August 20, 2018

By electronic submission to fsb@fsb.org

Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Re: FSB Consultative Document "Cyber Lexicon"

Dear Sir/Madam:

The Institute of International Finance (IIF) members appreciate the opportunity to respond to the Financial Stability Board (FSB) Consultative Document "Cyber Lexicon" ("the consultative document" or "Lexicon").[1] We also appreciate the active engagement of the FSB in the ongoing discussions among regulators, market participants and industry groups on this topic, and hope that our views will be taken into consideration in preparing the next stage of the Lexicon.

The IIF members believe that the Lexicon and its objective of reinforcing the work that the FSB, standard setting bodies (SSBs), authorities and private sector participants are undertaking to address cyber security and improve cyber resilience in the financial sector[2], is an important undertaking that will serve as a foundation for the various cyber-related industry initiatives such as the "financial sector profile", the certification of cloud providers, the homogenization of breach reporting, and the further development of cyber risk insurance.

The Lexicon is also a necessary first step towards reducing the regulatory fragmentation that we highlighted in the IIF Staff Paper – "Addressing regulatory fragmentation to support a cyber resilient global financial services industry.[3] The cross-sectoral application of the Lexicon – from

[1] See the FSB consultative document at: www.fsb.org/wp-content/uploads/P020718.pdf.
[2] Such work includes efforts to create a cross-sector common understanding of relevant cyber security and cyber resilience terminology, the assessment and monitoring of financial stability risk of cyber risk scenarios, information sharing, and the elaboration of guidance related to cyber security and cyber resilience, including identifying effective practices.
[3] See IIF Staff Paper on Addressing regulatory fragmentation to support a cyber resilient global financial services industry (May 2018) at: www.iif.com/publication/regulatory-comment-letter/iif-staff-paper-addressing-cybersecurity-regulatory

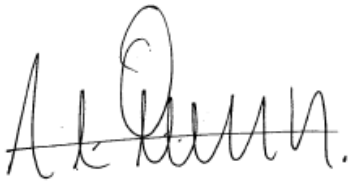
banks to insurers to financial market infrastructure – recognizes the similar impact of cyber events across the financial sector and sets forth a common framework that should help support the reduction of the number of similar, but not identical, industry cyber requirements. We encourage the FSB to work with SSBs and regional/national authorities across the financial sector to leverage the Lexicon where appropriate, and to only supplement it where needed (for instance in the alignment of existing taxonomies and the development of new ones), and to continue this important work to help further reduce regulatory fragmentation in the cyber space.

Accordingly, we fully support the FSB's work to create a common lexicon of terms related to cyber security and cyber resilience. We are concerned, however, that the proposed definitions for "cyber security" and "cyber resilience" may unintentionally intersect which makes it difficult to understand the difference between the terms and could hinder the lexicon's ability to support the work identified in the consultative document. For example, "cyber resilience" is defined to include "The ability…to adapt to changes in the environment." "cyber security", on the other hand, is the "Preservation of confidentiality, integrity, and availability of information…" It is unclear how the "ability to adapt to changes" differs from "preservation". Therefore, we encourage the FSB to include an in-depth discussion of the difference between "cyber security" and "cyber resilience" to clearly delineate the difference between those terms, which should better explain the objectives of the Lexicon.

In addition to the comments above, please find below our comments to the Consultation's specific questions.

We thank the FSB Secretariat for its consideration of our comments. If you have any questions, please do not hesitate to contact Martin Boer at mboer@iif.com or Jaime Vazquez at jvazquez@iif.com.

Sincerely,



Andrés Portilla
Managing Director, Regulatory Affairs
Institute of International Finance (IIF)

RESPONSES TO CONSULTATION QUESTIONS

Question 1*: Are the criteria used by the FSB in selecting terms to include in the draft lexicon appropriate in light of the objective of the lexicon?*

Yes, in general we think that the criteria used in selecting the terms is appropriate in the light of the objective. In particular, we support the decision to "generally" exclude technical, business and regulatory terms but that exceptions are allowed when they might have broader or multiple meanings in the supervisory context, which can create regulatory fragmentation.

We would also suggest clarifying further the meaning of "exclusion of technical terms" as the Lexicon currently includes such technical terms such as "access control"; "authentication"; "configuration management"; "Distributed Denial of Service (DDoS)"; "Recovery Point Objective (RPO)" and "Recovery Time Objective (RTO)", which is specific to Business Continuity. We have suggested that some of these terms not be included in the final Lexicon.

