September 25, 2023

To Whom It May Concern:

Re: Comments on proposed FCC cybertrust mark labeling

Thank you for the opportunity to provide feedback on the Notice of Proposed Rulemaking by the FCC's "Cybersecurity Labeling for Internet of Things" PS Docket No. 23–239, known informally as the U.S. Cyber Trust Mark. This comment responds to the request for comments regarding scope in Section III. Discussion, B. Eligible Devices or Products, Clauses 10–16. In my opinion as an expert in IoT and medical device security, **the Cyber Trust Mark should explicitly exclude FDA-regulated medical devices from its scope**. To prevent a weakening of the more rigorous FDA expectations of cybersecurity engineering, I strongly recommend removing FDA-regulated medical devices from the scope and instead pointing readers to 21CFR and the recently passed Consolidated Appropriations Act, 2023 ("Omnibus"), which was signed into law. Section 3305 of the Omnibus — "Ensuring Cybersecurity of Medical Devices" — amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices (section 3305). The new law took effect March 29, 2023. More information appears at the FDA Digital Health Center of Excellence[1] and the FDA draft cybersecurity guidance document about to be finalized[2], and the FDA CDRH Response to NIST Regarding President's Executive Order on Improving the Cybersecurity of the Federal Government (EO 14028)[3].

The reason for my recommendation is that medical devices already have a much more rigorous federal law and standards requiring certain pre-market cybersecurity engineering. Including medical devices in an FCC Cyber Trust Mark labeling program would cause confusion in the marketplace by proposing a weaker set of security controls than the status quo. A Cyber Trust Mark would not be sufficient for a manufacturer to legally sell a medical device in the United States. Manufacturers will get confused by two conflicting regulatory requirements where a labeling program is strictly weaker security that rigorous pre-market review. Regulatory confusion would harm the security of pacemakers, defibrillators, infusion pumps, insulin pumps, radiation therapy, patient monitors, and many more life saving devices that presently have much higher federal requirements by statute for cybersecurity engineering. It is presently a violation of federal law for a manufacturer to market a medical device in the United States without first receiving clearance and/or approval from FDA on the device's cybersecurity engineering and design.

[1] `https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity`

[2] `https://www.fda.gov/media/119933/download`

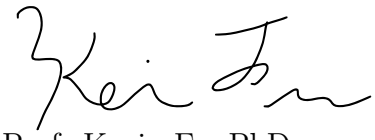
[3] `https://www.fda.gov/media/149954/download`

However, I agree that a U.S. Cyber Trust Mark would significantly help markets where there is less stringent regulation, such as non-therapeutic and non-diagnostic devices including step counters, personal health monitors, IoT weight scales, IoT lightbulbs, light switches, thermostats, and so on where there is presently little in terms of pre-market cybersecurity engineering requirements.

In this letter, I speak as an individual whose expertise is security and privacy of computer systems and the Internet of Things (IoT). My expert qualifications include being a Fellow of the Association of Computing Machinery (ACM) for contributions to computer security, and especially to the secure engineering of medical devices, a Fellow of the Institute of Electrical and Electronics Engineers (IEEE) for contributions to embedded and medical device security, and a Fellow of American Association for the Advancement of Science (AAAS) for contributions to computer security, and especially to the secure engineering of medical devices. I previously served as the nation's inaugural Acting Director of Medical Device Security at the U.S. Food and Drug Administration (FDA). I have testified in the U.S. House and Senate on cybersecurity matters, and I presently serve on a White House PCAST working group on Cyberphysical Resilience. I have a PhD from MIT on computer system security, and I founded the Archimedes Center for Health Care and Medical Device Cybersecurity. I served as a member of the U.S. NIST Information Security and Privacy Advisory Board and various federal science advisory groups. I am a Professor at Northeastern University in the Department of Electrical and Computer Engineering, the Khoury College of Computer Sciences, and the Department of Bioengineering. My opinions are my own, and do not necessary represent that of my past or present employers or groups to which I belong. I am speaking as an individual.

Please let me know if any additional information or testimony would be helpful. Thank you.

Sincerely,



Prof. Kevin Fu, PhD
ACM Fellow
IEEE Fellow
AAAS Fellow
Dwight E. Harken Memorial Lecturer
kf@kevinfu.com