (FIs) with protection, mitigation, and response. The proliferation of cyber incidents in recent years has only highlighted the importance of coordinated information sharing between and among the public and private sectors.

We greatly appreciate the FSB's efforts on this important issue and its recommendations towards a more harmonized global reporting framework. As the FSB has rightly identified in this consultation, and as has been detailed in a previous IIF Staff Paper,[3] CIR is often challenged by

[1] The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial, and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, professional services firms, exchanges, sovereign wealth funds, hedge funds, central banks, and development banks.
[2] FSB 2022. "Achieving Greater Convergence in Cyber Incident Reporting" October 17, 2022.
[3] IIF 2021. "IIF Paper on the Importance of More Effective Cyber Incident Reporting" June 10, 2021.

differing approaches and reporting requirements across various jurisdictions and authorities when it comes to what information is shared, in what format, and in what timeframe. There can be multiple policy objectives at play across the incident reporting landscape, such as providing early warning with actionable information and voluntary supplemental information sharing as an incident unfolds. We urge the FSB to encourage member jurisdictions to ensure that incident reporting requirements are simple, tied to an actionable purpose, and efficient. We similarly would encourage the FSB to highlight the importance of bidirectional sharing of reported information from authorities to FIs. Information related to material cyber incidents and operational outages that is reported to authorities should be fed back to FIs, which can then take measures to bolster their cyber security and thereby enhance the resiliency of the sector.

In the event that a cyber incident has occurred, firms would benefit from being able to launch processes and procedures in parallel instead of responding individually to jurisdictional stakeholders. Currently FIs are often faced with multiple national and transnational reporting requirements, which can slow down firms' own incident response efforts. These differences in reporting requirements are further compounded by differences and ambiguities in the terminology used, such as how firms and authorities define what constitutes a "cyber incident." Further, it is often the case that there is insufficient information-sharing, including from financial authorities to FIs, and inadequate cross-border cooperation and collaboration. Together, these issues lead to fragmentation and divergence, unnecessarily slowing the ability of firms and authorities to respond to malicious threats.

Given the fragmented state of the cyber incident reporting landscape, we very much appreciate the important role that the FSB has been playing to draw attention to these challenges and promote greater convergence between jurisdictions. In particular, the IIF commends the FSB's attention to promoting clearly defined objectives for incident reporting among financial authorities. Purposeful and clearly defined policy objectives will ensure that authorities receive actionable information in a timely manner during critical moments in incident response.

Ultimately, the FSB's recommendations should be aligned with leading global best practices of both the public and private sector, which would help address regulatory and supervisory fragmentation, advance robust standards for cyber security and incident reporting, and improve the resilience of the global financial system. The IIF and its members believe that financial firms are uniquely positioned to advance these efforts.

The financial services industry has long been a target of malicious cyber threats, and as a result has long understood the importance of not just preventing, detecting, and responding to cyber threats, but also of providing robust and timely disclosures about material cyber security incidents and vulnerabilities. As such, the financial services sector has invested considerably in the Financial Services Information Sharing and Analysis Center (FS-ISAC), which shares cyber threat information and best practices across nearly 7,000 members globally.

Since its inception in 1999, the FS-ISAC has been widely recognized as a global leader in threat intelligence sharing, and its model for information sharing has been replicated across other sectors. The ISAC model has been successful in disseminating information in a timely and confidential manner to industry stakeholders on a voluntary basis. Incorporating established reporting practices can help strengthen the overall resilience of the financial system, especially for FIs and authorities at different stages of cyber security maturity. We urge the FSB to encourage

jurisdictions to align CIR with established reporting practices used by existing platforms, such as FS-ISAC.

