Ashley Beaudry
Senior International Policy Analyst

August 20, 2018

Financial Stability Board
Centralbahnplatz 2
CH-4002 Basel
Switzerland
via fsb@fsb.org

Re: FSB Cyber Lexicon Consultative Document

To Whom It May Concern:

The American Council of Insurance Insurers (ACLI) is pleased to respond to the Financial Stability Board's (FSB) Cyber Lexicon Consultative Document (Lexicon). We thank you for the opportunity to submit these comments.

ACLI represents approximately 290-member companies dedicated to providing products and services that contribute to consumers' financial and retirement security. ACLI members represent 95 percent of U.S. industry assets, offering life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, dental and vision and other supplemental benefits.

We strongly support the objective of a lexicon aiding in a "cross-sector understanding of relevant cyber security and cyber resilience terminology." Financial services companies believe the most effective way to protect their customers' personal information and information technology systems is to employ cybersecurity frameworks that are risk-based, flexible, and workable. Overall, ACLI applauds the FSB's efforts to develop a Lexicon that meets these objectives. However, as the FSB relied on existing sources for the development of the Lexicon, there are several definitions which need further attention to ensure a comprehensive, coherent document which is less prescriptive and more flexible.

Definitions for Modification

Asset

ACLI recommends the definition of "asset" be changed to the following:

> *Asset: means 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.*

ACLI is aware that the FSB has looked to many existing standards to help inform its terminology; however, in this instance, the FSB definition is entirely too broad. Including "intangible" information or sources in a definition would add a level subjectivity which would make the definition broad

enough to encompass almost everything. The most effective cyber risk management systems allow for segmentation and for higher protection for more sensitive information or systems. ACLI does not think there is much value in treating all information assets equally.

To alleviate these concerns, ACLI proposes a definition used the U.S. National Association of Insurance Commissioners (NAIC) Data Security Model Law and New York State's Cybersecurity Requirements for Financial Services Companies. This definition provides a risk-based, flexible, and scalable definition that could be appropriately tailored for insurers.

Availability

ACLI recommends the definition of "availability" be changed to the following which is adapted from ISO and NIST:

> *Availability: Enabling timely and reliable access to authorized users (people, processes or devices) whenever it is needed*.

Confidentiality

Although ACLI agrees with the intent behind the current definition of confidentiality, the language is confusing and may present challenges to understanding the intent if not written in the reader's primary language. ACLI would instead recommend using the NIST definition which reads as follows:

> *Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*

Configuration Management

ACLI would suggest editing the definition of Configuration Management to remove the very terms the FSB is trying to define from the definition.

One possible alternative is the ITIL framework definition, which reads:

> *Configuration Management: The process responsible for ensuring that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets.*

To avoid confusion with the FSB definition of "asset," a replacement of the word "asset" in the ITIL definition above with "information system" would be acceptable.

Another alternative comes from the ICASA paper on Configuration Management in which the term means "*the process for recording and updating information that is related to the information technology infrastructure.*"

Cyber

ACLI recommends the definition of "cyber" be changed to the following:

> *Cyber: Relating to, within, or through the medium of information technology.*

Cyber Event and Cyber Incident

As currently written, the Lexicon defines Cyber Event and Cyber Incident as follows:

> *Cyber Event: Any observable occurrence in an information system. Events sometimes provide indication that a cyber incident is occurring.*
>
> *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 or security policies, security procedures or acceptable use policies – whether resulting from malicious activity or not.*

The Lexicon notes these two definitions as being adapted from their respective NIST definitions. However, in reality, ACLI would submit that the Lexicon's definition of "Event" is broader than that of NIST which defines it as "*A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).*" In practicality, the Lexicon's definition does not limit "event" to only those occurrences which could impact operations and would not be risk-based or workable.

NIST also defines "Incident" more narrowly to read, "*A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.*" The Lexicon's definition of "Incident" is actually a conglomeration of NIST's "event" and "incident" language as it includes both potential and realized impacts.

