August 2018

London Stock Exchange Group response to the FSB Cyber Lexicon Consultative Document

General remarks

London Stock Exchange Group (LSEG) is delighted to have the opportunity to comment on the draft FSB Cyber Lexicon.

As one of the largest operators of safe, efficient and diversified international financial market infrastructures (FMIs), LSEG has been undertaking prudent risk management across all operational risk areas including cyber resiliency. We recognise that cyber resilience can be a determining factor in the overall resilience of the financial system and broader economy. Due to the interconnectedness of FMIs, cyber attacks in the financial sector have the potential to create widespread financial instability. For this reason, we fully support the policymakers and the industry's ongoing efforts to enhance cyber resiliency and help raise the bar for the whole financial industry and wider economy.

We welcome the FSB's approach to reference the majority of the definitions from the existing ones defined by the leading authorities and institutions. We believe this facilitates the consistency and harmonisation of cyber security and cyber resilience terminology across jurisdictions.

Response to questions

Q1. 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?

Q2. 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?

Q3. 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.

We would suggest adding the definition of "Information Security" in the cyber lexicon as references to this concept are made multiple times in other definitions (e.g. "continuous

monitoring", "defence in depth"). We believe that it would be important to include such definition in order to understand clearly the interconnectedness with cyber security.

With the above reasoning, we would like to suggest adding the following definition:

- *Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.*

  Source: NIST SP 800-39

Q4. 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.

In line with the consistency criteria outlined, we would like to suggest modifications (underlined) to the following definitions:

- *"Information Security Continuous Monitoring": Maintaining ongoing awareness of information security, vulnerabilities and threats to support organisational risk management decisions.*

  Source: NIST 800-150, Appendix B (citing NIST 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, Sept. 2011)

- *"Cyber Incident": The result of 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.*

  We consider the current definition of cyber incident partially overlaps with the one of "cyber event". In this regard we believe it is important that the definition of cyber incident reflects the fact that it is the actual consequence of a cyber event.

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

  We understand that this definition includes both *unintentional and intentional threats* and would suggest adding a standalone definition of intentional threats (i.e. cyber attacks) in the Cyber Lexicon:

"Cyber Attack": An attempt to exploit one or more vulnerabilities, resulting in a loss of confidentiality, integrity or availability.

In addition, we would like to note our welcome to the FSB reference to the CPMI-IOSCO on such definitions. However, we would suggest enhancing the definition by specifying the subjects of which their "confidentiality, integrity or availability" are impacted.

- *"Cyber Security":* ~~*Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium.*~~ *The process of protecting information by preventing, detecting, and responding to attacks.*

  Source: Adapted from NIST Framework

Q5. 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 that an annual check and update of existing sources would be helpful in light of the FSB objectives.