To: NIST
cyberframework@nist.gov

From: Miriam Eckenfels-Garcia, Esq.
Director, EMR & Wireless Program
Children's Health Defense
[redacted]

Re: Public comment from Children's Health Defense supporting NIST CSWP 29 (Initial Public Draft) for NIST Cybersecurity Framework 2.0

Date: October 25, 2023

NIST,

On behalf of Children's Health Defense, a 501(c)(3) nonprofit organization, I am pleased to present this public comment supporting the initial public draft of NIST CSWP 29 for NIST Cybersecurity Framework 2.0.

One Requested Addition to NIST Draft

To harmonize NIST's Cybersecurity Framework 2.0 with federal agency precedent respecting state privacy law, please insert the following statement, which we suggest between lines 654-655 in Section 4.1 on Page 19 of the Public Draft: "Therefore, NIST's Cybersecurity Framework 2.0 respects state law providing stronger privacy protections than federal law for opt-out and opt-in rights."

Reason this Additional Sentence is Necessary

Federal agencies have consistently recognized that the States and the Federal Government both have important roles to play in protecting consumer privacy online,[1] especially where opt-in legal protections are afforded for children's privacy.[2]

[1] *See* Federal Communications Commission (FCC), 2016 CPNI Order, 31 FCC Rcd 13911 (17) at 14047-14048, para. 324 (recognizing that "[w]e have long appreciated and valued the important role states play in upholding the pillars of privacy and protecting customer information...the State AGs are 'active participants in ensuring that [their] citizens have robust privacy protections' and it is critical that they continue that work.").

[2] See e.g., The Children's Online Privacy Protection Act, 16 C.F.R. § 312.5; https://oag.ca.gov/cybersafety/children

For instance, the Federal Communications Commission (FCC) recognized in its 2016 Customer Proprietary Network Information (CPNI) Order that "it is important that we not 'undermine or override state law providing greater privacy protections than federal law,' or impede the critical privacy protections states continue to implement."[3]

That position was also confirmed in the FCC's 2007 CPNI Order, which asserts that the FCC "should allow states to also create rules for protecting CPNI."[4]

Additionally, the FCC observed in its 2002 CPNI Order that,"our state counterparts . . . bring particular expertise to the table regarding competitive conditions and consumer protection issues in their jurisdictions, and privacy regulation, as part of general consumer protection, is not a uniquely federal matter."[5]

With best regards,

Miriam Eckenfels-Garcia, Esq.
Director, EMR & Wireless Program
Children's Health Defense

[3] 2016 CPNI Order, 31 FCC Rcd 13911 (17) at 14049, para. 327.
[4] FCC, 2007 CPNI Order, 22 FCC Rcd at 6958, para. 60.
[5] FCC, 2002 CPNI Order, 17 FCC Rcd at 14891, para. 71.