December 31, 2022

Mr. Rupert Thorne
Deputy Secretary General
Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland
Submitted via email: fsb@fsb.org

Re: Achieving Greater Convergence in Cyber Incident Reporting

Dear Sir:

On behalf of the Global Financial Markets Association ("GFMA")[1], which consists of the Association for Financial Markets in Europe ("AFME"), the Asian Securities Industry and Financial Markets Association ("ASIFMA") and the Securities Industry and Financial Markets Association ("SIFMA") (collectively, the "Associations"), we appreciate the efforts by the Financial Stability Board ("FSB") and welcome the opportunity to respond to the Consultative Document ("CD"), "Achieving Greater Convergence in Cyber Incident Reporting," with input and feedback from our collective memberships around the world.

GFMA continues to believe that more should be done to reduce the fragmentation of cybersecurity regulations across the financial services industry. As the FSB highlighted in its important 2017 document "Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices," the trend in this area is for further unilateral regulation of cybersecurity practices of financial services firms by national authorities rather than greater coherence.[2] Rather than improving resilience, a globally fragmented cybersecurity regulatory environment for the industry increases financial stability risk by driving complexity and inefficiencies into the system. Where regulations relate to the management of incidents or the testing of systems, cross-border coordination is especially important to ensure that resources are not unnecessarily diverted away from the

[1] The GFMA represents the common interests of the world's leading financial and capital market participants, to provide a collective voice on matters that support global capital markets. We advocate on policies to address risks that have no borders, regional market developments that impact global capital markets, and policies that promote efficient cross-border capital flows, benefiting broader global economic growth. The Global Financial Markets Association ("GFMA") brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA.

[2] Financial Stability Board: "Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices" https://www.fsb.org/wp-content/uploads/P131017-1.pdf, October 2017.

management of cybersecurity incidents such as protecting financial firm critical data, systems as well as the financial ecosystem.

Along these lines, the FSB's 2021 publication, "Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence," found that fragmentation exists across sectors and jurisdictions in the scope of what should be reported for a cyber incident; methodologies to measure severity and impact of an incident; timeframes for reporting cyber incidents; and how cyber incident information is used.[3] This potentially subjects financial institutions that operate across many countries or jurisdictions to not only multiple, but varied reporting requirements for a single cyber incident.

Some global institutions reported during SIFMA's 2019 Quantum Dawn exercise that they would need to report to over 100 countries or jurisdictions creating significant operational challenges and inefficiencies.[4] Concurrently, financial authorities receive diverse and incomplete information for a given incident, which could undermine their ability to aggregate and share trends. This underscores a need to address divergent incident reporting frameworks as well legal and compliance constraints in information sharing between global regulatory authorities and financial institutions.

We concur with the FSB's survey findings related to financial authorities' reporting objectives noted in Annex 1 of the CD which are to:

- Support management of the impacts arising from a cyber incident at one or more institutions
- Play an active role in the technical resolution of a cyber incident at one or more institutions
- Build understanding and/or support coordination of sector-wide cyber incidents
- Inform supervisory understanding of the risk profiles and/or capabilities at affected institutions
- Identify potential weaknesses or areas for improvement in current regulation or requirements
- Provide a consolidated source of incident data, trends, threats and/or risks across peer firms or the financial sector as a whole

GFMA applauds the significant efforts undertaken by the FSB over the past several years to reduce regulatory fragmentation by developing common frameworks, lexicons, and a Cyber Incident Response and Recovery (CIRR) toolkit for cyber incident reporting and we look forward to continued collaboration on this important topic. As such, we are submitting responses to the questions posed in the CD with the following overarching themes:

Develop a globally consistent cyber incident reporting framework

The GFMA fully supports the concept of the Format for Incident Reporting Exchange (FIRE) framework with the goal of globally standardizing cyber incident reporting requirements between regulatory authorities and financial institutions.

[3] Financial Stability Board, "Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence: https://www.fsb.org/wp-content/uploads/P191021.pdf, October 2021.
[4] SIFMA Cyber Security Exercise: Quantum Dawn V, https://www.sifma.org/resources/general/cybersecurity-exercise-quantum-dawn-v.