The IIF also supports the FSB's proposal to update its Cyber Lexicon which, since its publication in 2018, has promoted a much-needed cross-sectoral, common understanding of relevant cyber security terminology across the financial industry, including among authorities and other industries. As such, the Cyber Lexicon plays an important role in helping to reduce regulatory fragmentation and promoting a common understanding of cyber security terminology. However, given that the Cyber Lexicon was published four years ago, and that cyber security is a discipline that is continually evolving, the IIF and its members encourage both this proposed update, as well as regular, periodic updates to ensure that it remains authoritative and relevant for both authorities and financial firms. In recognition of the overlaps and similarities, as well as distinct differences, between cyber security, operational resilience, third party risk management, business continuity management, and operational risk, we propose that the FSB develop and maintain a single Lexicon on non-financial risk as an important global resource for firms and authorities around the world.

The IIF has provided comments below to address the main areas of discussion and recommendations in the consultation. We look forward to continued collaboration with the FSB throughout the stakeholder feedback process.

Challenges to Achieving Greater Convergence in CIR

Malicious versus Non-Malicious Incidents

The IIF applauds the FSB's efforts to develop a more harmonized and consistent incident reporting landscape. Fragmented requirements and the growing complexity of the regulatory ecosystem have added to the challenges of managing and reporting cyber security incidents. The FSB should encourage authorities to converge around common definitions, and appropriate reporting thresholds and criteria, so that the most critical and materially impactful incidents fall under cyber incident reporting frameworks. We encourage the FSB to consider these policy objectives of CIR as it updates its Cyber Lexicon, particularly its definition of a cyber incident.

For a CIR framework to be successful, it is essential that notification and reporting be limited to malicious incidents that are of a sufficiently high threshold. By prioritizing incidents that meet these criteria, authorities and FIs alike can focus their attention on addressing those incidents that pose the most urgent risk to the sector.

While there should be incident notification and reporting for all material incidents, we recommend that the FSB narrow the definition of a cyber incident to those in which there is a motive-based characteristic (i.e., malicious intent). This distinction is crucial, as it recognizes that a cyber security incident is a malicious incident driven by malicious intent and a threat actor targeting an FI's systems, and thus necessitates a wholly different response and sense of urgency than a non-malicious incident caused by an operational, technological, or human error. Malicious incidents also pose very different threats to the financial system than non-malicious incidents, as other FIs may similarly be targeted.

The IIF recommends that the FSB clearly demarcate between a malicious cyber incident and an operational incident in its definitions. As such, we recommend the FSB remove "non-malicious" incidents from the scope of its definition of a cyber incident. Instead, as we discuss further on in this response, we propose that the FSB add a separate definition for operational incidents, such

as those incidents created by human error (e.g., failed change management, faulty hardware). Operational incidents meeting certain materiality thresholds, such as those with systemic implications, have the potential to meet defined incident reporting thresholds and therefore warrant reporting to financial authorities. However, the IIF encourages the FSB to distinguish a cyber incident as an incident driven by malicious intent because the criticality for early warning of a malicious cyber incident has a different set of actions than a non-malicious operational disruption. Non-malicious incidents (i.e., operational incidents) generally have different incident management policies, procedures, personnel, and reporting objectives when compared to malicious cyber incidents.

The IIF and its members recognize the importance of notification and reporting all material incidents that meet reporting thresholds. However, it is critical that FIs and authorities are able to streamline the processes for reporting the most important incidents – both malicious and operational incidents reaching a certain threshold – in order to help authorities and other firms address these issues as quickly as possible, and to prevent any contagion across the financial sector. Maintaining unique definitions will enable better management and reporting of malicious and non-malicious (i.e., operational) incidents. These distinctions, across definitions and reporting requirements, will ensure CIR remains fit-for-purpose and meets its intended policy objectives, namely providing actionable information to regulators and FIs, mitigating the threat, and optimizing resource allocation in times of stress. We understand that the FSB has a separate working group on third-party risk, which may consider third-party operational outages that can have financial stability implications. We would suggest there be continued collaboration between the FSB's cyber and third-party risk workstreams while also recognizing that each presents distinct challenges.

