FSSCC Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

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:

The Financial Services Sector Coordinating Council ("FSSCC") appreciates the opportunity to provide comments in response to the Financial Stability Board's ("FSB") "Cyber Lexicon Consultative Document" published on July 2, 2018.

The FSSCC is supportive of the development of a Cyber Lexicon and lauds the FSB for soliciting multi-stakeholder input in its development. In this submission, FSSCC will provide a brief introduction of the FSSCC organization, make a request as it pertains to the new, widely used term of "cyber resiliency" in the supervisory process, and respond to the five questions posed by the FSB, namely –

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?*

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?*

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.*

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.*

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 tool?*

A. The Financial Services Sector Coordinating Council (FSSCC)

FSSCC's mission is to strengthen the resiliency of the financial services sector and critical infrastructure against cyber and physical incidents by proactively identifying risks and promoting protection and mitigation, driving preparedness, and coordinating response for the benefit of its consumers, the sector, and the world. Established in 2002, FSSCC is now composed of over 70 member financial institutions, financial utilities, and financial services related trade associations (which, in turn, consist of 1000s of other member institutions). To achieve its mission, FSSCC and its member entities collaborate with appropriate government agencies and governmental bodies to develop and implement a variety of risk management and operational resilience strategies and initiatives. A list of FSSCC member entities can be found on its website: www.fsscc.org.

B. Usage of the Term "Cyber Resiliency" in the Supervisory Process

FSSCC supports both the inclusion of the terms cyber resiliency and cyber security and the selected definitions in the Cyber Lexicon. Recently, regulatory agencies across the FSB's member jurisdictions have been using the term "cyber resiliency" broadly in meaning in both draft policies and examinations (see e.g., CPMI's November 2014 "Cyber resilience in financial market infrastructures" and the European Central Bank's April 2018 "Cyber Resilience Oversight Expectations for Financial Market Infrastructures"). Until this Consultative Document, the term has not been appropriately defined or socialized widely with the private sector. In fact, the term as it has been used seemingly conflated three related concepts: cyber security, business continuity, and business resilience. Because of this, FSSCC requests that the FSB and its member jurisdictions begin a broader dialogue with the private sector, regulated community to ensure appropriate consensus and understanding is developed.

C. Question Responses for FSB's Consideration

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?*

FSSCC supports the overall objective(s) of the FSB Cyber Lexicon: supporting the work of the FSB, standards setting bodies, and the financial services private sector as it relates to –

- Advancement of a cross-sector common understanding of cyber security and resilience terminology;
- Information sharing; and
- Financial Stability Board and/or standards setting body cyber security and resilience guidance and effective practice identification.

The FSB's criteria for term selection to support this objective should be enhanced, however. As a preliminary matter, in selecting terms, the FSB should identify those terms that are "root" terms upon which other cyber relevant terms are built. To the extent that such terms vary in meaning and understanding (i.e., the definitions of those terms are controversial or debatable), the FSB should identify those terms and suggest a definition that retains meaning in a cyber security or resiliency context and can be largely agreed upon by FSB member jurisdictions, standards setting bodies, and private sector implementers. By doing so, the FSB will be able to more fully achieve its objective in advancing common understanding where it had been previously lacking. Using a "root" based or ontological approach also provides necessary context and meaning for terms derived or related to a root word that the FSB then not need address. As such, following this suggested approach, FSSCC will be recommending a series of terms (and associated definitions) that might otherwise conflict with the FSB's stated exclusionary categories related to business, regulatory, and technical terms. Those terms can be found in response to Question 3.

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?*

FSSCC supports the FSB's criteria of (1) reliance on existing sources, (2) use of comprehensive definitions, and (3) use of plain, non-technical language organized in a concise, grammatically correct fashion. In reviewing the definitions of FSB selected terms, FSSCC contends that FSB largely met this criteria. With respect to the third criterion, there are instances, however, wherein FSB opted for a more cyber nuanced definition for an otherwise general term. FSSCC suggests that for general and understood terms, the definitions should likewise be the more general, commonly understood definitions bereft of cyber or information security terms or phrases. To the extent that FSB wishes to use definitions with cyber or information security terms or phrases, FSB should consider replacing the general term with a more cyber specific term. As an example, the term "Alert" is a widely used and understood term which has broader definition and application than in the cyber context, and thus, the term "Cyber Alert" should be selected if the FSB would like to define that term in a cyber context. FSSCC is including other such examples in response to Question 4.