Minimize the impact of a cyber incident
Financial firms today balance a multitude of responsibilities to a significant number of constituencies around the world including operational, business and cyber resilience, client and data protection, compliance with regulatory mandates, swift and thorough resolution of incidents, and information sharing across the sector. The effective and efficient use of scarce resources to address a cyber incident must, however, take precedence over regulatory reporting and real time data collection, especially in the initial phases of an incident.

Establish Feasible Reporting Timelines Commensurate with Incident Severity Levels
We agree with the incident reporting lifecycle phases the FSB has laid out and recommend the following to bring convergence to reporting time frames:

- **Initial Report** – Upon indication of an issue and prior to submitting an initial report, an institution is assessing impact and materiality, therefore limited information may be available to report. Our recommendation for Initial Reporting is that a notification occur upon an institution confirming that an incident has reached their internal materiality threshold. This allows provision of a heads-up notification to regulators within a reasonable amount of time.

- **Intermediate Reports** – As knowledge and understanding of an incident increase, institutions should make authorities aware of any significantly new information that could change response efforts.

- **Final Report** – Following an incident, it may take anywhere from several weeks to months to determine the root cause, depending on the sophistication of the attack. The common reporting elements of the Format for Incident Reporting Exchange (FIRE) framework can be useful to authorities in helping to conduct horizontal analysis of the most sophisticated attacks, which should be shared with the industry to support uplift of its cybersecurity posture.

We would suggest the FSB consider the above recommendations when seeking to standardize incident reporting timelines and information reported. The FIRE framework could be helpful in setting out the common information elements that institutions should seek to identify and report as information becomes available.

Regarding severity levels, we would also urge the FSB to converge around high impact malicious intent cyber incidents that cause actual harm, i.e., systemic risk, financial instability, consumer harm, and/or public health and safety concerns.

Promote robust information sharing to achieve collective goals
Information sharing among regulatory authorities and financial institutions regarding cyber incidents through a uniform reporting framework can be of great assistance to the financial sector through financial authorities' consolidated reporting of intelligence, trends and best practices, furthering proactive prevention and resilience efforts. The FSB should ensure there is an effective "feedback loop" where information reported to authorities is anonymized, aggregated, analyzed, and converted into actionable intelligence that is shared with industry to foster near real-time mitigation of future cyber incidents.

We urge the FSB to clarify what institutions can expect in return from authorities following reporting. Institutions would welcome authorities sharing early warnings on significantly impactful incidents and following more detailed reporting, institutions would welcome any centralized, anonymized, aggregated horizontal analysis developed. Understanding what firms may expect from authorities will not only incentivize firms to share more if they see value added in return, but also it will help clarify the types of information that firms should share with authorities.

We would also underscore that to build strong trust and deepen information sharing, authorities should preserve the confidentiality, integrity and availability of information shared and ensure the transparency of the information sharing pathways.

Implement bi-directional cyber incident notification protocols

Financial firms have significant concerns, following Log4j, SolarWinds, and recent regulatory data breaches caused by insider threats, around the protection of sensitive data and client PII transmitted to regulatory authorities and government agencies. The FSB should consider that if a government agency or regulatory body is breached, resulting in the compromise or exfiltration of sensitive financial firm data, that there exist cyber incident notification protocols to rapidly notify the impacted financial institution(s). We suggest that the FSB, regulatory authorities, and government agencies consider adopting the FIRE framework as a method of reporting cyber incidents back to financial sector firms if during a breach, their data has been compromised.

The Associations would also recommend that regulatory authorities consider adopting SIFMA's data protection principles developed in 2016, post several regulatory data breaches, as a minimum resilience "standard" to ensure that sensitive data sent to regulatory authorities or government agencies are protected.[5] The following are key principles to consider:

- **Data Collection:** Limit the collection of sensitive data to that which is directly relevant and necessary to accomplish a specified purpose
- **Data Usage:** Implement preventative and detective controls limiting access to sensitive data to authorized users
- **Data Sharing:** Implement policies to protect information shared with external entities
- **Data Disposal:** Securely eradicate, dispose, or destroy sensitive data when appropriate

Align FIRE with existing frameworks

The existence of a vast complex network of cyber incident reporting (CIR) frameworks and systems by countries, jurisdictions, and regulators requires a significant investment of resources that could be better leveraged to managing the incident, rapidly returning the firm to business-as-usual operations and minimizing systemic risk.