Bidirectional Information Sharing

Bidirectional information sharing is important to the success of CIR, as it helps enable early warning of potential incidents, the continued resiliency of firms' cyber security measures, and prevention of future cyber incidents. Financial authorities are uniquely positioned to recognize cyber threat trends, as well as when a cyber incident may have a broader impact on multiple FIs. Firms would benefit from an information feedback loop with authorities, in which actionable information, threat intelligence, and/or vulnerability warnings that are shared with authorities are promptly also communicated to industry. FIs would also benefit from regular communications from authorities detailing broader trends and themes they are seeing, which could help them gain a more global understanding of the cyber security landscape. By sharing this information with FIs, authorities can help protect and safeguard the financial ecosystem.

However, current information-sharing efforts from authorities to firms are often inconsistent or too slow to have a meaningful impact on firms' cyber risk mitigation efforts, further hampering efforts to establish trusted public-private reporting frameworks. When actionable information is reported to authorities, it should be promptly aggregated, anonymized, analyzed, and shared with industry to foster the mitigation of future cyber incidents. Timely dissemination of such information is the best way for early warning systems to be effective and would have a meaningful impact on the resiliency of the sector.

Establishing Trust, and Secure and Timely Communications

The IIF welcomes the FSB's recommendation that financial authorities implement secure forms of incident information handling to ensure the protection of sensitive firm data, as we believe this

is critical for any effective CIR. As a central repository of highly sensitive cyber incident data, the reporting authority may itself become a target of malicious cyber actors. It is important to securely store sensitive cyber incident data that is shared with authorities.

CIR reporting requirements should be tightly linked with an actionable purpose and have clear descriptions of how authorities will utilize the reported incident information in furthering that purpose. Financial authorities may determine that reported cyber incident information should be shared with other financial authorities or FIs. Reported cyber incident information must be anonymized and transmitted using secure data transfer protocols. If financial authorities share reported information with industry, they must remove attribution details and, whenever possible, coordinate with the FI that provided the cyber incident information (originator) before disseminating the intelligence. In the event the financial authority shares reported information with another authority, particularly across jurisdictions, the originator would benefit from being informed prior to information being shared. In addition to establishing greater trust and transparency with respect to the use of the reported information, these measures can help FIs uphold their data security and privacy requirements, as well as prevent duplicative reporting across multiple authorities.

The IIF encourages the FSB to provide clear principles for how the reported information will be stored, secured, transmitted, and retained, both within the reporting authority as well as shared with, or accessed by, other reporting authorities or jurisdictional entities. The FSB could encourage financial authorities to align their security control and data retention standards with existing best practices, which could help ensure that the incident data collected through notification, reporting, and information sharing efforts remains protected. We again urge the FSB to encourage financial authorities to look to effective security controls and data retention requirements to enhance the confidentiality and protection of reported information.

Early Assessment and Safe Harbor Provisions

For a CIR framework to be effective, FIs should feel confident that, when reporting in the wake of a cyber incident, especially when done so on a voluntary basis, that the affected entities will not be penalized or publicly shamed for complying with CIR requirements. Furthermore, cyber incident data that is provided in notifications or reports is sensitive, confidential, and should not be subject to discovery in any legal action, which is not consistent across jurisdictions. The FSB should encourage authorities to extend liability protections to firms who notify or report on covered incidents. Such safe harbor provisions help incentivize proactive reporting and transparency, and by extension help strengthen sound cyber risk management practices across the industry.

The IIF also proposes that financial authorities adopt safe harbor provisions for reporting entities that may be unable to comply with all required disclosures when a potential incident is initially detected. The affected entity may only have minimal information during the early stages of detection and may not yet know the severity of the threat, or whether it is a cyber incident or an operational incident. During this early assessment period, FIs should have sufficient flexibility to report minimal, high-level information to the reporting authorities, as that is often the only information initially available to firms when a threat is first discovered.