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.*

As noted in response to Question 1, FSSCC supports the addition of a number of terms for which an agreed upon definition would help achieve common understanding and drive better cyber security and resiliency outcomes. Similar to the process articulated in Section 3.1 of the FSB Cyber Lexicon Consultative Document, the FSSCC developed the following terms through an extensive collaborative process, involving a diversity of views from financial institutions within FSB member jurisdictions and via 10s of working sessions. They can be found on the following pages, which have been rotated for ease of viewing:

Term	Definition Selected	Definition Source	Link to Definition Source	Rationale
Acceptable Risk	The IETF's "RFC 4949 - Internet Security Glossary, Version 2" definition modified to be the following: Risk that is understood and tolerated by a user, operator, owner, or accreditor.	The IETF's "RFC 4949 - Internet Security Glossary, Version 2" definition: Risk that is understood and tolerated by a system's user, operator, owner, or accreditor, usually because the cost or difficulty of implementing an effective countermeasure for the associated vulnerability exceeds the expectation of loss.	https://tools.ietf.org/html/rfc4949	Often conflated with risk acceptance, acceptable risk is distinct. As such, FSSC suggests the RFC definition with a slight modification: striking the language following "accreditor" because the language implies a level of quantification may not be available or otherwise attainable.
Critical Infrastructure	**"NIST IR 7298 (Rev. 2) — Glossary of Key Information Security Terms" Definition, but generalized for application in any nation. It would read:** System and assets, whether physical or virtual, so vital to a nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.	"NIST IR 7298 (Rev. 2) — Glossary of Key Information Security Terms" Definition: System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.	https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf	Critical infrastructure is a widely used term, but for which application is inconsistent and for which the definition is not commonly understood.
Risk	**ISACA's "Cybersecurity Fundamentals Glossary" Definition without modification.**	ISACA's "Cybersecurity Fundamentals Glossary" Definition: The combination of the probability of an event and its consequence.	https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf	It is the most accurate and concise and would serve as a better root definition to other "risk" based terms.
Risk Acceptance	**Combined language from the U.S. Department of Homeland Security "Risk Lexicon: 2010 Edition" and ISO Guide 73: 2009 "Risk management - Vocabulary" Definitions:** Explicit or implicit decision to take a particular risk.	DHS Cyber Lexicon definition: Explicit or implicit decision not to take an action that would affect all or part of a particular risk. ISO Guide 73:2009 - Risk acceptance definition: Informed decision to take a particular risk.	https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:en	In any risk environment, including cyber security, there is always a level of risk that an organization will accept either explicitly or implicitly. Despite its centrality, the term itself is one where there has been definitional debate. With respect to the DHS definition, it was potentially the most accurate, but caused pause due to its use of negative phrasing. ISO's definition was also accurate, but its use of the term "informed" has certain connotations that indicate a certain level of formality and documentation that might be above and beyond a decision based on past non documented experiences. Thus a combination of the two definitions seemed the most accurate and appropriate.
Risk Analysis	**Risk Analysis = Risk Assessment** **The ISACA "Cybersecurity Fundamentals Glossary" Definition for Risk Assessment,** which is "A process used to identify and evaluate risk and its potential effects."	ISACA's "Cybersecurity Fundamentals Glossary" Definition: A process used to identify and evaluate risk and its potential effects.	https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fu	Risk Analysis = Risk Assessment; they are synonymous and there are SSBs (e.g., NIST) that state the same. Like Risk Assessment, Risk Analysis is a widely used term, but for which application is inconsistent and for which the definition is not commonly understood. Additionally, with