As such, the FIRE framework is a significant development that could minimize systemic risk. We want to make the FSB aware of a similar effort in the U.S. following President Biden's "Cyber Incident Reporting for Critical Infrastructure Act," (CIRCIA) that passed in March 2022.

[5] SIFMA Data Protection Principles, https://www.sifma.org/resources/general/data-protection-principles/.

The U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) has implemented a framework similar to the FIRE concept.[6] We encourage the FSB to coordinate with authorities that have existing frameworks to reduce fragmentation and potentially accelerate the implementation of a unified solution.

The FSB has invited feedback on this consultative document, in particular on the questions set out below. The following comments are the Associations responses to the specific questions posed.

Challenges to achieving greater convergence in CIR
Section 2

1. **Is the emphasis on practical issues to collecting and using cyber incident information consistent with your experience? Does your institution want to provide any additional evidence for the FSB to consider from your experience?**

The FSB in the CD identified the following practical issues associated with CIR:

(i) operational challenges arising from the process of reporting to multiple authorities;

(ii) setting appropriate and consistent qualitative and quantitative criteria/thresholds for reporting;

(iii) establishing an appropriate culture to report incidents in a timely manner;

(iv) inconsistent definitions and taxonomy related to cyber security;

(v) establishing a secure mechanism to communicate on cyber incidents; and

(vi) legal or confidentiality constraints in sharing information with authorities across borders and sectors.

Regarding the first issue, GFMA members, especially those with a global footprint, must be prepared to comply with over 100+ country, jurisdictional and regional reporting requirements. This mandate poses significant operational challenges and strains resources required to mitigate the cyber incident.

An additional operational challenge is that circumstances surrounding a cyber incident can be ambiguous and fluid. An occurrence that may appear to be a technology disruption may in actuality be orchestrated by a bad actor with malicious intent.

Moreover, the pool of highly skilled cyber professionals with technical expertise is limited, but threat actors are becoming more sophisticated and skilled. As further insight into

[6] Cybersecurity and Infrastructure Agency (CISA) Incident Reporting System, https://us-cert.cisa.gov/forms/report#contact-information, OMB Control No.: 1670-0037; Expiration Date: 10/31/2024.

operational challenges, we would like to highlight that for many global institutions there are different teams in each region and country accountable for the actual reporting of the incident; however, only the Cyber Incident Response Team has control of and is privy to real-time information.; Therefore, as a resource, they are continuously consulted by reporting teams.

Incident reporting is also a key element of operational resilience as it is the moment in time in which an institution must shift gears into response and recovery mode during which many critical decisions must be made in chaotic moments. Therefore, eliminating the myriad operational challenges that plague incident reporting today, could lead to many positive outcomes, including:

- Providing an effective early warning mechanism not just for the financial sector but also for institutions that might share common vulnerabilities,

- Providing analysis to help firms identify the most effective security controls, and;

- Helping firms better build a collective defense against common threats and tactics.

With respect to establishing an appropriate culture to report incidents in a timely manner, our member firms seek to ensure their organizational culture provides regulatory authorities with timely information regarding materially impactful incidents. These efforts are necessarily predicated on an undercurrent theme of trust among internal stakeholders (management and employees); those on the first line of defense do not fear negative repercussions, but are incentivized to raise issues early within their organizations.

In addition to internal organizational trust, there is also external trust that needs to be built and fostered between the financial institution and its regulators. Authorities should strive to create a reporting culture in which a sense of teamwork exists, especially after an incident has happened. The threat of further regulatory scrutiny could only serve to disincentive timely reporting.

External trust also extends between and among financial firms. Cybersecurity should never be treated as a competitive advantage. Firms must be encouraged to identify timely ways to share actionable information with each other.

Regarding the fourth issue, inconsistent definitions and taxonomy, please refer to our proposed definition of cyber incident in questions six and seven.

