Via E-Mail (fsb@fsb.org)

20 August 2018

Financial Stability Board
Bank for International Settlements
CH-4002 Basel, Switzerland

RE: FSB Consultation on Cyber Lexicon

The Global Association of Central Counterparties ("CCP12") welcomes the opportunity to provide its response on behalf of our membership to the Financial Stability Board ("FSB") Cyber Lexicon consultative document. The CCP12 is a global association of 36 major organisations, which operate more than 50 central counterparties ("CCP") in the EMEA region, Asia-Pacific and the Americas. CCP12 was formed to share information, develop analyses and policy standards for common areas of concern. CCP12 members work toward the common purpose of creating conditions in which global CCP solutions can emerge to meet the needs of the marketplace.

A high priority of our membership is to maintain the confidentiality, integrity, availability, and performance of the systems upon which they rely and one in which significant resources have been invested. We therefore appreciate the engagement that FSB has taken to promote harmonisation between the regulators, standard setting bodies, and market participants on this topic.

CCP12 is supportive of the FSB's objective of developing a cyber lexicon as it is very helpful as an industry to have a consistent set of terminology considering our shared objectives of managing cybersecurity risk. CCP12 agrees that the development of the lexicon should draw on the extensive work that has been previously done; especially, the work of International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) in its glossary of key information security terms. The set of industry standards and best practices included in the NIST Cybersecurity framework are widely used to help organisations manage cybersecurity risk and already contribute to developing a common language on critical infrastructure cybersecurity globally.

CCP12's primary concern is that where the definitions selected for the terms were drawn from several different sources (e.g., ISO, NIST, CPMI-IOSCO) or were modified from the original source; the definitions could inherently vary in their interpretation from source to source. This may result in an inconsistency throughout the lexicon. CCP12 recommends that where any modifications were made to the definitions as they were listed in the original source, the FSB should ensure that the original connotation and essence is not altered, remains valid, and continues to foster a common understanding of the relevant cyber security and cyber resilience terminology across the global financial sector.

CCP12 recommends that where any inconsistencies were observed in the original sources and where any unification of terms would be deemed helpful, FSB should provide feedback into the relevant organisations accordingly.

CCP12 Comments

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? (See Section 2 for the objective, Section 3.2 for the criteria and the Annex for the lexicon.) Should additional criteria be used?*

The focus on proposing common definitions for a core set of terms relevant to financial sector participants seems appropriate in light of the objective of the lexicon.

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? (See Section 3.3 for the criteria.) Should any additional criteria be used?*

CCP12's primary concern is that where the definitions selected for the terms were drawn from several different sources (e.g., ISO, NIST, CPMI-IOSCO, ISACA) or were modified from the original source; the definitions could inherently vary in their interpretation from source to source. This may result in an inconsistency throughout the lexicon. CCP12 recommends that where any modifications were made to the definitions as they were listed in the original source, the FSB should ensure that an unintended disjointed list is not created and that the original connotation and essence is not altered, remains valid, and continues to foster a common understanding of the relevant cyber security and cyber resilience terminology across the global financial sector.

Question 3. *In light of the objective of the lexicon, should any particular terms be deleted from, or added to, the draft lexicon? If any particular terms should be added, please suggest a definition, along with any source material for the definition and reasons in support of inclusion of the term and its definition.*

CCP12 proposes including some new terms considering that the lexicon defines "Threat Actor" without defining Threat and "Red Team Exercise" without defining "Red Team"

Suggested Definitions:

- **Red Team** - A group of people authorised and organised to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

- **Threat** – Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations, or nation state. Source: https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

- **Threat Objective** – The end goal or action pursued by any combination of threat actors, vectors, and methods.

- **Threat Objective Lifecycle** – A high-level risk assessment and cybersecurity strategy prioritisation approach that focuses on adversary objectives rather that identities, actors, tools, techniques, or vectors. The threat objective lifecycle methodology defines a small number of specific actions such as sabotage, extortion, or fraud and is useful for Board-level discussion on the areas of focus for a cybersecurity strategy.

CCP12 proposes other terms that to include that would fit the definition of core set of terms:

- **Authorisation** – *Access privileges granted to a user, program, or process or the act of granting those privileges.*
  Source: *https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf*

- **Data Security** - *Protection of data from unauthorised (accidental or intentional) modification, destruction, or disclosure.*
  Source: *https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf*

- **Resilience** – *The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning.*
  Source: *https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf*

- **Risk Assessment** – *The process of identifying risks to organisational operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations.*
  Source: *https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf*

- **Intrusion** – *Unauthorised act of bypassing the security mechanisms of a system.*
  Source: *https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf*

Question 4. *Should any of the proposed definitions for terms in the draft lexicon be modified? If so, please suggest specific modifications, along with any source material for the suggested modifications and reasons in support thereof.*

Information System
The definition of Information System is very broad and can be modified to explicitly include software programs as well as related manual procedures and requirement documentation.

- **Information System -** Set of applications (hardware and software systems), services, information technology assets or other information-handling components, including related manual procedures and system requirements.

Penetration Testing
The definition of Vulnerability Assessment is at a different level of detail from a Penetration Test (which enumerates and attempts to actively exploit vulnerabilities). The definitions do not lead to a clear understanding of the differences. As such we provide an alternative definition for Penetration Testing:

- **Penetration Testing** – *A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.*
  Source: https://csrc.nist.gov/Glossary/?term=523#AlphaIndexDiv

Situational Awareness

Regarding the definition of Situational Awareness it is not very clear as to why it has been defined in this manner. Given it is a military term that has been co-opted for Security Operations, it is suspected that a clearer definition would assist in the overall understanding of the term to a broader audience. As such, we propose an alternative definition:

- **Situational Awareness** – *Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.*
  Source: https://csrc.nist.gov/Glossary/?term=1448#AlphaIndexDiv

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 too?*

CCP12 encourages the FSB to limit the lexicon to "core" terms only, which will limit the need to update the lexicon more frequently. Additionally, the FSB should engage participants through a consultative process on a regular basis to ensure that the list of "core" terms included remains current (up-to-date) and relevant. CCP12 also recommends that where any inconsistencies were observed in the original sources and where any unification of terms would be deemed helpful, FSB should provide feedback into the relevant organisations accordingly.

Sincerely,

Marcus Zickwolff,
CEO of CCP12