Recommendations (Section 3)

The IIF and its members largely agree with the recommendations outlined here. However, Recommendation 8, which proposes extending materiality-based triggers to include <u>likely</u> breaches, is inconsistent with the revised cyber incident definition. Given this incompatibility, the

IIF proposes that materiality-based triggers *do not* include likely breaches, as that would expand the scope far too broadly and would prevent excessive reporting to financial authorities.

Financial authorities that use materiality thresholds should explore adjusting threshold language, or use other equivalent approaches, to ensure FIs only report incidents that caused actual harm and where reporting criteria have been met.

Common terminologies for CIR (Section 4)

The IIF appreciates the FSB's efforts to promote greater harmonization in CIR among global authorities through the use of common definitions, as outlined in the Cyber Lexicon. The IIF supports the FSB's update to both the definitions of "Cyber Incident" and "Cyber Incident Response Plan," in line with feedback from the IIF and other stakeholders. As mentioned in this response, cyber incident notification and reporting to financial authorities should be restricted to malicious incidents that result in actual harm and are of a sufficiently high threshold. Aligning terms will help reduce the risk of undue market fragmentation while also streamlining the overall cyber incident reporting process for FIs. The four added terms – "Insider Threat," "Phishing," "Ransomware," and "Security Operations Centre" – are welcome, as they were also put forth as suggested new terms in previous IIF submissions.

There is an increased focus globally on operational resilience, third party risk management, and other operational and non-financial risks both at the domestic and global levels. As this work proceeds, the IIF encourages the FSB to maintain one "non-financial risk" Lexicon that could be leveraged across both operational resilience and cyber resilience, as opposed to producing different resources. As other global standard-setters increasingly turn their attention to these non-financial risks, the IIF calls on the FSB to encourage the Basel Committee on Banking Supervision (BCBS), Committee on Payments and Market Infrastructures (CPMI), the International Association of Insurance Supervisors (IAIS) and International Organization of Securities Commissions (IOSCO) to use the updated Cyber Lexicon and proposed "non-financial risk" Lexicon as their main reference work. Relatedly, the FSB should continue to encourage domestic/regional member authorities to harmonize definitions as much as possible around the updated Lexicon(s).

Refining the Cyber Incident Definition

The IIF strongly agrees with the decision to remove "jeopardizes" from the definition of cyber incident to limit the scope to incidents that cause *actual* harm, rather than those with merely the potential of being an incident. When combined with material thresholds, this will enable authorities to focus on the materially impactful incidents and not be overwhelmed by excessive reporting. It would also be useful if the FSB encouraged member authorities to consider this definition in their own regulations and polices so that "potential" impacts remain out of scope for CIR.

The IIF would also recommend further revisions aimed at strengthening the cyber incident definition. The FSB should consider removing point (ii) from the cyber incident definition. While violations of security policies, security procedures, or acceptable use policies may weaken the security posture (e.g., overdue security patches, weak passwords) and lead to a cyber incident, the presence of these violations by themselves are not incidents.

Further, as noted above, the IIF recommends removing "non-malicious" incidents from the scope of cyber incident definitions. While incident notification and reporting should occur for all material incidents, the definition of cyber incidents should be limited to incidents stemming from malicious intent. Operational incidents, such as those incidents created by human error (e.g., failed change

management, faulty hardware), have the potential to meet defined incident reporting thresholds and warrant reporting to financial authorities. However, operational and technology issues that are not of a sufficiently high threshold and do not have a material impact should generally be reported through other channels, such as information-sharing platforms like the FS-ISAC.

Add Operational Incident Definition
Given that cyber and operational incidents use the same incident reporting framework, the IIF proposes adding a definition for operational incident to the Cyber Lexicon to further distinguish between malicious and non-malicious incidents. The following definition is proposed:

Operational Incident: An event that adversely affects the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, as a result of human error or non-malicious systems failures (e.g., hardware failure).