The fifth issue, "establishing a secure mechanism to communicate on cyber incidents" is a foundational element of cyber incident reporting. Our members have three main points to address: security, back up, and streamlining.

- Security - The contents of the online portal used to transmit cyber incidents to regulatory authorities could become a high value target. It is crucial that the existing data on the portal is adequately protected. The security of the platform also relates to the theme of trust as the organizations that are submitting data are trusting that regulatory authorities have appropriate data protection controls in place.

- Back Up - While consolidating modes of reporting is important, during a cybersecurity incident, it may not be feasible for an institution to use a portal. Our members have recommended there be at least two methods of reporting should one method become unavailable.

- Streamlining - While regulatory authorities have established secure mechanisms to communicate cyber incidents, the complicated network of reporting systems requires significant operations and technology investments creating operational challenges that reduce the efficiency and effectiveness of cyber, legal and compliance related staff. Streamlining and reducing the number of reporting mechanisms will greatly assist the financial firms in maximizing scarce resources.

For the final issue, "legal or confidentiality constraints in sharing information with authorities across borders and sectors," our members take their regulatory reporting obligations seriously and abide by these requirements in all reporting, including that which is voluntary. For all mandatory and non-mandatory reporting, it is recommended that the regulator or other entity collecting cyber incident notification reports does not individually identify the reporting financial institution and aggregates reported information. This accomplishes several goals: building trust with reporting institutions, potentially lessening reputational risk concerns, and increasing incentives to report all the while accomplishing the collective goal of information sharing. Along these lines, the United States Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA), in their April 2022 "Sharing Cyber Event Information: Observe, Act, Report," advises reporters that "… we will share anonymized information about this activity with others to help them manage their risk."[7]

In keeping with the theme of trust between financial institutions and regulators and the notion that cyber security is not a competitive advantage, the Associations ask for legal liability and Safe Harbor protections. While no global framework exists, we have looked to the United States as an example. For example, the March 2022 CIRCIA law and various state laws have liability and other protections around the following principles:

General Liability and Safe Harbor Protections
The Associations request that any cyber incident report made to a regulator by a financial institution be provided liability and safe harbor protections. There must be a guarantee that neither a regulator, organization, or private individual be permitted to utilize information reported for a legal action or proceeding. The information reported is to accomplish the mutual goals of cyber security. It is in all stakeholders' best interest to not disincentivize financial institutions to report by threat of litigation or other regulatory enforcement action.

Anonymous Information Sharing
Earlier in this letter, the Associations support robust information sharing for the mutual benefits and objectives of greater cyber security. However, we ask that any data and information gleaned from cyber incident reports be anonymized and unattributable to the reporter.

[7] Cybersecurity & Infrastructure Security Agency (CISA) "Sharing Cyber Event Information: Observe, Act, Report," https://www.cisa.gov/sites/default/files/publications/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf, April 2022.

Disclosure Prohibition
The Associations also request that a broad subpoena request exemption be applied to any report made. This shall apply to any third-party request made by a government, private entity, or individual.

Public Records
The Associations also request that any cyber incident reports be exempt from disclosure by a public record request made by any government, private entity, or individual.

Recommendations
Section 3

2. Can you provide examples of how some of the practical issues with collecting and using cyber incident information have been addressed at your institution?

Cyber incident reporting may arise from occurrences internal to an organization and actions committed by employees. An individual may be hesitant to report a cyber event because of the fear that doing so may show negligence on his end, risk job security, and damage professional reputation. To address this, financial firms encourage, incentivize, and reward early reporting.

Management may also be concerned about reputational risk and repercussions from clients. Premature disclosure of cyber events may result in financial issues such as increased insurance or other costs required to close capability gaps. The Harvard Business Review has also identified various concerns that organizations may have including: "…avoid[ing] disclosing vulnerabilities to bad actors," and "[potential] reputational or financial damage that can come with such a disclosure." The article encourages preserving anonymity of reporting organizations but making the reported data useful and meaningful by categorizing it by industry type, organization size, revenue, and geographic area.[8]

Finally, given there are so many entities requesting the same information in different ways, firms have had to create entity-specific flowcharts and jurisdictional-specific workflows. The creation, maintenance, and execution of these complex documents is not an efficient use of resources. Mindful of the regulators and financial institutions' shared goals of optimal operations, reduction of systemic risk, and protection of customer data, we respectfully suggest that during a cyber incident, all available resources be allocated towards incident resolution.

