Dear Ms. Pascoe and Team,

Regarding the draft release on August 8, 2023 of the NIST Cybersecurity Framework 2.0.

Please refer to my prior comments for a more explanation. I will only repeat those there the are most important.

By so closely following OMB Circulars https://www.whitehouse.gov/omb/information-for-agencies/circulars/, this document becomes a gift to China, Russia, North Korea and Iran.

I would encourage your team to escalate to whomever is necessary to change to the basis of the CSF from bookkeeping checks to Industrial-Strength Design Thinking as used widely elsewhere in federal government for over a century.

This suffers from the same problems as the current CSF:

- **It starts with the flawed assumption that the nature of the system in which cyber risks lives is like bookkeeping – linear, stable and highly rules-based.**
    - This is incorrect.
    - The nature of the system in which cyber risk lives is **complex, dynamic, adaptive and chaotic**. The enemies mostly do not have employee badges. The enemies are external.
- **Thus, the CSF relies far too much on bookkeeping checks instead of real/automated controls. This creates wasted budget 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 the 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.

- **The CSF lags decades behind the methods and math common in other disciplines** – including those widely used in federal government. Please see partial list at the end of this document.
- 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.
- 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, school systems, universities, 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.

Please see the review report of NIST made public last for the larger picture.

Very respectfully submitted,

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

Resource List: Federal Government and other source on Industrial-Strength Design Thinking (the combination of critical, systems and design thinking) …

Industrial-Strength Design Thinking summary for cybersecurity – this was the basis of my keynote at the ISACA Washington conference in 2022.

- www.thinkdesingcyber.com
    - Please see the "Insights" page with links to other resources
- www.tdcleadershub.com

Authentic Zero Trust Strategies

- President Biden's Executive Order including Zero Trust https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- NSTAC Report for authentic Zero Trust (many uninformed resources are incorrect) https://www.cisa.gov/sites/default/files/publications/Final%20Draft%20NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf

Critical Thinking

- https://files.eric.ed.gov/fulltext/EJ1143316.pdf

- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4216424/
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4235550/
- https://www.dol.gov/sites/dolgov/files/odep/topics/youth/softskills/problem.pdf
- https://leb.fbi.gov/articles/perspective/perspective-need-for-critical-thinking-in-police-training
- https://emilms.fema.gov/is_0453/groups/46.html
- https://www.dhs.gov/publication/media-literacy-and-critical-thinking-online
- https://humancapital.learning.hhs.gov/e-blast/eblast201904.asp
- https://appel.nasa.gov/course-catalog/critical-thinking-and-problem-solving-appel-ctps/
- https://psnet.ahrq.gov/issue/developing-critical-thinking-skills-delivering-optimal-care

Systems Thinking

- https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final
- www.ntsb.gov
- www.csb.gov
- https://pubmed.ncbi.nlm.nih.gov/17566541/ -- Medical Team Training at the Veterans Health Administration
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3940421/
- https://www.dhs.gov/publication/st-operations-and-requirements-analysis-overview-fact-sheet
- https://www.dhs.gov/science-and-technology/ora
- https://apps.dtic.mil/sti/citations/AD1045468
- https://www.airforcemedicine.af.mil/News/Display/Article/1089321/afms-uses-systems-thinking-to-keep-everyone-on-the-same-team/
- https://archive.epa.gov/ged/tutorial/web/html/index.html
- https://www.fs.usda.gov/treesearch/pubs/60063
- https://asrs.arc.nasa.gov/publications/callback.html

Design Thinking –
Please note: 1) for cyber security only industrial-strength design thinking is appropriate, not the UX flavor although UX flavors are include in the resource list and 2) use in military

- Department of Defense Joint Special Operations University https://www.youtube.com/channel/UCL7hOd0ihWzmJlga_Y4wCJg
- https://www.dyess.af.mil/News/Features/Article/2552100/afgsc-design-thinking-course-leads-to-dyess-afbs-first-sbir-phase-3/
- https://www.dhs.gov/sites/default/files/publications/OCIO%20Strategic%20Plan.Dec2018.pdf
- https://www.secnav.navy.mil/agility/assets/documents/WCD%20Fac%20course%20version%2020200830.pdf
- https://juniorofficer.army.mil/turn-your-meetings-into-intrapreneur-workshops/
- https://www.nist.gov/blogs/manufacturing-innovation-blog/five-hottest-innovation-tools-0
- https://www.cdc.gov/pcd/issues/2018/18_0128.htm
- https://www.acf.hhs.gov/ofa/report/creating-solutions-together-design-thinking-office-family-assistance-and-3-grantees
- https://www.ed.gov/sites/default/files/documents/stem/cybersecurity-slides.pdf
- https://niccs.cisa.gov/training/search/skillsoft/prototyping-design-thinking
- https://assets.section508.gov/files/Copy%20of%20Universal_Design_%20White%20Paper_vFinal_0.pdf

- https://18f.gsa.gov
- https://www.nps.gov/edis/learn/kidsyouth/edison-and-his-era.htm

Non-governmental

- Written
  - https://www.linkedin.com/company/think-design-cyber/ -- includes posts mention
  - The Operational Risk Handbook https://www.harriman-house.com/the-operational-risk-handbook-for-financial-companies -- what you saw in the talk grew from 3 chapters of The Handbook
  - Why Controls Have Become Wasteful, A False Sense of Security, and Dangerously Distracting—and How to Fix it https://www.tandfonline.com/doi/full/10.1080/07366981.2015.1041815
  - CYBERSECURITY: THE ENDGAME – PART ONE https://www.tandfonline.com/doi/abs/10.1080/07366981.2020.1752466
  - CYBERSECURITY: THE ENDGAME – PART TWO https://www.tandfonline.com/doi/full/10.1080/07366981.2021.1944024
  - https://www.nytimes.com/2003/11/30/magazine/the-guts-of-a-new-machine.html
  - https://www.amazon.com/They-Made-America-Centuries-Innovators/dp/0316277665 (also abridged into PBS series)

Fun videos --- How cyber pros are setup to fail, lessons from decades ago…

- From YouTube:
  - Charlie Chaplin factory scene (1936) https://www.youtube.com/watch?v=6n9ESFJTnHs
  - Lucy & Ethel in the Chocolate Factory (1952) https://www.youtube.com/watch?v=AnHiAWlrYQc
- From Netflix:
  - "The Founder" on Netflix (1950s) – with Michael Keaton, watch the tennis court scene about 10-15 minutes in about how the McDonald brothers used critical, systems and industrial-strength design thinking to design the restaurant kitchen
  - Disney Pixar story