January 19, 2018

Andrea Arbelaez
National Institute of Standards and Technology
100 Bureau Drive
Stop 2000
Gaithersburg, Maryland 20899

RE: Comments of ACT | The App Association to the National Institute of Standards and Technology regarding *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1 (Draft 2)*

ACT | The App Association writes to provide input to the National Institute of Standards and Technology (NIST) on its *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Draft 2)* (Draft Framework)[1] and companion *Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1* (Draft Roadmap).[2] We appreciate NIST's extensive consultation with stakeholders to help influence and inform updates to these landmark risk management deliverables.

I. Statement of Interest and General Views of the App Association on the Draft Framework and Roadmap

The App Association represents thousands of small business software application development companies and technology firms that create the apps consumers use on mobile devices around the globe. Our members develop the innovative solutions that power the growth of the internet of things (IoT) across modalities and segments of the economy, including for critical infrastructure. The growth of the digital economy depends on the rise of IoT, an encompassing concept where everyday products use the internet to communicate data collected through sensors. IoT has the potential to improve efficiencies in processes, products,

[1] https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

[2] https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf

and services across every sector, from agriculture to retail to healthcare and beyond. By 2019, IoT is projected to be worth more than $947 billion.[3]

The real power of IoT comes from the actionable information gathered by sensors embedded in every connected device. IoT devices are useful for direct consumer interactions, but IoT's greatest value is set to come from what is now commonly referred to as "big data," which are structured or unstructured data sets so large or complex that traditional data processing applications are not sufficient for analysis. As sensors become smaller, cheaper, and more accurate, big data analytics create more efficiencies for consumers and enterprises.

The app ecosystem has been in existence for less than a decade but has experienced explosive growth. Today, the $143 billion app ecosystem[4] is led by U.S. companies, the vast majority of which are startups or small businesses. IoT sensors are included in nearly every fathomable object in daily lives, and the interface for communicating with these devices is likely to remain a mobile app on a smartphone. The rise of the IoT will hinge on the sustained innovation, investment, and growth in the app economy. In short, apps are the interface for the IoT revolution.

While the rise of IoT holds great promise, it also raises security threats. Due to a broadened attack vector, the rise of IoT will require more evolved and dynamic risk management practices. No data is more important to Americans than their own personal information. Our members appreciate the personal value of our data and put extensive resources into ensuring the security and privacy of end user data. These practices help earn and maintain consumer trust and meet market demand.

We support ongoing and emerging public-private partnership initiatives and strategies to improve the nation's cybersecurity risk management efforts, and we continue to work with our members to advance improved cybersecurity risk management practices. Small businesses represent 99.7 percent of all U.S. firms,[5] and they require heightened assistance and must play a more significant role in the development of cybersecurity risk strategies. It is important that policymakers remain mindful of the fact that large companies often dedicate large budgets to create and maintain cybersecurity control processes and have the ability to hire staff and consultants to mitigate cybersecurity risks. Unfortunately, small- and medium-sized enterprises (SMEs) do not. For many of our members, the role of chief security officer may be one of five hats worn by a single employee. The essential role of American small businesses, along with

---

[3] "Internet of Things Market and M2M Communication by Technologies, Platforms and Services (RFID, Sensor Nodes, Gateways, Cloud Management, NFC, ZigBee, SCADA, Software Platform, System Integrators), by M2M Connections and by IoT Components - Global Forecasts to 2019," MarketsandMarkets (November 2014), *available at* http://www.marketsandmarkets.com/Purchase/purchase_report1.asp?id=573.

[4] http://actonline.org/wp-content/uploads/App_Economy_Report_2017_Digital.pdf

[5] https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf.

the unique resource constraints they face, make the NIST Cybersecurity Framework even more important to the security and stability of the nation's critical infrastructure.

We believe the NIST Cybersecurity Framework provides a scalable, flexible, voluntary toolbox that any organization can use to reduce vulnerabilities, prevent intrusions, and mitigate damage caused by cybersecurity attacks. However, our SME members often struggle with the detail and complexity of the Framework or must focus on other market-driven priorities that make it difficult to fully leverage the Framework. Version 1.0 of the Framework is 41 pages long, and the draft of Version 1.1 is even longer at 61 pages. For small businesses, including those in the tech sector, time is valuable. Few have the precious time and resources to review dense documents, particularly those that recommend consultation with large suites of risk management standards or require expensive certifications.