***3.* Are there other recommendations that could help promote greater convergence in CIR?**

While we are supportive of the FIRE framework to enable convergence, we would urge that the FSB encourage other authorities to not impose divergent reporting elements. Any

[8] Harvard Business Review, "We Need a Global Standard for Reporting Cyber Attacks" authored by Marc Barrachin and Algirde Pipikaite; November 6, 2019; https://hbr.org/2019/11/we-need-a-global-standard-for-reporting-cyber-attacks.

deviation from the FIRE framework would undermine convergence and potentially exacerbate fragmentation.

4. Could the recommendations be revised to more effectively address the identified challenges to achieving greater convergence in CIR?

Greater convergence in CIR can be achieved through consistent and robust collaboration between financial authorities and financial institutions with consideration for operational differences across the financial sector. The comments below reflect this sentiment.

Recommendation 1: GFMA supports the recommendations to establish and maintain clearly defined objectives for incident reporting and recommends consulting with private sector partners when defining and refining those objectives to ensure that all stakeholders fully understand and commit to the objectives.

Recommendation 3: While recommendation three is a productive step toward addressing reporting format fragmentation, allowing financial authorities to "individually" identify common requirements and "where appropriate," develop standardized formats for exchanging information could result in continued fragmented reporting standards. Financial authorities should collaborate, in partnership with covered entities, to simplify and unify their respective reporting formats, allowing financial institutions to reallocate resources from reporting to incident management and response.

Recommendation 4: GFMA appreciates the inclusion of recommendation four, "Implement phased and incremental reporting requirements" and recommends consultation with financial institution stakeholder representative organizations to ensure that financial authorities' phased reporting structures are unified and avoid fragmentation.

Recommendations 5 and 6: GFMA recommends that the reporting trigger allows financial institutions the time and flexibility to understand an incident's impact and whether it rises to a reporting threshold. We strongly encourage that reporting should not be triggered upon discovery. Once an institution has determined that an incident requires notification to authorities, we encourage that institutions are allowed a reasonable amount of time to notify (reporting window).

Recommendation 7: GFMA supports the suggestion to engage with financial institutions to minimize interpretation risk. In addition to providing an appropriate level of detail in setting reporting thresholds, regulators should allow for flexibility in their guidance to account for potential differences in operations and lines of business.

Recommendation 8: Recommendation eight requires further clarification as it may be read to suggest that financial authorities should reclassify reporting thresholds to capture non-material information spanning an arbitrary distance backward along the timeline of a financial institution's analysis, despite the burden imposed or the impact required early reporting might have on consumer data security.

Recommendation 9: Financial authorities should avoid imposing invasive or unnecessary reporting requirements on financial institutions. GFMA welcomes collaboration with financial authorities to confirm the strong reputation financial institutions maintain for cybersecurity standards, but review of CIR processes and procedures should be limited to

avoid excessive burden on financial firm resources.

Recommendation 15: GFMA appreciates the suggestion for financial authorities and financial institutions to collaborate to identify and implement mechanisms to proactively share event, vulnerability, and incident information and pool knowledge in collective defense of the financial sector. To that end, we hope this recommendation contemplates the need for information sharing of cyber incidents between government and financial institutions, particularly if there are potential downstream impacts to other parts of the financial sector, national security, the global economy, and/or investor confidence. Should a financial authority experience a cyber incident affecting the operations and security of systems holding sensitive private sector data, notifying the private entity would allow institutions to take proactive measures to mitigate potential attacks.

Common Terminologies for CIR
Section 4

5. Will the proposed revisions to the Cyber Lexicon help to encourage greater adoption of the Cyber Lexicon and promote greater convergence in CIR? Are there any other ways in which work related to CIR could help to encourage greater adoption of the Cyber Lexicon and promote greater convergence in CIR? Comments?