Term	Definition Selected	Definition Source	Link to Definition Source	Rationale
			ndamentals_glossary.pdf	respect to ISACA's definition of the synonymous term Risk Assessment, it is not limited to just information technology and IT systems like other SSB definitions; it takes a broader view of risk in terms of assessment.
Risk Appetite	**The COSO "Strengthening Enterprise Risk Management for Strategic Advantage" definition.**	The COSO's "Strengthening Enterprise Risk Management for Strategic Advantage" definition: A broadbased description of the desired level of risk that an entity will take in pursuit of its mission.	https://www.coso.org/documents/COSO_09_board_position_final102309PRINTandWEBFINAL_000.pdf	Risk appetite is core to an enterprise's strategy, strategic thinking, and the initiatives it undertakes. Despite its centrality to the firm, itself, it is a term that is often conflated with risk tolerance and for which SSBs and regulators have offered disparate definitions. With respect to the COSO definition, it is the clearest articulation of the difference between risk appetite (something a firm pursues) vs. risk tolerance (something that a firm is willing to accept).
Risk Assessment	**ISACA's "Cybersecurity Fundamentals Glossary" Definition without modification.**	ISACA's "Cybersecurity Fundamentals Glossary" Definition: A process used to identify and evaluate risk and its potential effects.	https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf	Risk Assessment is a widely used term, but for which application is inconsistent and for which the definition is not commonly understood. Additionally, with respect to ISACA's definition, it is not limited to just information technology and IT systems like other SSB definitions; it takes a broader view of risk in terms of assessment.
Risk Management	**U.S. Department of Homeland Security "Risk Lexicon: 2010 Edition" selected, but modified to substitute out the term "controlling" for "mitigating" as it relates to managing risk. It now reads:** Process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or mitigating it to an acceptable level	DHS Cyber Lexicon Definition: Process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.	https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf	Risk Management is a widely used term, but for which application is inconsistent and for which the definition is not commonly understood. With respect to the DHS Cyber Lexicon Definition, it is the most concise in terms of what it means to manage risk. The one issue is that in the DHS definition, it uses the term "controlling" when the more accurate term (and more widely used term) is "mitigating."
Risk Management Framework	**"NIST IR 7298 (Rev. 2) — Glossary of Key Information Security Terms" Definition**	"NIST IR 7298 (Rev. 2) — Glossary of Key Information Security Terms" Definition: A structured approach used to oversee and manage risk for an enterprise.	https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf	Risk Management is a widely used term, but for which application is inconsistent and for which the definition is not commonly understood. With respect to the NIST IR definition, it is the most concise definition, as it applies to the enterprise space.
Risk Management Plan	**Risk Management Plan = Risk Management Strategy** **U.S. Department of Homeland Security "Risk Lexicon: 2010 Edition" definition of Risk Management Strategy selected.**	DHS Cyber Lexicon definition for Risk Management Strategy: Course of action or actions to be taken in order to manage risks.	https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf	Risk Management Plan = Risk Management Strategy given the symmetry in language from among the various SSB definitions. With respect to Risk Management Plan/Risk Management Strategy, they are widely used terms wherein there is confusion as to their interchangeable nature, there is inconsistent application, and for which a unifying definition is not commonly understood. With respect to the Risk Management Strategy definition, it is the most clear and concise among available SSB definitions.

