FSB FINANCIAL STABILITY BOARD

12 November 2018

Cyber Lexicon

Overview of Responses to the Public Consultation

Introduction

On 2 July 2018, the Financial Stability Board (FSB) published a consultative document – *Cyber Lexicon* – that set forth a draft cyber lexicon for public comment. The objective of FSB work to develop a cyber lexicon is to support the work of the FSB; standard-setting bodies (SSBs), including the Basel Committee on Banking Supervision (BCBS), Committee on Payments and Market Infrastructures (CPMI), International Association of Insurance Supervisors (IAIS) and International Organization of Securities Commissions (IOSCO); authorities; and private sector participants, e.g. financial institutions and international standards organisations, to address cyber security and cyber resilience in the financial sector. The lexicon is not intended for use in the legal interpretation of any international arrangement or agreement or any private contract. The consultative document indicated that a lexicon could be useful to support work in the following areas:

- Cross-sector common understanding of relevant cyber security and cyber resilience terminology;
- Work to assess and monitor financial stability risks of cyber risk scenarios;
- Information sharing as appropriate; and
- Work by the FSB and/or SSBs to provide guidance related to cyber security and cyber resilience, including identifying effective practices.

The FSB received 29 responses to the public consultation from individual financial institutions; industry associations and other groups representing participants and service providers in the financial and other sectors, including banks, insurers, asset managers, exchanges, retirement plan providers and information technology and telecommunications firms; and consultants and individuals.[1] Respondents generally welcomed the consultative document and supported the FSB's work to develop a Cyber Lexicon for the financial sector and the objectives of the work.

[1] The comment letters are published on the FSB's website except when a respondent requested confidential treatment: http://www.fsb.org/2018/08/public-responses-to-the-cyber-lexicon-consultative-document/.

This note summarises the issues raised in the public consultation and sets out the main changes that have been made to the lexicon to address them.

Summary of Main Issues

Criteria for Selecting Lexicon Terms: General

Respondents generally supported the criteria used to select terms included in the draft lexicon. Three respondents expressed the view that the criteria resulted in terms that, overall, are generic and not related specifically to the financial sector and its activities. While the focus of the lexicon is on cyber-related terms that are relevant to the financial sector and useful to support work undertaken by the FSB and SSBs, as well as financial sector regulators, supervisors and private sector participants, there may be considerable overlap between terms that are relevant and useful in the financial sector and those that are useful in other sectors. Indeed, this overlap has the potential to enhance communications across the financial and other sectors. Therefore, we have clarified that while the terms selected for the lexicon are relevant to the financial sector, the lexicon does not exclude terms that also may be relevant to other sectors.

Criteria for Selecting Lexicon Terms: Exclusion of Technical Terms

Three respondents suggested clarifying the criteria that technical terms should generally be excluded to explain the inclusion of certain terms (e.g. *Access Control*, A*uthentication*, *Configuration Management*, *Distributed Denial of Service*, *Recovery Point Objective* and *Recovery Time Objective*). Two respondents questioned whether certain technical terms should be removed from the lexicon. The following terms have been removed from the final lexicon: *Authentication*, *Configuration Management*, *Recovery Point Objective* and *Recovery Time Objective*. The line between terms that are strictly technical and terms that are useful both within and outside of the technical sphere is not always clear, however, and some terms that may be considered technical, such as *Access Control*, *Denial of Service* and *Distributed Denial of Service*, have been included because the FSB determined that they were likely to be useful in meeting the objectives of the lexicon.

Criteria for Selecting Lexicon Terms: Additional or Enhanced Criteria

- ***Root Terms.*** Two respondents suggested adding a criterion to include "root" terms upon which other cyber relevant terms are built, even when a term might otherwise conflict with stated exclusionary categories related to business, regulatory and technical terms. Having considered all the specific additional terms suggested by respondents, the FSB concluded that it was not necessary to add this criterion in order to appropriately develop the final lexicon.
- ***Attack Methods and Mitigation Options.*** Two respondents suggested the addition of a criterion to include terms suitable for describing attack methods and mitigation options. This criterion has not been added because, consistent with the objective of the lexicon, a determination was made that terms generally would not be included in the lexicon where they are principally related to the areas of law enforcement or national security rather than to financial sector regulation or supervision. In addition, some of the suggested terms in this area (e.g. different types of *Cyber Incidents*) are too granular for inclusion in a lexicon of core terms.
- ***Divergence or Discrepancy in Meanings***. One respondent suggested that terms should be included only when there is or could be a divergence or discrepancy in meanings

which is material to affected parties' ability to collaborate and that such terms should be included even when their inclusion might conflict with stated bases for exclusion. This criterion has not been added because the inclusion of basic terms in the lexicon may contribute to building common understanding across a broad constituency in the financial sector, particularly those who are new to the issues around cyber security and cyber resilience, even when the terms do not have multiple or divergent meanings.