Our members applaud the efforts of the FSB for seeking to create common definitions through its cyber lexicon. It is challenging to find common definitions of words, given differing translations and associations. The FSB's efforts underscore the fact that definitions matter immensely by helping determine how we think about concepts and impacting how we act. They affect how work is done and develop the correct and reliable data on how to guide action.

We would encourage the FSB to distinguish a cybersecurity incident as a high impact incident driven by malicious intent. The criticality for early warning of a malicious cybersecurity incident has a different sense of urgency and action than a non-malicious intent technology disruption. Behind a cybersecurity incident is an intelligent threat actor with specific motives. Therefore, these incidents are treated differently from the beginning as the seek to identity and elimination of the actor is sought, to the point of reconnection where an evaluation of whether it is safe to continue business as usual is performed.

6. Do you agree with the definition of 'cyber incident' which broadly includes all adverse events, whether malicious, negligent, or accidental?

We recognize and appreciate the FSB's efforts to standardize terminology, given the vast universe of definitions of "incident" and related terms.

The FSB's Cyber Lexicon[9] defines a cyber incident as:

"A cyber event[10] that:

[9] FSB, Cyber Lexicon, https://www.fsb.org/wp-content/uploads/P121118-1.pdf, November 2018.
[10] FSB's Cyber Lexicon's definition of "Cyber Event: "Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring."

i. jeopardizes the cyber security of an information system or the information the system processes, stores or transits; or

ii. Violates the security policies, security procedures, or acceptable use policies, whether resulting from malicious activity or not."[11]

The FSB's October 2022 document proposes that "jeopardizes" be replaced by "adversely affects."

We respectfully disagree with the FSB's 2018 definition and proposed edits to "cyber incident." We understand the inclination to include data resulting from activity stemming from both malicious and non-malicious intent. However, it is by strong consensus that there be a differentiation between those incidents driven by malicious intent and those that are not. We encourage the FSB, therefore, to distinguish a cyber incident as a high impact incident driven by malicious intent because the criticality for early warning of a malicious cybersecurity incident has a different sense of urgency and action than a non-malicious operational disruption.

It is common industry terminology that a cyber event[12] occurs with non-malicious intent, such as an accidental or negligent disclosure of information. A cyber event typically receives internal classification as a technology operations incident and is often handled by different teams with different expertise.

Further, the Associations recommends removing "(ii) Violates the security policies, security procedures, or acceptable use policies, whether resulting from malicious activity or not" from the cyber incident definition. While violations of security policies, security procedures, or acceptable use policies may weaken a firm's security posture (e.g., overdue security patches, weak passwords) do not imply malicious intent.

We as an industry, agree that we should notify non-malicious high impactful incidents. Operational or technology 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.

Non-malicious incidents (i.e., operational incidents) also generally have different incident management policies, procedures, personnel, and reporting objectives when compared to a malicious cyber incident. For example, one objective to reporting operational incidents may be to alert financial authorities so other financial institutions can understand downstream impacts, whereas the objective to reporting malicious cyber incidents is to alert financial authorities of potential threat actors targeting numerous financial institutions or critical infrastructure operators. We believe, however, that the processes for both cyber and non-malicious should have a harmonized process with some key differences – such as not reporting on attribution or having a law enforcement exemption.

We would suggest that FSB, if it chooses to harmonize non-malicious events as well, consider aligning notification language with the following: Office of the Comptroller of the Currency

[12] FSB, Cyber Lexicon, https://www.fsb.org/wp-content/uploads/P121118-1.pdf, November 2018.

(OCC), Treasury; the Board of Governors of the Federal Reserve System (Board); and the Federal Deposit Insurance Corporation (FDIC) Computer-Security Incident Notification Requirements for Banking Organizations and their Bank Service Providers[13] which can result from destructive malware or malicious software (cyberattacks), as well as non-malicious failure of hardware and software, personnel errors, and other causes.

