March 17, 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 NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

Introduction and General Views of ACT | The App Association

ACT | The App Association writes to provide input to the National Institute of Standards and Technology (NIST) in response to its request for information to aid in updating the NIST Cybersecurity Framework to account for the changing landscape of cybersecurity risks, technologies, and resources.[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 $1.7 trillion and is responsible for 5.9 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution. We applaud NIST's efforts to provide guidance to organizations to better understand, manage, reduce, and communicate cybersecurity risk across emerging technology areas. We believe that NIST is well-positioned to serve as a leader and coordinator within the U.S. government with respect to realizing a more safe and productive tech economy, and that this request for information takes an important step in establishing this role.

The App Association urges NIST to prioritize the following regarding the scope and approach of the NIST Cybersecurity Framework:

- Adopting a simplistic approach that easily aligns with other resources, mitigating barriers to effective risk management and compliance efforts;
- Utilizing public-private partnerships and collaborations to mitigate security risk to the supply chain;
- Leveraging technical measures like encryption to ensure data privacy; and
- Promoting the Cybersecurity Framework both domestically and abroad.

[1] https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

Adopting a simplistic approach that easily aligns with other resources, lessening barriers to effective risk management and compliance efforts

In general, 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 companies need clear guidance on where and how to share cyber threat information. Key efforts, like the NIST Cybersecurity Framework[2] have embraced a scalable cybersecurity risk management approach which offers a feasible plan of action for smaller entities. As the digital economy continues to expand, powered by smaller organizations that develop software apps, fluid bi-directional sharing of information between and among these entities and the government will be crucial. Therefore, we support the update that expands the Framework's scope beyond critical infrastructure by now providing insight on risk mitigation for all organizations across government, industry, and academia.

Utilizing public-private partnerships and collaborations to mitigate security risk to the supply chain

Pursuant to Executive Order 14028,[3] "Improving the Nation's Cybersecurity," NIST should prioritize cybersecurity supply chain management (C-SCRM) strategy suggestions within the Framework to better identify, assess, and manage first- and third-party risk. The NIST Cybersecurity Framework should continue to endorse and promote public-private partnerships as a necessary tool to mitigate increasing risks to emerging technology within the supply chain.

Additionally, the voluntary timely sharing of cybersecurity threat indicators among organizations from both the public and private sectors will be crucial in the detection, mitigation, and recovery of cybersecurity threats, particularly with the rise of IoT. These organizations, from the most formal to those more loosely organized, can be of assistance to organizations looking to improve their cybersecurity posture through the sharing of threat information. For example, Information Sharing Analysis Organizations (ISAOs), are envisioned in Executive Order 13691[4] to be formed to fulfill the needs of unique communities large and small, sometimes across economic segments. ISAOs, as a complement to Information Sharing Analysis Centers (ISACs), are expected to help address the resource limitations of small businesses as well as the convergence of business models that may make it difficult to determine the best way to engage in information sharing. We encourage NIST to ensure that these key fora are supported in its report to Congress.

---

[2] Federal Register, *Developing a Framework To Improve Critical Infrastructure Cybersecurity* (Feb. 26, 2013), https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity; IT SCC Comments to NIST (2013), https://www.nist.gov/system/files/documents/2017/06/12/20131220_angela_mckay_itscc.pdf.

[3] Executive Order 14028, Improving the Nation's Cybersecurity (May 12, 2021), https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

[4] Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing (Feb. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurityinformation-shari.

Leveraging technical measures like encryption to ensure data privacy

While the rise of the internet of things holds great promise, it also raises more security threats due to a broadened attack vector, necessitating more evolved and dynamic risk management practices. No data is more important to Americans than their own personal information. Our members appreciate this and put extensive resources into ensuring the security and privacy of end-user data to earn and maintain the trust the market demands.

End-user education is a crucial aspect of improving cybersecurity in IoT because many cyber-based attacks are preventable. In evaluating and improving the Cybersecurity Framework, we urge NIST to address how the U.S. government can inform end users across the business and consumer communities of steps to take to ensure that proper cyber "hygiene" is impressed.

The App Association supports fully leveraging technical measures including end-to-end encryption as a critical element to protecting data broadly, enabling key segments of the economy—from banking to national security to healthcare—by protecting access to, and the integrity of, data. Encryption's role should not be understated – without encryption, entire economies and industries are put at a significantly heightened risk of their data being compromised. NIST itself currently plays an important role in promoting the use of encryption. NIST's Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia.[5] NIST also provides the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography-based standards.[6]

Despite the important role encryption plays, some interests persist in demanding that backdoors be built into encryption for the purposes of lawful access. We reject such proposals as mandates that degrade the safety and security of consumers. Worse still, these backdoors could create vulnerabilities that are guaranteed to be exploited by state-backed hackers and criminals. The App Association strongly believes that NIST should recognize the vital role encryption and other technical measures play in securing the data that makes IoT so invaluable and commit to preserving the availability of these tools.

Promoting the Cybersecurity Framework both domestically and abroad

In short, while NIST's comprehensive Framework provides key resources to mitigate cyber threats for a myriad of institutions and industries, it is only as good as the number of entities that know about it. The App Association appreciates NIST's investment in promoting usage of the Cybersecurity Framework, while also educating small businesses on how to use it effectively. We encourage NIST and other U.S. government partners to increase investments in promoting the adoption and use of the Cybersecurity Framework both domestically and internationally. We

[5] See http://csrc.nist.gov/.
[6] See http://csrc.nist.gov/groups/STM/cmvp/.

support NIST engaging in international standards activities that leverage the Framework as part of a broader effort. A collaborative approach that prioritizes engagement with international stakeholders—including governments, industry, and civil society—creates a more inclusive Framework and could set a foundation for future international standards on cyber safety.

Conclusion

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
[redacted]