- ***Exclusion of Trendy Terms.*** One respondent suggested adding a criterion to exclude trendy terms. This criterion has not been added because such terms are already excluded by the criterion that the lexicon draws on existing, established sources. Terms that are not already defined by such sources – such as *Cyber Hygiene* – are not included in the lexicon.
- ***Align Regulatory Terms.*** One respondent suggested adding a criterion that would align regulatory terms with those in the lexicon. Among other things, as noted above, the lexicon could be useful in fostering cross-sector common understanding of cyber security and cyber resilience terminology and to work by the SSBs to provide guidance related to cyber security and cyber resilience. As a result, over time, the lexicon may contribute to alignment of terms in the regulatory sphere, and it was determined that it was unnecessary to add this as a separate criterion in selecting terms for the lexicon.
- ***Expansion of Lexicon.*** One respondent suggested modifying the criteria to expand the lexicon to improve understanding of more niche, or specialised, concepts associated with core terms defined in the lexicon. This criterion has not been added because it is inconsistent with a lexicon that is limited in scope and focused on the core terms necessary to support the objective of the lexicon. For example, because of the focus on core terms, terms relating to defining the scope of coverage under insurance policies are not included in the lexicon.

Criteria for Definition of Terms: Intended Users of Lexicon

Two respondents suggested that the intended users of the lexicon should be clarified because this may affect the appropriate level of detail in the definitions, and a third respondent suggested that definitions may need to be more detailed in order to provide an opportunity for specialists to discuss the risks and required actions. As noted in the consultative document, the users of the document include the FSB itself, the SSBs, authorities and private sector participants. It was determined that the intended users need not be specified in further detail. However, the intended users are a broad constituency, whose representatives include many individuals who are not professionals in the field of Information and Communications Technology (ICT). Therefore, the FSB has clarified in the Plain Language criterion for developing definitions that, whenever possible, the lexicon should not use highly technical language designed to facilitate communications among ICT professionals.

Criteria for Definition of Terms: Existing Sources

Five respondents suggested that the use of multiple sources or modification of definitions from original sources could create a risk that cohesiveness between related terms may be weakened or that inconsistencies could be introduced. The determination was made to continue to rely on multiple sources in order to make use of a broader range of approaches and insights than would be available from a single source. In addition, even within any single existing source, definitions may not be fully consistent because some terms have been defined at different times and in different contexts. The FSB, however, has undertaken to ensure that the final lexicon is internally consistent to the greatest extent possible.

Some respondents expressed preferences for particular sources. Two respondents expressed a preference for the International Organization for Standardization (ISO) alone; two respondents expressed a preference for ISO and the US National Institute of Standards and Technology (NIST); two respondents suggested using sources that would make the lexicon more globally representative, e.g. the European Central Bank or the European Union Agency for Network and Information Security (ENISA) *Incident Classification Taxonomy* (2018). One respondent suggested using the newest sources and those which have dealt specifically with cyber security. As noted above, the FSB relied on multiple sources in order to make use of a broader range of approaches and insights than would be available from a single source. In finalising the lexicon, the FSB carefully considered all specific language from any source that was suggested by respondents.

Criteria for Definition of Terms: Plain Language

Two respondents suggested that, in cases where the FSB used definitions that contain cyber or information security terms or phrases, the FSB should consider replacing a more general term label with a more cyber-specific term label. Modifications were made to the lexicon to address this suggestion, e.g. *Advisory* was replaced with *Cyber Advisory* and A*lert* was replaced with *Cyber Alert*.

Specific Suggestions for Deletion, Addition and Modification of Terms

Respondents suggested the **deletion** of 11 terms from the lexicon.

