Dear Ms. Pascoe and Team,

Please refer to my prior comments on the first discussion draft for a more explanation.

The key statement in this document is “Network and system architectures are assessed for design and implementation weaknesses affecting confidentiality, integrity, availability, and resilience.”
This reflects both the strengths and weaknesses of the document overall.

- **Strength** is that it mentions “systems” and “design … weaknesses” in the same sentence.
- **Weakness** is that it 1) does not address any of the math and method problems where cyber lags decades behind other disciplines and 2) the focus is on CIA with a:
    - Limited add for “resilience.” “Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).” This is a limited notion compared to that put forward by IBM over two decades ago.
    - No recognition of other considerations (see ISACA’s COBIT)

More broadly, this suffers from the same problems as the current CSF:

- **The CSF lags decades behind the methods and math common in other disciplines** – including those widely used in federal government.
- It is not a “framework” as used by NIST for other disciplines or by other government agencies and labs for understanding systems. **A recognized test of a framework is that anything that can change the outcome of a system is part of the system included in the framework.** (Would you fly on a plane or have surgery where the people responsible for your safety had an incomplete understanding of the system?) The CSF does not incorporate enough of SP 800-160.
- **The CSF relies far too much on bookkeeping checks instead of real controls. This creates waste and vulnerabilities:**
    - Incorrectly referred to as “controls” – they are not controls as the concept has been used since the industrial revolution and even in COSO ’92.
    - These false controls are wasteful and **set up cybersecurity professionals for failure leading to breaches**. Systems approaches (SP 800-160) are safer.
        - It is a meme online – people set up for failure.
        - The inefficiency and ineffectiveness of bookkeeping checks is easy to see with basic systems math (see Bayesian analysis -- part of high school math).
        - Does not mention the typical errors in cybersecurity math that are responsible for so many errors in priority setting and thus undermines the strengths of CSF.
    - Part of the waste is the need for an army of “checkers checking checkers.”
        - This approach is wasteful.
        - **This is a lesson from federal government decades ago.** It was not done during WWII (with insights from W. Edwards Deming and Russell Ackoff who worked in what is now the Ford Office Building). It was not done in cyber in the private sector through the early 2000s (the Y2K challenge was addressed with systems methods focusing on dependency analysis). It is not done today even though widely used in other systems – such as the device you are using to read this document.
        - Yet, this waste and loss of mission effectiveness is what happens when people are not trained in a system understanding as in SP 800-160, cooking, sports, aviation, logistics, winemaking, music, medicine, climate change and more.

- This reflects a **lack of systems and root cause analysis** (again as done within government for about a century). Mr. Ishikawa's famed Fishbone Diagram – starting with the "Environment" bone reveals what is missing in this CSF Draft. Again, reflected in SP 800-160.
- The CSF draft in current form is a threat to national security for failing to apply knowledge that has been proven and practical for decades in other disciplines, including government.
- Rather, the **objective of the revised CSF could be to reduce stress and burnout for cyber pros, reduce waste and inefficiency** (especially for hospitals, municipal government, public utilities and other smaller organizations**), and make it easier for cyber pros to protect people from danger.** NIST and the federal government have so much to offer to make this objective easily attainable.

Very respectfully submitted,

Brian Barnier
OCEG Fellow
2015 ISACA V. Lee Conyers Award recipient
2021 ISACA Joseph J. Wasserman Award recipient