Federal Register Notice: 89 FR 78915, Federal Register :: Networking and Information Technology Research and Development Request for Information on Cyber-Physical Systems Resilience Research, September 26, 2024.

Request for Information on the National Cyber-Physical Systems Resilience Plan

Mitchell Berger

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

Mitchell Berger
[redacted]
October 20, 2024

To: Melissa Cornelius, NITRD, [redacted]

Re: **Networking and Information Technology Research and Development Request for Information (RFI) on a National Plan for Cyber-Physical Systems Resilience, https://www.regulations.gov/document/NSF_FRDOC_0001-3403/comment**

Note: This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in the National Cyber-Physical Systems Resilience R&D Strategic Plan and associated documents without attribution.

Dear Ms. Cornelius: In response to NITRD's and NSF's above RFI, I write to emphasize the importance of focusing on cyber-physical systems (CPS) resilience in the context of health and healthcare. The PCAST plan referenced in the RFI, while including participants from the health sector, does not particularly emphasize health care needs or challenges.[1] On the other hand, the Department of Health & Human Services' Healthcare and Public Health Sector-Specific Cyber Performance Goals have limited discussion of CPS.[2]

Research needs concerning medical CPS have been noted.[3] One group of authors points out that "There is [….] an urgent need for an empirical study on MCPS and the nature of the relationship between the key characteristics of healthcare service delivery. The studies should also explore the use of MCPS in preventative, curative, palliative and rehabilitation healthcare services in terms of SWOT analysis."[4] Within health care, the Internet of Things (IoT) can support for patient monitoring and treatment.[5] Such devices may be overlooked in traditional vulnerability assessments.[6] In some cases, medical devices and other technologies have been accessible from the public internet.[7] 0

One company studying IoT at 300 hospitals notes that "53% of connected medical and other IoT devices in hospitals have a known critical vulnerability, including a third of the bedside devices

[1] https://www.whitehouse.gov/pcast/briefing-room/2024/02/27/pcast-releases-report-on-strategy-for-cyber-physical-resilience/; Xu H, Yu W, Griffith D, Golmie N. A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. IEEE Access. 2018;6:10.1109/access.2018.2884906. doi: 10.1109/access.2018.2884906. PMID: 35531371; PMCID: PMC9074819.

[2] https://hhscyber.hhs.gov/documents/cybersecurity-performance-goals.pdf

[3] Sony, M., Antony, J. and McDermott, O. (2022), "The impact of medical cyber–physical systems on healthcare service delivery", The TQM Journal, Vol. 34 No. 7, pp. 73-93. https://doi.org/10.1108/TQM-01-2022-0005

[4] For more information on SWOT see https://www.mindtools.com/amtbj63/swot-analysis; https://ndupress.ndu.edu/Media/News/News-Article-View/article/2053087/cyber-physical-systems-the-coming-singularity/

[5] Chunyan Li, Jiaji Wang, Shuihua Wang, Yudong Zhang, A review of IoT applications in healthcare, Neurocomputing, 2024: 565: 127017, https://doi.org/10.1016/j.neucom.2023.127017; Verma R. Smart City Healthcare Cyber Physical System: Characteristics, Technologies and Challenges. Wirel Pers Commun. 2022;122(2):1413-1433. doi: 10.1007/s11277-021-08955-6.

[6] https://claroty.com/blog/10-examples-of-cyber-physical-systems

[7] https://medcitynews.com/2024/10/cybersecurity-healthcare-2/; https://www.cdotrends.com/story/17594/iot-security-giving-healthcare-heart-attacks

that patients most depend on for optimal health outcomes."[8] Devices using outdated operating systems, including IV pumps and nursing call systems, may place patients at risk.[9]

CPS also is beginning to support within health care use of robotics, enhanced data management (e.g., through use of blockchain technologies) and personalized care.[10]

In addition to CPS within the health sector itself, health care agencies and organizations also are reliant on other critical infrastructure sectors such as food and water and transportation and electricity and vice versa as many of these sectors would rely on the health care sector in an emergency.[11]

NITRD, NSF and partners should support further research into how CPS is used within health care and interdependencies within health care and other sectors using CPS. Privacy and confidentiality also should be further understood and emphasized.[12] NITRD and its partners also should research how best to obtain input from members of the public and end-users. As CPS capabilities evolve, so too will ethical and policy questions about use of these systems and the data they collect become more complex. Obtaining public input on an ongoing basis will be essential.[13] There also is a need to offer objective, comprehensive education about these topics to state, local, tribal and territorial policymakers and their staff.

I appreciate your consideration of this input.

Sincerely,

Mitchell Berger

Note: Please note that I am submitting these suggestions in my personal/private capacity and not on behalf of any organization or agency. The views expressed are mine only and should not be imputed to other individuals nor to any public or private entity.

[8] The State of IoMT Device Security, Cynerio, https://www.cynerio.com/landing-pages/the-state-of-healthcare-iot-device-security-2022; https://www.cynerio.com/blog/visibility-is-not-enough-key-takeaways-from-cynerios-2022-state-of-healthcare-iot-device-security-report

[9] Id., See also, https://healthitsecurity.com/news/1-in-5-connected-medical-devices-run...1

[10] H. M. Khater et al., "Empowering Healthcare With Cyber-Physical System—A Systematic Literature Review," in IEEE Access, vol. 12, pp. 83952-83993, 2024, doi: 10.1109/ACCESS.2024.3407376; https://www.nationalacademies.org/news/2023/11/the-rise-of-cyber-physical-systems

[11] https://www.naccho.org/blog/articles/the-department-of-homeland-security-sector-risk-snapshots-released

[12] https://pages.nist.gov/cpspwg/; Differential Privacy Techniques for Cyber Physical Systems: A Survey. MU Hassan, MH Rehmani, J Chen. IEEE Communications Surveys & Tutorials 22 (1), 746-789.

[13] See e.g., https://ecastnetwork.org/;https://participedia.net/