We would also suggest further elaborating on the "Scope" criteria to clarify that terms are included in the lexicon only where there is (or could be) a divergence or discrepancy in meanings which are material to affected parties' ability to collaborate together and reach a common understanding on implementing the objectives. Inclusion of certain key technical terms may be necessary to meet the "Scope" objective for instance given the above issue, even when such term might otherwise be excluded by applying other criteria. Conversely, applying these criteria may result in a decision that certain definitions are not required.

For example, the term "Alert" is well understood and we are not aware of any potential misunderstandings or sources of conflict in respect of this word in the cyber security or resilience context. While the choice of including this term in the Lexicon complies with the requirements of section 3.2 (e.g. that the term not be technical and not be one that only has a general business or regulatory usage), its definition does not support the objectives. Indeed, including such terms may cause greater confusion on what disparity or fragmentation issue is being resolved by including the term in the first place.

Question 2: *Are the criteria used by the FSB in defining the terms in the draft lexicon appropriate in light of the objective of the lexicon?*

Yes, we find the criteria used in defining the terms in the draft Lexicon overall to be appropriate in the light of the objective.

Given that these terms will be used in the development of new consultative guidance, standards, and rulemaking while ensuring a consistent cyber dialogue between the FSB, SSBs, authorities

and private sector participants, it is our opinion that that the terms should be defined precisely and as clear as possible.

IIF members also advise, in some instances, to include definitions from cybersecurity regulations where the source is different from those mentioned in the Cyber Lexicon, such as from the European Central Bank. Including some of their terms and definitions would help make the Lexicon more globally representative.

That said, while we support inclusion of diverse sources, this should not undermine the internal coherence of the lexicon. Clearer references to other defined terms within the proposed definitions will ensure a better overall framework (with hierarchies and subsets of terminology where required).

We would also suggest that where contractions are used, they are defined with a reference to the original long form term in order to ensure accurate definitions.

Question 3: *In light of the objective of the lexicon, should any particular terms be deleted from, or added to, the draft lexicon?*

We propose to include the following terms:

Term	Definition
Advanced Persistent Threat	An advanced persistent threat (APT) is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time. Source: ISACA
Anomalous Activity	The process of comparing activity that is considered normal against observed events to identify significant deviations; or, activity that deviates from normal. Source: Adapted from the FFIEC IS Handbook
Attack Vector	An attack vector is a path or means by which a malicious actor can gain access to a computer or network server in order to deliver a desired outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element. Source: eforensics magazine
Compensating Control	A management, operational, and/or technical control (e.g., safeguard or countermeasure) employed by an organization in lieu of a recommended security control used to lessen the risk of an Information System. Source: Adapted from the FFIEC IS Handbook

Term	Definition
Control	The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature. Source: FFIEC IS Handbook
Crisis Management	The plans and actions taken to protect and defend the reputation of the organization, its brand and its products/services. An institution's ability to communicate with employees, customers, and the media, using various communications devices and methods, is a key component of crisis management.
Cyber Kill Chain	A kill chain is used to describe the various stages of a cyber-attack used for identification and prevention of cyber intrusions. The steps in a kill chain trace the typical stages of a cyber-attack from early reconnaissance to completion where the intruder achieves exploitation and data exfiltration. Source : Adapted from Lockheed Martin Cyber Kill Chain Framework
Cyber-Physical System	Cyber-Physical Systems or "smart" systems, are co-engineered interacting networks of physical and computational components. These systems provide the foundation of critical infrastructure, form the basis of emerging and future smart services, and improve quality of life in areas such as personalized healthcare, traffic flow management and emergency response. Source : Adapted from NIST
Cyber Resillience	The ability of an organization to continue to carry out its mission in the presence of actual or threatened stress or disruption to its information systems. Source: Adapted from the definition of "Operational Resilience" in CERT Glossary. Alternatively, see NIST glossary definition of "Information System Resilience".
Cyber Risk Management	The continuous process of identifying, analyzing and addressing cyber risk to an organization that could adversely affect the operations and delivery of services, including: (1) risk assessment, (2) implementation of a risk mitigation strategy including risk transfer, and (3) employing techniques and procedures for the continuous monitoring of the security state of the information system. Source: Adapted from CERT Glossary and NIST Glossary
Cyber Threat	Any circumstance or event with the *potential* to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the