Additional terms that would be worth adding include “materiality thresholds,” “supply chain risk,” and “third party service provider.” All of these terms are becoming increasingly important for cyber security, as well as in the areas of operational resilience, and third-party risk management, where the FSB is also undertaking important work. To the extent that these definitions can be made consistent across FSB initiatives and across member jurisdictions, would better enable the financial services sector to respond and report more effectively.

Modify Cyber Event and Insider Threat Definitions
The IIF recommends modifying the cyber event definition to include “network” to align with NIST. The proposed definition is, "*Any observable occurrence in an information system or network. Cyber events sometimes provide indication that a cyber incident is occurring.*"

Additionally, the IIF recommends modifying the insider threat definition. In its current definition, the term “trusted entity” is undefined and could be overly broad. We suggest amending the definition to, “*the threat that an employee will use authorized access, wittingly or unwittingly, to do harm to the organization’s mission, resources, personnel, facilities, information, equipment, networks, or systems*.”

Format for Incident Reporting Exchange (FIRE) (Section 5)

The IIF supports the idea of a Format for Incident Reporting Exchange (FIRE) to help firms share information on relevant cyber incidents efficiently and effectively. It is important that financial authorities work together to develop a common reporting approach to CIR. As mentioned in the consultation, FIs comply with a number of reporting requirements that maintain different definitions, timelines, and reporting thresholds, as well as oversight and enforcement mechanisms. For a CIR harmonized framework to be successful, it will need to allow for flexibility, including allowing financial regulators options to customize the form. However, the IIF recommends setting the common data points that would be standard across all cyber incident reporting forms (e.g., description of incident, impact, contact information). Establishing certain limitations on the extent to which financial authorities can customize the form will help reduce time spent on reporting by financial institution’s incident response teams and create a more uniform approach to CIR.

Reported information for the initial notification of an incident should be simple to convey, consisting of only high-level indicators, and closely tied to an actionable purpose so that authorities and institutions both understand the utility of any reported information and how it will be used. It is important to ensure that the approach is accepted by member jurisdictions, and that

it will ultimately replace, and not come on top of, existing frameworks. Otherwise, it would further add to market fragmentation.

It would be instructive for the FSB to advise stakeholders on what other actions are under consideration as part of the FIRE process, such as whether one organization will collect and house all the reported information. Such a central repository of cyber incident and firm data could lead to challenges, depending on which organization is hosting the repository, how it is protected, and what time of information it would hold. Depending on the nature of the data collected, the content of a FIRE portal could itself become a high value target and would therefore require substantial protections. As such, FIRE should not require overly sensitive information, and should be protected according to industry standards and best practices. Financial authorities should collaborate with FIs to determine what data can be comfortably shared on the portal (e.g., attribution, indicators of compromise). As mentioned earlier, increased bidirectional information sharing would be tremendously beneficial, and could be incorporated into the FIRE process, facilitated by a more standardized approach to reporting.

Conclusion

We appreciate the opportunity to comment on the FSB Cyber Incident Reporting consultation and the important issues it raises. As noted above, the IIF and its members are strong supporters of information-sharing and appreciate all the efforts being undertaken by the FSB and other authorities to protect and safeguard the global financial system. We encourage the FSB to work collaboratively, and with other global standard-setters, to promote the harmonization of reporting requirements and to achieve an appropriate balance between the benefits of CIR and the risks and consequences of reporting too many cyber events, when the thresholds are set too low.

We thank the FSB for its consideration of our comments and welcome any additional stakeholder engagement around this topic to help the FSB in its efforts to encourage and achieve greater convergence in cyber incident reporting. If you have any questions, please do not hesitate to contact Martin Boer at mboer@iif.com or Melanie Idler at midler@iif.com.

Sincerely,

Martin Boer
Senior Director, Regulatory Affairs
Institute of International Finance (IIF)

CC: Grace Sone, Head of Cooperation and Organisation, FSB