- Five of these terms have been removed from the final lexicon.
  - *Configuration Management* was determined to be a technical term.
  - *Continuous Monitoring*, *Recovery Point Objective* and *Recovery Time Objective* were determined to be general business and regulatory terms that are used in areas extending beyond cyber security and cyber resilience.
  - *Cyber Hygiene* was determined to be an emerging term without a well-established definition.
- Six of the terms suggested for deletion have been retained in the final lexicon.
  - We do not agree with one respondent who suggested that *Data Breach* should be removed because it is redundant with *Cyber Incident*. The definitions of both terms, however, have been modified in the final lexicon in a way that further clarifies the difference between them.
  - *Campaign*, *Course of Action*, *Threat Actor* and *Traffic Light Protocol* were retained in support of the objective to support work in the area of information sharing as appropriate, notwithstanding the view of some commenters that these terms did not support the objective of the lexicon.
  - *Alert* was suggested for deletion by one respondent on the basis that its meaning is not subject to potential misunderstanding. This term has been renamed *Cyber Alert* and the definition has been modified. *Cyber Alert* is included in the lexicon because of its potential to contribute to building common understanding across a broad constituency in the financial sector and in support of the objective to support work in the area of information sharing as appropriate.

Respondents suggested the **addition** of almost 90 terms to the lexicon.

- Consistent with the criterion that the lexicon should be limited in scope and focused on the core terms necessary to support its objective, only three of these terms are included in the final lexicon. These terms are *Advanced Persistent Threat*, *Threat Assessment* and *Threat Intelligence*. In addition, *Threat Vector* was added because it is referenced in the definition of *Advanced Persistent Threat*.
- To enhance the consistency of the lexicon, several terms not suggested by commenters have also been added. The term *Compromise* has been added to the lexicon to enhance clarity of the lexicon because that term is referenced in the term label *Indicators of Compromise* and in the definition of *Data Breach*. The terms *Accountability*, *Authenticit*y, *Non-Repudiation* and *Reliabilit*y, each of which is referenced in the definition of *Cyber Security*, are also included in the final lexicon. The term *Verification*, which is referenced in the definition of *Patch Management*, has also been added.
- Careful consideration was given to each of the terms suggested by respondents for inclusion in the final lexicon. Terms not included were determined not to meet the stated criteria for inclusion. Some of the common reasons for exclusion and examples of excluded terms are as follows:
  - General business and regulatory terms that are used by financial sector participants in areas extending beyond cyber security and cyber resilience were not included in the final lexicon. This included the term *Risk* and a set of compound terms including the term *Risk*, e.g. *Acceptable Risk*, *Risk Acceptance*, *Risk Analysis*, *Risk Measurement* and *Risk Tolerance*. It also included a number of individual terms, e.g. *Anomalous Activity*, *Control*, *Crisis Management*, *Incident Management*, *Likelihood of Occurrence of a Threat*, *Privacy Violation*, *Supply Chain Risk* and *Third Party Service Provider*.
  - Terms that were determined not to be "core" terms were not included in the final lexicon. The lexicon includes the core terms *Cyber Event* and *Cyber Incident*. A set of terms that would, in essence, have created a taxonomy of events and incidents was determined to be too granular for inclusion, e.g. *Accidental Events*, *External Events*, *Internal Events*, *Hardware Problem*, *Phishing*, *Ransomware* and *Unauthorised Access (intentional)*. Another example of exclusion based on this criterion was a set of specialised, insurance-related terms, e.g. *Affirmative Cyber Risk/Non-Affirmative Cyber Risk*, *Communication and Media Liability*, and *Crisis Management Costs*. A number of individual terms were also excluded on this basis, e.g. *Flaw Remediation*, *Legal Entity Identifier* and *One-Time Password or PIN*.
  - As referenced earlier, the term *Attack* and related terms, e.g. *Cyber Attack*, *Attack Surface*, *Cyber Crime* and *Cyber Terrorism* are not included in the lexicon because they are principally related to law enforcement or national security rather than to matters of financial sector regulation or supervision.
  - Technical terms generally were excluded, e.g. *Backup* and *Removable Media*.
  - Terms that were determined to be emerging and without sufficient basis for a definition were not included in the lexicon, e.g. *Crown Jewels*, *Cyber Kill Chain* and *Cyber-Physical System (Smart System)*.

- o The terms *IT-Security* and *Information Security* were excluded as beyond the scope of the lexicon, which is to support work to address, specifically, cyber security and cyber resilience in the financial sector.