Term	Definition
	Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Source: Adapted from US NIST
Incident Management	The process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences Source: Adapted from the FFIEC IS Handbook
Information and Communication Technology (ICT)	The use of computers and other electronic equipment and systems to collect, store, use, and send data electronically. Source: Adapted from CPMI-IOSCO
Information System	A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems. Source: New York DFS Cybersecurity Requirements For Financial Services Companies
Intrusion Detection	Techniques that attempt to detect unauthorized entry or access into a computer or network by observation of actions, security logs, or audit data; detection of break-ins or attempts, either manually or via software expert systems that operate on logs or other information available on the network. Source: Adapted from the FFIEC IS Handbook
Software problem/ system failure	Malfunctions of applications or basic software programs/ Performance degradation of services. Source: Adapted from ECB (European Central Bank, Annex B – Reporting Significant Cyber Incidents (2017)
Third Party Service Provider	Any entity that enters into a business arrangement with a financial institution that permits the outsourcing of activities that the institution itself is authorized to perform (e.g.,technology service provider) Also known as Third Party Vendor. Source: FFIEC IS Handbook
Traceability	The ability to create, record and preserve data about events generated, executed or actioned directly by an information system, or the results of an action carried out by a user of an information system. Source: Adapted from The Business Dictionary

Generally, IIF members find the current terms in the Lexicon to be helpful but would further suggest removing the following terms:

- **Campaign:** The definition is not necessarily the commonly understood usage of the term in information security.
- **Configuration Management:** this term relates to IT, but not to Cyber Security.
- **Continuous Monitoring:** This is a common phrase, not a term.
- **Course of Action:** Technical and commonly used.

Question 4: *Should any of the proposed definitions for terms in the draft lexicon be modified?*

We propose to modify the following definitions:

Term	Current Definition	Proposed Definition
Availability	Property of being accessible and usable on demand by an authorised entity.	Property of information (or an information system) that it is accessible on demand.
Reasoning: availability has a different meaning than usability, hence we suggest removing the term "usable". In addition, an unauthorized entity could access information that is available, the concept of authorization should not be included in the definition.		
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities or processes.	Property that information or data (whether discrete or in whole) that should not be made available or disclosed (except in a permitted manner or form) to unauthorized individuals, entities, processes *or systems*.
Reasoning: Addition of "system" for completeness. Confidentiality is generally considered to mean ensuring the right person has the right access to the right data and preventing any other combination of these three factors. Therefore definition needs to refer to right information (i.e. information can include subsets), right access (i.e. there are different types of access, such as		

Term	Current Definition	Proposed Definition
read-only, vs ability to edit), and right person (already included by use of the word "unauthorised").		
Cyber **(Change the term to Cyberspace)**	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.	**Change the name of the term to "Cyberspace"** : A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Source: NIST "Glossary of Key Information Security Terms". Definition taken from CNSSI-4009
Reasoning: The term "Cyberspace" is more technical, accurate, and informative than the lexicon's definition of "cyber", while still getting at the main point that cyber/cyberspace is about the interaction of these systems and processes within a certain domain.		
Cyber Incident	A cyber event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies -- whether resulting from malicious activity or not.	A cyber event that actually jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies -- whether resulting from malicious activity or not.
Reasoning: We propose removing the word "potentially" from the definition. Given that Cyber Event is used to describe potential attempts, Cyber Incident should be used for successful attempts to circumvent security controls.		
Cyber Risk	The combination of the probability of cyber events occurring and their consequences.	*Any type of risk resulting of the likelihood of cyber events occurring and their impact emanating from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity*

Term	Current Definition	Proposed Definition
		incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – being related to individuals, companies, or governments. *Source: IAIS (2016) Issues Paper on Cyber Risk to the Insurance Sector*
Reasoning: Modifying the definition to better specify what cyber risk is.		
Data Breach	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to protected data transmitted, stored or otherwise processed.	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to confidential data transmitted, stored or otherwise processed.
Reasoning: 'Confidential data' should be used rather than 'Protected data', in particular as protected data itself is not defined.		
Detect	Develop and implement the appropriate activities to identify the occurrence of a cyber event	To identify the occurrence of a cyber event
Reasoning: Detect is unrelated to "develop and implement".		
Identify	Develop the organizational understanding to manage cyber risk to systems, assets, data and capabilities.	Develop the organizational understanding to manage cyber risk to *assets*.
Reasoning: For simplification, given the definition of "Asset" already includes people, information, infrastructure, finances and reputation.		
Incident Response Team (IRT) [commonly known as CERT or CSIRT]	Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle.	Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle and that might also organize activities such as education and auditing to improve security quality.

