[redacted] [redacted]
To: cyberframework
[redacted] [redacted]
Subject: ISACA Comments on NIST CSF 2.0 Core Discussion Draft
Date: Wednesday, May 24, 2023 1:18:06 PM
[redacted]

RE: Discussion Draft of the NIST Cybersecurity Framework 2.0 Core
Dated April 24, 2023

Dear NIST CSF 2.0 team:
Thank you for the opportunity to submit comments and provide feedback on the 4/24 discussion draft on CSF 2.0 Core. ISACA's comments are as follows:

1. In general, as we discussed in previous comments and during the workshops in February – CSF should consider/address 2 primary use cases/audiences:
    a. **Those who are new to CSF and want to adopt and need example best practices to tell them both what to do and examples of HOW to address that requirement**.
    b. **Those who want to appraise/assess their maturity or capability levels against the CSF**. As we heard from several folks during the workshops – they use CMMI maturity levels to assess their maturity against the CSF, so we want to make that both easy and consistent. Accordingly, we are plannin on a mapping between CMMI V3.0 and CSF 2.0, and believe there will be great opportunity for synergy and reciprocity given the clear overlap in many areas of both frameworks. We are also looking at similar overlap for COBIT. The folks may not need the detailed "how to" unless they have gaps in their implementation and then having the examples can help to address those gaps.
2. **Other comments**
    a. **Prominence and escalation of the importance of Governance** is the CSF is a good thing and was needed.
    b. **Table 1** proposed CSF 2.0 Core Function and Category names:
        - The addition of Govern sections to CSF 2.0 updates CSF 2.0 to a more modern approach that emphasizes the importance of Governance and Executive leadership to overall success of an organization cybersecurity program. Realignment and clarification of categories also improves the overall flow and effectiveness of CSF 2.0.
    c. **Table 2** – Sample of implementation examples:
        - The addition of implementation examples will assist both new and experience CSF 2.0 users as per general comment above. We would suggest a select number are placed in each section and the complete list of these examples / "controls" are placed in a separate appendix to be reference/used when needed and not "clog up" the key concepts and points of the framework
    d. **Table 3** – Draft NIST Cybersecurity Framework 2.0 Core: Functions, Categories, and Subcategories:
        - The category mappings to previous CSF 1.1 framework are helpful because it

should enable easier conversion to the newer CSF 2.0.

e. **Simpler is better**. Consider running the CSF through Flesch Kincaid analysis (available in MS Word) for targeting better readability and lower grade level objectives – continue to reduce the number of subcategories, and intentionally focus on plain language where possible.
f. Additionally, the increased of information and explanations of each subcategory is a much-needed improvement.

3. **Where there are no mappings to the previous version CSF 1.1, we recommend additional information or explanations in a note to help the user understand why this is new** and what is the intended purpose (addressing cyber insurance, improving supply chain management, introduction of ethics into strategy thinking…).
4. **We would also recommend additional notes are added to address why categories and subcategories were added**, realigned, dropped, or renamed.

Thank you again for the opportunity to provide our feedback, and we look forward to seeing more and continuing to partnering with NIST over the next several months and seeing the eventual launch of CSF 2.0. Please let us know if there is anything else we can help with.

Ron Lear, **CHMLA, LSSGB, ISO Lead Auditor**
Vice President, Frameworks and Models
[redacted]

ISACA

[redacted]