Aug. 16, 2018

NAIC National Association of Insurance Commissioners

NAIC Comments in Response to the FSB Consultative Document – Cyber Lexicon

The FSB invites comments on the draft Cyber Lexicon and the following specific 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?

No comment.

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?

No comment.

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.

- *Propose adding the term "Phishing" as this is an important cybersecurity challenge facing organizations as follows: "Tricking individuals into disclosing sensitive personal information through deceptive computer-based means."* https://csrc.nist.gov/Glossary/?term=562#AlphaIndexDiv *– NIST SP 800-45 Version 2*

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.

- *Propose adding the following to the Denial of Service (DOS) definition for further clarification: "A denial-of-service is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. (resource: US-CERT -* https://www.us-cert.gov/ncas/tips/ST04-015*)*

- *Propose replacing existing definition of Social Engineering with the NIST definition as it is more comprehensive as follows: "A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.* https://csrc.nist.gov/Glossary/?term=1467 *NIST SP 800-114*

NAIC National Association of Insurance Commissioners

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?

Given the evolving nature of this area, the Cyber Lexicon should be reviewed on a regular basis to ensure that the definitions defined therein remain up to date and relevant in order to continue to meet the stated objectives in the document to support the work of the FSB, SSBs and private sector participants to address cybersecurity and cyber resilience in the financial sector.