American Insurance Association

555 12th Street, NW
Suite 550
Washington, DC 20037
202-828-7100
Fax 202-293-1219
www.aiadc.org

August 20, 2018

Financial Stability Board
Basel, Switzerland

VIA Electronic Mail: fsb@fsb.org

RE: Public Consultation on the Cyber Lexicon

The American Insurance Association (AIA) appreciates the opportunity to provide comments on the Financial Stability Board's (FSB) draft Cyber Lexicon (Lexicon). AIA is the leading trade association for the U.S. property-casualty insurance industry. AIA's members write all types of property-casualty insurance, and our membership is comprised of more than 330 companies, collectively writing more than $134 billion in premiums each year. Our members are physically present in over seventy countries, and serve customers in over one-hundred and seventy countries and territories around the world.

Data security is a priority issue for the insurance industry, and as such, insurers devote considerable resources to protect data, information systems, and consumer trust. As international standard-setting bodies and authorities develop supervisory regulations and guidance, we support efforts for global harmonization, to the extent possible. As such, we have a keen interest in the FSB's work and, in particular, the effort to develop a Cyber Lexicon to promote a consistent base-line understanding of key cybersecurity terms to support the FSBs work streams moving forward.

Additionally, the property-casualty insurance industry has a unique voice in the cybersecurity dialogue. Our industry offers cyber insurance products that can serve as a beneficial risk transfer mechanism. Importantly, the guidance identifies the limited purpose of the Lexicon and that it is not intended for use in legal interpretations of any international arrangement or agreement or any private contract. Cyber insurance products are private contracts and this stage of development, insurance options should not be stifled or constrained by any forced standardization, which might only serve to limit innovation and product offerings that insurers are developing to meet the needs of our clients and the ever evolving and dynamic nature of the information security risks. As correctly identified in the FSB description, it should be up to the private party, in this case the insurer, to determine if, and how, to utilize the Lexicon for their market purposes.

We offer specific recommendations for the terms included, or to be included, in the Lexicon from our perspective as companies managing operational cyber risks.

Proposed Amendments to Proposed Lexicon

"Availability" - Using ISO and NIST as resources we propose the following more descriptive definition: "Enabling timely and reliable access to authorized users (people, processes or devices) whenever it is needed."

"Campaign" – We recommend deleting this term.

"Confidentiality" – Since the current definition focuses on "property" and the understanding of "property" can have varying interpretations, we recommend using NIST as a reference to define Confidentiality. AIA recommends: "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."

"Course of Action" – We recommend deleting this term.

"Cyber" – The FSB may consider whether such a detailed definition is necessary or whether it is sufficient to state that cyber is "Relating to, within, or through the medium of the information technology."

"Cyber Incident" – Given that the definition is talking about an "incident" there is an inherent suggestion that this is something concrete. For this reason and because a broad definition in a regulatory context could take-away from a risk-based assessment we recommend the following: "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."

"Cyber Resilience" –Promoting consistency with the term, "operational risk" in the CERT Glossary we offer the following for your consideration: "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" - This is an important definition in the lexicon, one which some supervisory authorities have already defined. In borrowing from the U.S. perspective we offer a risk-based definition for your consideration. In a supervisory context, we believe that the element of risk is an important one and should not encompass the idea of remote probabilities, which is overly broad and could promote inefficient risk management. Our proposed definition is as follows: "An actual risk emanating from unauthorized access to, interruption of, or misuse of, an Information system or non-public information stored on such Information System."

"Data Breach" – We suggest amending this definition as follows: "Compromise of security that leads to the ~~accidental or unlawful destruction, loss, alteration,~~ unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed.

"Integrity" – Using NIST as a resource we suggest: "Guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity."

"Incident Response Team" (IRT) – We offer the following recommendation, "Team of appropriately skilled ~~and trusted~~ members of the organization that handles incidents during their life cycle."

<u>Additional Terms to Consider</u>

While we do not have specific definitions to propose, we do recommend considering adding definitions for Attack Surface and Attack Vector. These are terms that can often have different understandings or interpretations, but in order to ensure there is consistency in identifying risk, we believe the Lexicon would benefit from the inclusion of these terms.

Including a definition of Control may also be helpful to encourage consistency in communication and understanding. We recommend using a definition derived from CERT as follows: “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.”

Additionally, there would be benefit in clarifying what is understood by “cyber warfare” and “cyber terrorism.” There is currently no definition in the Lexicon for these terms, yet there may be varying interpretations among jurisdictions and even between how the media may describe an incident verse how an institution or supervisory authority may understand the incident. A consistent global base-line understanding would be beneficial.

“Risk Management” is a term that is often referred to in the context of cyber discussions and as such we recommend using CERT and NIST to add the following definition to the Lexicon – “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.

****

AIA appreciates the opportunity to provide feedback and welcomes the opportunity to answer any questions you may have.

Respectfully submitted,

Angela Gleason

Angela Gleason
Senior Counsel