Term	Current Definition	Proposed Definition
Reasoning: Members such as analysis, education, and auditing are to be included in CSIRT. Source: the Nippon CSIRT Association (NCA, which is the organization to cooperating among CSIRT in Japan beyond industries).		
Indicators of Compromise	Evidence of an intrusion that can be identified in an information system.	Indicators of Compromise (IOC) consists of forensic data observed on a network or in an operating system that indicate a computer intrusion. Typical IOCs are virus signatures and IP addresses, MD5 hashes of malware files, or URLs or domain names of Command and Control servers.
Reasoning: Important term used by regulators, for example regarding information sharing. Source : Adapted from SANS InfoSec Reading Room		
Information Sharing	An exchange of data, information and/or knowledge that can be used to manage cyber risks or respond to cyber incidents.	An exchange of data, information and/or knowledge that can be used to identify, detect, respond to or manage cyber events or cyber incidents or generally reduce cyber risk.
Reasoning: More specific and uses defined terms. Information sharing in respect of identifying and detecting risks should be emphasised. Note we use lower case "detect" as in this context this relates to more than just identifying a cyber event; it covers any information which may relate to a cyber event or cyber risk.		
Protect	Develop and implement the appropriate safeguards to ensure delivery of services.	Maintaining the confidentiality, availability and integrity of data.
Reasoning: Protect is unrelated to "develop and implement". Protection is wider than delivery of services. To make the definition more complete than only referring to "delivery of services".		
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber event."	To restore any capabilities or services that were impaired due to a cyber event."

Term	Current Definition	Proposed Definition
Reasoning: The current definition is adapted from the Recover Function in the NIST Framework. The Recover Function includes three categories: Recovery Planning (RC.RP), Improvements (RC.IM), and Communications (RC.CO). The latter two Categories of the Recover function in particular include actions beyond what is typically considered as to "recover" in terms of existing regulatory requirements (i.e. the 2hr RTO). (For example: "Recovery plans incorporate lessons learned" (RC.IM-1), "Recovery strategies are updated" (RC.IM-2), and "Reputation is repaired after an incident" (RC.CO-3) – it would not be realistic to complete these in two hours.) Therefore, the proposed revision brings the definition of "recover" in line with that used in the CPMI-IOSCO cyber guidance. This would not preclude jurisdictions from developing guidance or standards re: recovery planning and other activities that are contemplated within scope of the NIST Recover Function.		
Recovery Point Objective (RPO)	Point to which information used by an activity is restored to enable the activity to operate on resumption.	Point in time to which information used by an activity is intended to be restored to enable the activity to operate on resumption.
Reasoning: The RPO is set to a point in time and is set in advance as an objective for intended restoration.		
Recovery Time Objective (RTO)	Period of time following an incident within which a product or service or an activity is resumed, or resources are recovered.	Period of time following a cyber incident within which a product or service or an activity is intended to be resumed, or resources are intended to be recovered.
Reasoning: The Lexicon defines recovery in terms of cyber events, not incidents. RTO definition should be updated to maintain its consistency.		
Respond	Develop and implement the appropriate activities to take action regarding a detected cyber event.	Execution of the appropriate activities regarding a Detected Cyber Event.
Reasoning: Respond is separate to "develop and implement". While RPOs and RTOs are set in advance for material Cyber Incidents, the definition of Respond should apply to Cyber Events, as, once unusual Cyber Events are Detected, an appropriate Reponse may be to escalate / investigate.		
Social Engineering	A general term for trying to deceive people into revealing confidential information or performing certain actions.	A general term for trying to deceive people into revealing information or performing certain actions.
Reasoning: Information does not need to be confidential for social engineering to occur.		

Question 5: *Going forward and following the publication of the final lexicon, how should the lexicon be maintained to ensure it remains up to date and a helpful tool?*

We believe the success and utility of the Lexicon can only be obtained if:

- The number of terms is contained, relatively short and within the defined scope.
- The Lexicon is updated periodically with new or updated terms where misunderstandings, misinterpretations, etc. are being identified.
- There is a balanced group of stakeholders from regulators, supervisors, governments and industry representatives that can keep it current and contribute with terms used in different geographies.
- It is key that the FSB coordinates with other SSB's so that they try to align definitions within this Lexicon within their own domestic rules, regulations and guidelines.
- Similarly, the organizations or standard setting bodies that are quoted as the source of reference should be informed that the FSB Cyber Lexicon referenced their work. In providing this notification, the FSB should request that they inform the FSB of any change(s) to these definitions, to ensure the Cyber Lexicon remains aligned with new standards and market developments.

In our opinion, the Lexicon, once published, should be maintained by the FSB, if possible, and updated annually. Those updates should ideally:

- Take input from both the public and private sector in the light of the issues identified during their work on cyber-related initiatives.
- Be subject to a short consultation period.
- Take into consideration the criteria for limiting the scope described in the consultative paper, so that the Lexicon only include a reasonable and small amount of terms.

The FSB might also consider issuing FAQ's in the periods between updates to help address any potential conflicts or other issues notified to it when using the Lexicon.