Term	Definition Selected	Definition Source	Link to Definition Source	Rationale
Risk Management Policy	**ISO Guide 73: 2009 "Risk management - Vocabulary" Definition**	ISO Guide 73: 2009 "Risk management - Vocabulary" Definition: Statement of the overall intentions and direction of an organization related to risk management.	https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:en	Risk Management Policy is a term that is widely used term and a term for which a universally accepted definition is needed given it ubiquity in risk management programs.
Risk Management Process	**ISO Guide 73: 2009 "Risk management - Vocabulary" Definition**	ISO Guide 73: 2009 "Risk management - Vocabulary" Definition: Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.	https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:en	Risk Management Process is a term that is widely used term and a term for which a universally accepted definition is needed given it ubiquity in risk management programs.
Risk Management Strategy	**Risk Management Plan = Risk Management Strategy** **U.S. Department of Homeland Security "Risk Lexicon: 2010 Edition" definition of Risk Management Strategy selected.**	DHS Cyber Lexicon definition for Risk Management Strategy: Course of action or actions to be taken in order to manage risks.	https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf	Risk Management Plan = Risk Management Strategy given the symmetry in language from among the various SSB definitions. With respect to Risk Management Plan/Risk Management Strategy, they are widely used terms wherein there is confusion as to their interchangeable nature, there is inconsistent application, and for which a unifying definition is not commonly understood. With respect to the Risk Management Strategy definition, it is the most clear and concise among available SSB definitions.
Risk Measurement	**The Federal Financial Institutions Examination Council's (FFIEC) "IT Examination Handbook Infobase" definition, but with modification. The modification is striking the definition's last sentence and stopping the first sentence at "potential impact."** A process to determine the likelihood of an adverse event or threat occurring and the potential impact.	The Federal Financial Institutions Examination Council's (FFIEC) "IT Examination Handbook Infobase" Definition: A process to determine the likelihood of an adverse event or threat occurring and the potential impact of such an event on the institution. The result of risk measurement leads to the prioritization of potential risks based on severity and likelihood of occurrence.	https://ithandbook.ffiec.gov/glossary.aspx	Risk Measurement is a widely used term, but for which application is inconsistent and for which the definition is not commonly understood. With respect to the FFIEC definition and its shortening, the reason for doing so is because the last sentence in no way contains defining language, and with respect to the shortening of the first sentence, measurement may not always be at an enterprise level.
Risk Tolerance	**COSO Definition:** "Reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve." **Rationale: Other definitions were bypassed in favor of COSO's definition because participants felt that any definition selected could not conflate the two, but rather had to make the distinction of "appetite" is what you actively pursue and tolerance is what you can accept.**	COSO's "Strengthening Enterprise Risk Management for Strategic Advantage" definition: Risk tolerance reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve.	https://www.coso.org/documents/COSO_09_board_position_final102309PRINTandWEBFINAL_000.pdf	Risk tolerance is also a core term that is often conflated with risk appetite and for which SSBs and regulators have offered disparate definitions. With respect to the COSO definition, it is the clearest articulation of the difference between risk appetite (something a firm pursues) vs. risk tolerance (something that a firm is willing to accept).

Term	Definition Selected	Definition Source	Link to Definition Source	Rationale
Threat	**"NIST IR 7298 (Rev. 2) — Glossary of Key Information Security Terms" second definition modified to be as follows:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals.	"NIST IR 7298 (Rev. 2) — Glossary of Key Information Security Terms" Definition(s): 1. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. 2. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf	The term Threat is a widely used "root" term for which there are numerous definitions. Regarding the selected definition, with the removal of "information systems" language, it is expansive enough to account for all types of impactful circumstances or events and the term could be more readily be modified with adjectives such as global, cyber, etc.
Threat Analysis	**Threat Assessment = Threat Analysis** **NIST 800-30, Rev. 1 (and CNSSI No. 4009) Definition of Threat Assessment:** Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.	**NIST 800-30, Rev. 1 (and CNSSI No. 4009) Definition of Threat Assessment:** Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf	Threat Assessment and Threat Analyses are a widely used and interchangeable terms, but for which application is inconsistent. With respect the NIST definition, it is the most succinct.
Threat Assessment	**Threat Assessment = Threat Analysis** **NIST 800-30, Rev. 1 (and CNSSI No. 4009) Definition of Threat Assessment:** Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.	**NIST 800-30, Rev. 1 (and CNSSI No. 4009) Definition of Threat Assessment:** Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf	Threat Assessment and Threat Analyses are a widely used and interchangeable terms, but for which application is inconsistent. With respect the NIST definition, it is the most succinct.
Threat Intelligence	**CPMI-IOSCO's "Guidance on cyber resilience for financial market infrastructures (Annex A - Glossary)" Definition, slightly modified to be as follows:** Information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event.	CPMI-IOSCO definition: Information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event (may also be referred to as “cyber threat information”).	https://www.bis.org/cpmi/publ/d146.pdf	With respect to the CPMI-IOSCO definition, it is the most concise and aligns with other selected definitions; the reason for removal of the parenthetical is because it in effect confuses two separate terms - "Threat Intelligence," which encompasses a variety of threats (not just cyber) and more specific to contextualized information, and "Cyber Threat Information," which is inclusive of a narrow threat category and non-contextualized information.