ACLI would propose the FSB edit the Lexicon's definitions to more accurately reflect the NIST definitions' separation of possibility and actuality. This in turn would provide greater clarity and coherence to other definitions within the Lexicon which are also adapted from NIST and rely on the definition of "event." Should the FSB decide not to edit these definitions, ACLI would recommend updates to the language in the definitions of "cyber risk," "cyber threat," "detect," "recover," and "respond" to refer to cyber incident rather than the overly broad definition of cyber event.

Furthermore, ACLI would recommend the FSB look to the NAIC definition of "cybersecurity event[1]" for its definition of "cyber incident[2]". The NAIC language provides the appropriate caveats of circumstances when unauthorized access is not an incident and would not require further action by the companies and/or regulators.

[1] "Cybersecurity Event" means an event resulting in unauthorized access to, disruption or misuse of, and Information System of information stored on such Information System.

The term "Cybersecurity Event" does not include the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization.

Cybersecurity Event does not include an event with regard to which the Licensee has determined that the Nonpublic Information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

[2] ACLI recommends the NAIC definition be in place of incident, rather than event in the FSB Lexicon because it is referring to actualized impact rather than possible impact. This would also keep it in line with the NIST Framework while provide greater clarity.

Cyber Resilience

ACLI recommends the definition of "cyber resilience" be changed to the following which is adapted from the definition of "Operational Resilience" in the CERT Glossary:

> *Cyber Resilience: 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.*

Cyber Risk

ACLI recommends the definition of "cyber risk" be changed to the following which is adapted from the IAIS (2016) Issues Paper on Cyber Risk to the Insurance Sector:

> *Cyber Risk: Any type of risk emanating from the use of electronic data and its transmission, including technology tools such as the internet, information systems and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity 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.*

Cyber Threat

In line with our comments on "cyber event" and "cyber incident," should those definitions not be modified, ACLI recommends changing the definition of "cyber threat" to be as follows:

> *Cyber Threat: A circumstance or cyber incident with the potential to intentionally or unintentionally exploit one or more vulnerabilities, resulting in a loss of confidentiality, integrity or availability.*

Detect

In line with our comments on "cyber event" and "cyber incident," should those definitions not be modified, ACLI recommends changing the definition of "detect" to be as follows:

> *Detect: Develop and implement the appropriate activities to identify the occurrence of a cyber incident.*

Integrity

ACLI recommends the definition of "integrity" be changed to the following NIST definition:

> *Integrity: Guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity.*

Recover

In line with our comments on "cyber event" and "cyber incident," should those definitions not be modified, ACLI recommends changing the definition of "recover" to be as follows:

> *Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that we impaired due to a cyber incident.*

Respond

In line with our comments on "cyber event" and "cyber incident," should those definitions not be modified, ACLI recommends changing the definition of "respond" to be as follows:

> *Respond: Develop and implement the appropriate activities to take action regarding a detected cyber incident.*

Definitions for Addition

Attack Vector or Threat Vector

The FSB should consider adding a definition for "attack vector" or "threat vector." Both terms are well-used, often interchangeably, to describe the following:

> *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. Vectors enable hackers to exploit systems.*

Control

ACLI proposes the FSB add the following definition for "control" from the CERT Glossary:

> *Control: Methods, policies and procedures – manual or automated – that are adopted by an organization to safeguard assets and protect the confidentiality, availability and integrity of information.*

Risk Management

The following definition for "Risk Management" from the CERT Glossary and NIST should also be added:

> *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.*

Definitions for Deletion

ACLI recommends the deletion of the term "campaign" since it is not commonly used as term in information security.

"Course of action" should also be removed; this is a technical term and thereby at odds with the FSB's stated criteria for the Lexicon.

Finally, ACLI recommends the deletion of the term "data breach." This definition is redundant with cyber incident in its current form and unnecessary.

ACLI would welcome the opportunity to discuss our concerns about the FSB Cyber Lexicon Consultative Document. We thank you for your consideration.

Sincerely,

Ashley Beaudry
Senior International Policy Analyst
American Council of Life Insurers