August 20, 2018
Via Electronic Submission to fsb@fsb.org

RE: THE FINANCIAL STABILITY BOARD'S "CYBER LEXICON CONSULTATIVE DOCUMENT"

To Whom It May Concern:

Citi appreciates the opportunity to provide comments in response to the Financial Stability Board's ("FSB") "Cyber Lexicon Consultative Document" published on July 2, 2018. With Physical operations in 98 countries and doing business in circa 175 countries and jurisdictions, consistent and coherent use of language across the private and public sectors is vital, especially in such a cross-border issue. We fully support the FSB's cyber work and very much wish to support you as you continue in this field. Below please find proposed comments and feedback on the Lexicon from Citi.

Terms are in Bold/Blue and Feedback is in Black.

Alert: An alert is an indication of an anomalous event that is believed to be malicious.

Campaign: Suggest this definition specify this is normally one adversary group or more than one defined adversarial group that is working together. Otherwise, it confuses the random adversarial behaviors of many actors and groups against one target to also be a campaign.

Continuous Monitoring: Please add in Cyber Security Framework for words that are not Cyber specific to give context and meaning.

Cyber: Suggest using a definition closer to the NICCS definition of cyber ecosystem - The interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.

Cyber Attack/Breach: A cyber attack is the malicious exploitation by a cyber threat actor of a weakness or vulnerability in a business system or process. A cyber breach is a cyber-attack that is successful.

Cyber Security: To be the people, processes, policies, and technologies that contribute to the prevention of damage to, protection of, and the response and recovery of information technology systems, business information systems, business processes, the associated electronic communication channels and systems, and the information and data contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Cyber Risk: Cyber Risk as the risk posed by an event that results in a breach of sensitive information and/or the compromise of business information assets or operations which leads to a potential or actual financial loss, reputational impact, or other undesirable outcome as a result of a cybersecurity failure.

Data Breach: Recommend removing the word "unintentionally" as this blurs the line between cyber & Technology / operational risk which conflicts with purpose of glossary.

Defence-in-Depth: Recommend "Processes" is added as people, processes & technology are commonly referred to together.

- **E.g.** https://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/Developing-a-Successful-Governance-Strategy.pdf.

- Bruce Schneier popularized the People, Process, Technology Triangle (https://www.schneier.com/blog/archives/2013/01/people_process.html) in 1999 but it has been

referenced since ver 1 of ITL back in the 1980s
http://www.itilnews.com/index.php?pagename=ITIL__Back_to_basics_People_Process_and_Technology

Detect: Please add in Cyber Security Framework for words that are not Cyber specific to give context and meaning.

Event: Language to be included here is an event is anomalous but not malicious. If an event is indicative of a cyber incident, it may generate an alert.

Identify: Please add in Cyber Security Framework for words that are not Cyber specific to give context and meaning.

Identity and Access Management (IAM): Recommend changing word "Products" to "Technology" to be more in line with industry standard terminology. Please add in the word “and.”

Indicators of Compromise (IoCs): Recommend changing to something like "An Indicator of Compromise (IoC) is information that can help with identifying specific malicious behavior on a system or within a network. Information regarding an incident at one organization can lead to detection and possibly prevention within other organizations." Adopted from https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/factsheets/factsheet-indicators-of-compromise/1/ncsc_factsheet_indicators_of_compromise.pdf

Information Sharing: Suggest also including the word "identify."

Protect: This definition feels more like 'resilience' than protection. In terms of protecting assets from cyber threats, it is really more about protecting all three in the CIA triad, not just access. This may be yet another term that is too broad to narrowly define here. The word 'protect' is pretty well understood in anyone's dictionary. Please add in Cyber Security Framework for words that are not Cyber specific to give context and meaning. This definition could also be leveraged in Preparedness, Prevention and Respond.

Red Team Exercise: Red-team exercise: A security test performed by an adversarial expert team, using a documented test methodology, based on a risk-based scenario consisting of an identified system target, a specified threat actor, and a documented set of test objectives, generating documented and actionable findings. Consider also including a reference to Purple Team Exercises, or Red Team End to End Exercises, which signifies the use of the full kill chain from an adversarial perspective.

Situational Awareness: Is not equal to actionable intelligence. Situational awareness is more like knowledge for background sake... in a prepared mode rather than a reaction mode.

Social Engineering: Suggest changing 'confidential' information to 'sensitive' information. The word confidential is defined differently in different jurisdictions and public and private sector organizations.

Traffic Light Protocol (TLP): (document classification/labels) Recommend definition is expanded to include TLP categories:

- TLP-RED - “For your eyes only”: Only to be used by you and not to be spread to other people, even within your own organization.
- TLP-AMBER: To be used and shared with co-workers within your organization on a need-to-know basis and with clients or customers who need to know this information to protect themselves or prevent further damage.
- TLP-GREEN: Used for information that is not very sensitive and can be shared with partners and peers, but not via publicly accessible channels (e.g. websites).
- TLP-WHITE: Public information that can be shared freely, taking into account standard copyright rules.

Source: https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/factsheets/factsheet-indicators-of-compromise/1/ncsc_factsheet_indicators_of_compromise.pdf