Despite its complexity, we believe the NIST Cybersecurity Framework is a comprehensive guide and should be the touchstone to enhance private sector cybersecurity efforts. Therefore, federally suggested cybersecurity best practices must include references to the Framework and should work to simplify its recommendations. Recognizing this challenge, we commend NIST for developing a deliverable to define the fundamentals of an SME-focused Framework.[6] In addition, the Federal Trade Commission (FTC) develops best practices in the form of its *Start with Security* guide for SMEs, which draws from the NIST Framework.[7]

These SME-targeted efforts by NIST, the FTC, and other agencies are a great start, but we have much work to do. Bottom lines often drive business decisions; therefore, we suggest that future education efforts make the business case (i.e., it provides a return on investment) for using the Framework. The App Association has encouraged greater use of the NIST Cybersecurity Framework throughout our community in a few key ways, including direct member education and public-private partnerships like the Information Technology Sector Coordinating Council. We commit to working closely with NIST and other public and private stakeholders to develop and help implement more small business-focused cybersecurity risk management practices that support the global digital economy.

[6] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

[7] https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

II. Specific Views of the App Association on Proposed Updates to the NIST Cybersecurity Framework

The App Association generally supports NIST's proposed updates to the Cybersecurity Framework. Our specific views and recommendations on the proposed updates include the following:

- The App Association supports NIST's new discussion describing the applicability of the Framework to IoT. IoT products and services have strong potential to improve and protect critical infrastructure, though we note that products and services that reside on the network edge, including IoT, are not critical infrastructure. The Cybersecurity Framework offers an important cybersecurity risk management tool for the digital ecosystem at large.
- Fully leveraging technical measures, like end-to-end encryption, is a critical element to protecting data. Encryption's role should not be understated. Without encryption, the data of entire economies and industries would be placed at a heightened risk of being compromised. NIST 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 industry, government, and academic users.[8] 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.[9]

  The App Association appreciates NIST's efforts to better account for authorization, authentication, and identity proofing, which are important technical protection mechanisms. However, we urge NIST to include a Subcategory for the use of strong encryption (*e.g.*, end-to-end encryption) within the Protect Function's Data Security Category in the "Framework Core."
- We support NIST's addition of Section 4.0, "Self-Assessing Cybersecurity Risk with the Framework," because small businesses often do not have the same resources as larger entities to undertake expensive consultations. NIST's inclusion of Section 4.0 is an important indicator for small businesses to undertake measurements and assessments that scale to their capabilities and risks.

[8] *See* http://csrc.nist.gov/.

[9] *See* http://csrc.nist.gov/groups/STM/cmvp/.

- We support NIST's addition of a new Subcategory related to the vulnerability disclosure lifecycle. The voluntary and timely sharing of cybersecurity threat indicators from public and private sector organizations will be crucial in the detection, mitigation, and recovery of cybersecurity threats, particularly with the rise of IoT. As small and medium app development companies continue to help to expand the digital economy, the bi-directional sharing of information between public and private sector entities will be crucial.

III. Specific Views of the App Association on the Draft Roadmap

The App Association supports proposed updates to the NIST Roadmap. Our specific views and updates include the following:

- The App Association supports the proposal to focus on the cyber-attack lifecycle. As discussed above, the ability to engage in the timely sharing of cybersecurity threat information is crucial to securing America's critical infrastructure and the digital economy at large.
- The App Association supports the proposal to focus on developing a cybersecurity workforce. The App Association is committed to this goal and recently filed detailed comments with NIST on cybersecurity workforce development.[10] As founders of the Computer Science Education Coalition,[11] we stand in partnership with NIST and other public and private stakeholders to develop a robust American cybersecurity workforce that is essential to securing critical infrastructure and the digital economy.
- The App Association supports NIST's proposal to focus on the international aspects, impacts, and alignment of cybersecurity efforts. Increasingly, App Association members seeking to grow their businesses and create new jobs face inflexible, one-size-fits-all, regulatory mandates in key markets around the world. The NIST Cybersecurity Framework must serve as a leading example of a successful, voluntary public-private partnership that addresses dynamic cybersecurity threats to critical infrastructure. While NIST notes several national frameworks are modeled on or similar to the Cybersecurity Framework, we note that many key markets, as well as developing nations, are increasingly adopting top-down, requirement-based approaches to cybersecurity threat mitigation. These examples include China's Cybersecurity Law and the European Union's General Data Protection Regulation. We commit to partner with NIST and other U.S. government entities to promote the Cybersecurity Framework's approach in an international arena.

[10] https://www.nist.gov/sites/default/files/documents/2017/08/04/act_the_app_association.pdf.

[11] http://www.csecoalition.org/.

- Finally, the App Association strongly supports NIST's proposed focus on small business outreach. As discussed above, it is more important than ever to engage small businesses across America on cybersecurity threat mitigation and use of the Cybersecurity Framework. NIST's proposed "listening sessions" will be an important outreach tool and feedback loop to address issues related to uptake and utilization. We also support the development of starter framework profiles.

IV. Conclusion

ACT | The App Association appreciates this opportunity to provide input on the Draft Framework and Roadmap. We remain committed to working with all stakeholders to realize a cyber-secure future for critical infrastructure and the digital economy in the United States.

Sincerely,

Brian Scarpelli
Senior Policy Counsel

Joel Thayer
Policy Counsel

McKenzie Schnell
Associate

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005