November 6, 2023

Katherine MacFarland
Cybersecurity Framework
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, Maryland 20899

RE: Comments of ACT | The App Association on the National Institute of Standards and Technology's Draft Cybersecurity Framework 2.0

ACT | The App Association writes to provide input to the National Institute of Standards and Technology (NIST) on its Cybersecurity Framework 2.0 draft (Draft CSF 2.0).[1]

The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Today, the value of the ecosystem the App Association represents—which we call the app economy—is approximately $1.8 trillion and is responsible for 6.1 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution.[2] We applaud NIST's efforts to provide guidance to organizations to better understand, manage, reduce, and communicate cybersecurity risk across emerging technology areas.

The App Association continues to advocate for the development of frameworks that will responsibly support the development, availability, and use of innovations across the app ecosystem. Small app companies and connected device makers are increasingly threatened by cyber-based attacks. With fewer resources than larger entities, small business digital economy innovators need guidance and assistance in cybersecurity threat risk mitigation.

Through its creation and maintenance of the next version of the CSF, NIST has demonstrated its position as a leader and coordinator within the U.S. government in guiding the management of cybersecurity risk across sectors and in aiding communication between technical and nontechnical staff. This has positively influenced private sector cybersecurity risk management practices, U.S. (and other) government requirements that have developed since 2014, and the behaviors of federal, state, and local governments in their own cybersecurity risk management. The CSF embraces a scalable cybersecurity risk management approach which offers a feasible plan of action for smaller entities.

---

[1] https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework
[2] ACT | The App Association, State of the App Economy (2022), https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL.pdf.

The App Association supports NIST's collaborative approach to improving the CSF and welcomes its release of the Draft CSF 2.0. Specifically, the App Association notes its support for the following:

- ***Expanded scope past critical infrastructure:*** As the digital economy continues to expand, powered by smaller business innovators, an improved risk posture across critical infrastructure and non-critical infrastructure entities will be crucial. Therefore, we support the proposed update to the CSF 2.0 that expands the Framework's scope beyond critical infrastructure by now providing insight on risk mitigation for all organizations across government, industry, and academia, regardless of size.

- ***Added "Governance" Function:*** The App Association agrees with NIST's proposal to add a new (sixth) function to its CSF to address governance. We agree that guidance on internal support of CSF implementation will be particularly beneficial to the small business digital economy innovators with limited resources that the App Association represents.

- ***Expanded Implementation Guidance:*** More detailed recommendations for function subcategories will do much to make the CSF actionable to resource-limited small businesses, particularly those in sectors the current CSF may not adequately address. Similarly, NIST's CSF 2.0 Reference Tool will provide a valuable means for, as appropriate, understanding the relationships between the CSF and other resources to enable complementary use of the CSF with other standards and guidances for managing cybersecurity risk.

Moving forward, a focus on small business education and resources will be required for the CSF to realize its full potential. We encourage NIST's support for small business cybersecurity risk management improvements through focused outreach and education, the development of further small business-focused resources, and grants and other means of support for small business implementation of the CSF. The App Association commits to assist NIST in its small business support across these, and other, means, and welcomes the opportunity for further collaboration moving forward.

The App Association appreciates the opportunity to provide input on the updates to the NIST Cybersecurity Framework and looks forward to continued collaboration with NIST and other U.S. governmental partners on this topic.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Leanna Wade
Regulatory Policy Associate

ACT | The App Association