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.*

FSSCC supports the inclusion of a substantial majority of FSB selected terms and definitions. There are instances, however, where FSSCC supports either the modification of definitions, the modification of terms, or striking of terms. With respect to definitions that FSSCC recommends modifying, they are for the following terms and reasons:

Term	FSB Definition	Definition Selected and Rationale
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)**	The FSB definition was selected, but FSSCC suggests modifying it to be more generalized because the term "Continuous Monitoring" is a more general term. The suggested definition is as follows: "Maintaining ongoing awareness of systems, processes, technology, operations and threats to support organizational risk management decisions."
Cyber Incident	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. **Source: Adapted from NIST (definition of "Incident")**	FSSCC suggests modifying the FSB definition of Cyber Incident to be more succinct and to avoid inclusion of possible, hypothetical harm, which may be implied by the inclusion of the term "jeopardize" or terms "potentially jeopardize". The suggested definition is as follows: "A cyber event that compromises the confidentiality, integrity or availability of an information system."
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. **Source: Adapted from CPMI-IOSCO**	In order to relate back to the suggested additional term of Threat, FSSCC recommends the following: "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service." Source: "NIST IR 7298 (Rev. 2) — Glossary of Key Information Security Terms," the second definition of the term Threat.

Information Sharing	An exchange of data, information and/or knowledge that can be used to manage cyber risks or respond to cyber incidents. **Source: Adapted from NICCS**	The FSB definition was selected, but FSSCC suggests modifying it to be more generalized because the term "Information Sharing" is a more general term. The suggested definition is as follows: An exchange of data, information and/or knowledge that can be used to manage risks or respond to security incidents.
Recovery Point Objective (RPO)	Point to which information used by an activity is restored to enable the activity to operate on resumption. **Source: ISO 22300:2018**	FSSCC recommends modifying the FSB's to include the modifier "normally." The objective is to not just restore information or systems, but to do so in a way that restores information or system integrity. The suggested definition is as follows: "Point to which information used by an activity is restored to enable the activity to operate normally on resumption."
Traffic Light Protocol (TLP)	A set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colours to indicate expected sharing boundaries to be applied by the recipient(s). **Source: FIRST**	FSSCC suggests FSB modify its definition. TLPs vary across domains, they do not always consist of four colors, and even within the traditional 4 color TLP regime, white means that information is not always sensitive. As such, those modifiers have been deleted and FSSCC suggests the following amended definition: "A set of designations used to ensure that information is shared only with the appropriate audience. It employs a pre-established color code to indicate expected sharing boundaries to be applied by the recipient."
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation. **Source: NIST**	The FSB definition was selected, but FSSCC suggests modifying it to be more generalized because the term "Information Sharing" is a more general term. The suggested definition is as follows: "Systematic examination of a system, product, control, or process to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation."

With respect to the terms that FSSCC recommends modifying, they are the NIST Cybersecurity Framework Functions of "Identify," "Detect," "Protect," "Respond," and "Recover." FSSCC suggests that those terms should be modified to "The Identify Function," "The Detect Function," "The Protect Function," "The Respond Function," and "The Recover Function." By changing the terms, FSB can keep the NIST definitions, but avoid creating definitional confusion for otherwise general terms with long understood definition and meaning.

Lastly, FSSCC recommends striking the following terms altogether because the terms do not meet the "objective" criteria and are sourced from non-authoritative sources, such as white papers:

- Campaign;
- Course of Action;
- Cyber Hygiene; and
- Threat Actor.

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 tool?*

To the extent that FSB retains ownership and maintenance of the Cyber Lexicon, FSSCC recommends the FSB continue with a consultative process to identify new candidate terms and corresponding definitions. If additional terms are considered, depending on the terms themselves, the FSB should recognize cases in which usage of a term differs by jurisdiction. FSSCC anticipates that a periodic review cycle should be sufficient.

Additionally, as part of the process, FSB should provide a mechanism for users to locate the most current version of the lexicon (i.e., a public repository for the authoritative document).

Finally, upon publication of the final lexicon, FSSCC requests that FSB member jurisdictions integrate those terms and definitions into their future supervisory functions, guidance, and cross-border cooperation.

Respectfully submitted,

____

Craig Froelich
Chair
Financial Services Sector Coordinating Council