For reference and perhaps as an addition to the Cyber Lexicon, a computer-security incident is defined as an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits. The regulation further defines a "notification incident" as a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's—

(i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;

(ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or

(iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

7. Are there other terms that should be included in the Cyber Lexicon to cover CIR activities?

There are several terms we suggest be included in the Cyber Lexicon:

- Blue, White and Purple Teaming
- Computer-security incident: We recommend the FSB utilize the Federal Reserve's definition: "…an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."[14]
- Operational incidents (differentiate between cyber and operational)
- Supply chain risk
- Third-party risk

[13] The US Interagency Computer-Security Incident Notification Requirements for Banking Organizations and their bank Service Providers (November 2021) is an example of a broad-based incident notification framework.

[14] Federal Reserve: Supervision and Regulation Letters: SR 22-4/CA 22-3: Contact Information in Relation to Computer-Security Incident Notification Requirements, note 2, "https://www.federalreserve.gov/supervisionreg/srletters/SR2204.htm#:~:text=The%20final%20rule%20defines%20a%20%E2%80%9Ccomputer%2Dsecurity%20incident%E2%80%9D%20as,processes%2C%20stores%2C%20or%20transmits, March 29, 2022.

- Zero-day viruses/vulnerabilities

8. Are there other definitions that need to be clarified to support CIR?

Please find below suggested modifications of definitions for terms from the FSB's Cyber Lexicon.

- Cyber Threat
    - Current definition: A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security.
    - Suggested definition: "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."
- Information Sharing
    - Current definition: "An exchange of data, information and/or knowledge that can be used to manager risks or respond to events."
    - Suggested definition: "A voluntary exchange of data, information and/or knowledge that can be used to manage risks or respond to security incidents."
- Vulnerability Assessment
    - Current definition: "Systemic examination of an information system, and its controls and processes to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation."
    - Suggested definition: "Systematic examination of a system, product, control, or process to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation."

Format for Incident Reporting Exchange (FIRE)
Section 5

9. Would the FIRE concept, if developed and sufficiently adopted, usefully contribute towards greater convergence in incident reporting?

GFMA appreciates the common baseline the FIRE concept would provide for financial institutions to comply with reporting requirements. The FIRE concept, if developed and adopted by all financial authorities, would usefully contribute to greater convergence in incident reporting. The consultative document states that, "Authorities can decide the extent to which they wish to adopt FIRE, if at all, based on their individual circumstances." Incident reporting requirements ought to be standardized across financial authorities to avoid regulatory fragmentation. That goal may be unrealized if not all financial authorities adopt the FIRE concept.

10. Is FIRE readily understood? If not, what additional information would be helpful?

While GFMA supports the general concept of a harmonized incident reporting format, several questions remain regarding scope, form, data security and treatment, the range of participants involved, and rules governing access to information within the system. Additional information needed includes:

- The role of financial authorities in developing, implementing, and maintaining the FIRE framework.
- The "owner" of the centralized database of cyber incident reports to be made available to the private sector, if considered as part of the FIRE framework implementation.
- The data security and record keeping protocols to protect financial institutions and their customers from data breaches (malicious or otherwise).
- The authority of financial institutions to determine which financial authorities can access their reported information within the system.
- The role of financial authorities in developing, implementing, and maintaining the FIRE framework.
- Which financial authorities are interested or committed to adopting joint system as well as those that that may decline.
- Whether financial authorities will be obligated to submit information regarding their own cyber incidents through the FIRE framework to support bi-directional reporting.
- The funding source of the FIRE system maintenance.

11. If FIRE is pursued, what types of organizations (other than financial institutions) do you think would need to be involved?

We recommend the FSB consider engaging with other critical infrastructure players the financial industry relies upon, such as power and telecommunications, as potential contributors to the FIRE reporting framework.

12. What preconditions would be necessary to commence the development of FIRE?

The FSB should consider collaborating with the Associations to establish points of contact and an open line of communication with these parties to involve them in relevant decisions as the development process begins and through the implementation journey.

***

GFMA appreciates your consideration of our comments. If you would like to discuss these comments further, please reach out to Thomas Wagner at twagner@sifma.org.

Sincerely,

Allison Parent
Executive Director
GFMA
aparent@global.gfma.org

New York 140 Broadway, 35th Floor | New York, NY 10005
Washington 1099 New York Avenue, NW, Suite 600 | Washington, DC 20001

www.GFMA.org