

Comments on NIST CSF 2.0 Concept Paper

https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

<https://csrc.nist.gov/News/2023/csf-2-0-concept-paper-released>

cyberframework@nist.gov

Hello, a few comments...

- The NIST CSF is not a “framework” as used in other disciplines. Thus, delete the term “framework.”
 - Formally, a “framework” provides a comprehensive understanding of a phenomenon/system (varies by discipline). This means that anything that can change the outcome of a system is included in the system and thus part of a framework.
 - Consider the incompleteness in the context of other disciplines...
 - If the CSF were used for building codes in Washington, DC or Rockville, MD buildings would fall. For more, see the systems thinking at <https://www.nist.gov/buildings-construction/understanding-building-codes> or <https://www.iccsafe.org/products-and-services/i-codes/2018-i-codes/ibc/>
 - If the CSF were used for aviation, airplanes would fall out of the sky. For more, see the systems thinking at <https://www.cast-safety.org/> and www.nts.gov (especially investigations section), www.faa.gov or <https://asrs.arc.nasa.gov/publications/callback.html>.
 - Or frameworks created by NIST or federal government for other disciplines.
 - The closest that the cybersecurity world has to a framework is ISACA’s COBIT, led by a former naval officer.
 - The governance material proposed for CSF 2.0 in item 4 is already there – and better integrated with risk management. (Please see more on risk management math below.)
 - NIST has systems thinking in cybersecurity in SP 800-160 – secure systems engineering. This systems approach should be the centerpiece of NIST for cybersecurity.
- That CSF points to SP 800-53 compounds the magnitude of the problem.
 - The simple reason is that SP 800-53 dangerously conflates two very different types of “controls” – 1) bookkeeping checks and 2) automated controls. The first dates to ancient Egyptian grain accounting and the second to ancient animal traps.
 - While tire pressure can be “checked” like a bookkeeping tally the accurate pressure comes from a systems understanding <https://www.nist.gov/news-events/news/2016/11/national-aviation-history-month-nist-tests-airplane-wheels>.
 - Recall the aviation analogy, it would be massive cognitive overload on pilots to do bookkeeping checks (similar problems for nurses in ICUs or other high-demand cognitive occupations). <https://www.nist.gov/news-events/news/2021/03/calling-all-firefighters-new-research-study-wants-hear-you>. This is a structural flaw, seeing cyber security as a mostly technical problem, rather than that cyber pros are setup to fail by bad math and methods (the words “human” and “people” do not appear at all in the Concept Paper despite decades of research).

- This conflation stems from an error in the 1970s in U.S. federal government that viewed computers as largely for accounting, thus applying bookkeeping checks to them. It was a structural flaw to spread these to info/IT/cyber security. Why? Because the nature of the two distinct systems are extremely different.
- When the systems math is calculated most “controls” in 800-53 are ineffective, another set are a waste of money, and some are both efficient and effective.
- Items 2.5 and 2.6 mention Zero Trust. But those NIST documents references are in error. Authentic ZT is found at <https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf>
- Item 4.2 is structurally flawed because it points to sources that use bookkeeping (audit) and insurance (after a loss) math. Systems math should be used.
- Item 5 could be flawed if the approach is to treat IT supply chain as disjointed as the comments suggest. NIST already has SP 800-160. And ISACA COBIT addresses this. The need is for integration as is noted. This reinforces the earlier point that the CSF is not a “framework” as used in other disciplines.
- Item 6, great caution for the proposals in this section to avoid “meets minimum.” As discussed at the workshop, a “seal of approval” would not be advised. Look to aviation, process safety, sports, military and/or musical performance for guidance.
- In short, these flaws can be easily exploited by attackers who do nothing more than eat popcorn and watch old movies.
 - Systems and root cause analysis (as used in other disciplines and federal government since at least WWII, not the flavor of RCA typically used in cyber security) reveals that most all breaches are self-inflicted.
 - The CSF lags by decades the proven and practical methods used elsewhere in NIST and the federal government.
 - In this sense, CSF creates vulnerabilities.
 - This update is an opportunity to close that gap and jump decades ahead. NIST already has the resources in other areas and SP 800-160.

Very respectfully submitted,

Brian Barnier

Co-founder, Think.Design.Cyber and CyberTheory Institute.

ISACA Conyers and Wasserman awards recipient, OCEG Fellow