Respondents suggested the **modification** of the term labels or definitions for over 40 of the terms in the draft lexicon. Each of these suggestions was considered, and modifications were made where appropriate (although not always corresponding precisely to the suggestions made by commenters), e.g. to add omitted concepts to definitions (e.g. adding the concept of **coordinated** behaviours to the definition of *Campaign*), to clarify the distinction between terms (e.g. *Cyber Event* and *Cyber Incident*), to clarify term labels (e.g. adding *(function*) after *Detect*, *Identify*, *Protect*, *Recover* and *Respond*) or to make a definition relevant to a broader audience (e.g. modifying the reference to four colours in the definition of *Traffic Light Protocol* to drop the specific reference to the number of colours). One modification not attributable to respondents was the substitution of the defined term *Threat-Led Penetration Testing (also known as Red Team Testing*) for the draft definition of *Red Team Testing*. The newly substituted definition was recently published by the G-7.

Maintenance of the Lexicon.

Commenters provided many thoughtful views on maintenance of the lexicon as outlined in this section. The FSB has determined to take these views under advisement and consider them further in the light of actual experience with use of the lexicon.

Commenters generally expressed the view that the lexicon should be updated, although one commenter suggested an alternative approach of contributing to a consistent set of ISO definitions.

Six respondents that addressed **who** should update the lexicon either suggested that it should be the FSB or assumed that it would be the FSB. Two commenters made more generic suggestions, e.g. a group with mixed expertise or the global multi-stakeholder community. One commenter suggested that the FSB ask the sources referenced in the lexicon to inform the FSB of any changes to the source definitions.

Many respondents addressed the **frequency** with which the lexicon should be updated. Suggestions included periodic or regular (nine respondents), twice a year (two respondents), annual (five respondents), every three years (one respondent), every five years (one respondent), when triggered by a source document change or other event (four respondents) and continual monitoring and cross-checking with other existing organisations (one respondent).

A number of respondents addressed the **process** for updating the lexicon. Many respondents noted the importance of stakeholder involvement in the process, including both the public and private sectors. Eight respondents specifically favoured public consultation, with two respondents suggesting a more streamlined process without public consultation for simple updates. One commenter expressly supported transparency in the updating process. One commenter suggested that the FSB consider issuing frequently asked questions (FAQs) to address issues that arise between updates. One commenter expressly supported continuing use of content underpinned by established sources and comparison with leading taxonomy publications.

Some commenters addressed the **substance** of potential future updates to the lexicon. Three commenters expressed support for continuing to maintain a limited scope such that the lexicon only includes a reasonable and small number of terms. One commenter suggested that the FSB periodically review the criteria to ensure that they continue to provide the quality that the FSB seeks when determining whether to include additional terms. One commenter suggested the development of a plan of gradual expansion of the lexicon, and one commenter suggested expanding the lexicon to include cloud-specific terminology.

The FSB will be mindful of these recommendations as it considers maintenance of the lexicon as appropriate in light of experience with the lexicon's use.

Technical Suggestions

As requested by one commenter, the FSB has enhanced cross-references within the lexicon by italicising terms used in definitions when those terms are defined within the lexicon. The FSB has retained full references to underlying sources at the end of the lexicon in order to facilitate traceability to underlying sources as requested by one commenter. One commenter suggested adding examples to definitions to aid understanding. Examples have not been added; examples could lead to more rapid outdating of the lexicon. That said, as experience with use of the lexicon grows, communication among the various users with respect to examples could prove helpful.

Public Availability of the Lexicon

As requested by one commenter, the FSB will provide a public repository for the lexicon by maintaining the final version, with any updates, on its website.

Use of the Lexicon

Two commenters expressed views on how FSB member jurisdictions should use lexicon terms and how the FSB should coordinate with the SSBs with respect to the lexicon. The objective of the lexicon was covered in the consultative document and is again set forth in the material accompanying the final lexicon, and this has not been changed. Two commenters suggested that, where any inconsistencies were observed in original sources and where any unification of terms would be helpful, FSB provide feedback to the relevant organisations. As noted in the consultative document, in the course of developing the lexicon, the FSB working group met with organisations that have been active in the establishment of, and/or training with respect to, cyber security standards. It is expected that additional dialogue with these organisations, as appropriate, would be undertaken as experience with use of the lexicon develops.