September 9, 2016

Attn: Nakia Grayson
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 *Information on Current and Future States of Cybersecurity in the Digital Economy* (Docket No. 160725650–6650–01)

ACT | The App Association writes to provide input to the National Institute of Standards and Technology (NIST) on its Request for Information (RFI), for the Commission on Enhancing National Cybersecurity (Commission), on current and future states of cybersecurity in the digital economy.[1] We appreciate Executive Order 13718's[2] goals and its directive for the Commission to recommend ways to strengthen cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions, and bolstering partnerships between federal, state, and local governments and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices.

ACT | The App Association represents thousands of small business software application development companies and technology firms that create the apps used on mobile devices around the globe. As the world has quickly embraced mobile technology, our member companies have been creating innovative solutions that power the growth of the Internet of Things (IoT) across modalities and segments of the economy. We applaud Executive Order 13718's efforts to understand the digital economy and to examine ways to enhance cybersecurity in both the public and private sectors. These comments address some of the questions raised in the RFI, particularly the "Internet of Things."[3]

The growing "digital economy" which the Commission will formulate cybersecurity-themed recommendations around is a widely-understood concept. However, the digital economy's continued growth is dependent on the rise of IoT, an encompassing concept where everyday

[1] *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 81 Fed. Reg. 19956 (April 25, 2016) (RFC).

[2] Exec. Order No. 13718, Commission on Enhancing National Cybersecurity, 81 FR 7441 (February 9, 2016) (RFI).

[3] *Id.* at 52828.

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org /actonline.org

products use the internet to communicate data collected through sensors. The IoT will enable improved efficiencies in processes, products, and services across every sector. In key segments of the U.S. economy, from agriculture to retail to healthcare and beyond, the rise of IoT is demonstrating efficiencies unheard of even a few years ago. The IoT is projected to be worth more than $947 billion by 2019.[4]

The real power of the IoT comes from the actionable information gathered by sensors embedded in every connected device. IoT devices are useful in direct consumer interactions, but will see the largest value in how the data becomes part of what is now commonly referred to as "big data." For the purposes of this document, we define this term to mean 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 enable more efficiencies across consumer and enterprise use cases.

IoT deployment will be highly use case-dependent. The technology industry, to date, has done well through open Application Programming Interfaces (APIs) and other widely-adopted standards (e.g., TCP/IP) to enable interoperability. For example, in healthcare, a miniaturized and embedded connected medical device must be able to automatically communicate bi-directionally in real-time. This capability enables a healthcare practitioner to monitor a patient's biometric data as well as facilitates the patient's ability to communicate with a caregiver in the event of a medical emergency. Other uses, such as sensors deployed to alert security of an unauthorized presence, may only require the ability to send data to security professionals with minimal or no capability to receive communications.

The app industry has been in existence less than a decade; it has experienced explosive growth alongside the rise of smartphones. As we detail in our annually released *State of the App Economy* report,[5] apps have revolutionized the software industry, touching every sector of the economy. The app economy is a $120 billion ecosystem today that is led by U.S. companies, the vast majority of which are startups or small businesses. While IoT devices encompass every fathomable object in our lives, 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 app economy's continued innovation, investment, and growth. In short, apps are the interface for IoT revolution.

---

[4] "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.

[5] ACT | The App Association, State of the App Economy 2016 (Jan. 2016), available at http://actonline.org/state-of-the-app-economy-2016/.

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.

Based on the above, The App Association makes the following specific recommendations to the Commission:

A Coordinated U.S. Government Approach to Cybersecurity is Essential

Initially, we strongly urge the Commission to recognize that the coordination of federal agencies is essential to enhancing public and private cybersecurity, and to examine ways to bring about a unified approach in this respect. A lack of harmony between federal regulatory agencies, states, and even localities creates legal uncertainties. Due to the rise of the app economy across industries and use cases, countless agencies play key roles in empowering the future of mobile apps and therefore IoT. Agency coordination will not only help avoid duplicative or conflicting regulations and parallel efforts, but it will also help agencies ensure that inquiries into opportunities and actions are well-informed. ACT | The App Association is committed to working in partnership with the U.S. government and other stakeholders towards a coordinated approach to enable the IoT.

The Commission's undertaking also presents a unique and appropriate opportunity to position NIST as a coordinator of other agencies, building on a successful track record. For example, in addition to statutory roles related to electronic health records,[6] standards coordination,[7] and information security standards and guidelines for federal agencies,[8] the National Institute of Standards and Technology (NIST) has led in the development of the Cybersecurity Framework[9] and the National Strategy for Trusted Identities in Cyberspace (NSTIC).[10] We urge the Commission to consider utilizing NIST to coordinate and harmonize the U.S. government's approach to enhancing cybersecurity.

[6] NIST's roles in this context have been articulated in both Federal Health IT strategic plans (2008–2012 and 2011–2015) and in the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009.

[7] Under the National Technology Transfer and Advancement Act (NTTAA), NIST manages assigned responsibility to coordinate federal, state, and local technical standards and conformity assessment activities, as well as coordinates with those in the private sector.

[8] Title III of the E-Government Act of 2002 (P.L. 107-347).

[9] http://www.nist.gov/cyberframework/index.cfm.

[10] http://www.nist.gov/nstic/.

The Commission Should Endorse Flexible and Risk-Based Approaches to Improving Cybersecurity

Prescriptive and/or sector-specific approaches by the U.S. government to cybersecurity pose a serious threat to the ability of organizations—large and small—to detect, respond, and mitigate dynamic cyber-based attacks. By creating the illusion that adhering to a stagnate and finite list of requirements makes an organization "secure," such an approach actually creates an artificial ceiling to the innovative approaches to dealing with cybersecurity threats. We therefore strongly recommend that the Commission promote flexible and scalable risk management approaches to addressing cybersecurity. For example, the Federal Trade Commission's approach to data protection, based on consumer protection principles and a reasonableness standard, is sector-agnostic and encourages a holistic risk-based methodology for organizations.

The Commission's Recommendations Should Affirm the Ability to Utilize Strong Encryption

Fully leveraging technical measures including end-to-end encryption is a critical element to protecting data broadly, by enabling key segments of the economy—from banking to national security to healthcare—through 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.[11] 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.[12]

Despite the important role encryption plays and the Department of Commerce's related responsibilities, 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 state-backed hackers and criminals can exploit. The App Association strongly believes that the Commission 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.

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

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

The Commission Should Recommend an Enhanced Leveraging of the Public-Private Partnership Approach

Public-private partnerships are a useful vehicle for cooperation on ways to confront both current and emerging cyber-based threats, and facilitate the ability to rapidly change in response to ever-developing risks. We are committed to working collaboratively with all public and private stakeholders in these fora to ensure a secure cyberspace. For example, the App Association co-chairs the Federal Communications Commission's (FCC) Commission Communications Security, Reliability, and Interoperability Council (CSRIC) Working Group 6 which has developed "security-by-design" recommendations and best practices for securing the core communications network[13] and continues to develop voluntary assurance mechanisms around these recommendations and best practices.

The Commission Should Endorse and Help Augment Voluntary Sharing of Timely Cybersecurity Threat Information Amongst and Between Public and Private Entities

The voluntary timely sharing of cybersecurity threat indicators among organizations from both the public and private sector 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 those looking to improve their cybersecurity posture through the sharing of threat information. For example, Information Sharing Analysis Organizations (ISAOs), which are envisioned in Executive Order 13691[14] to be formed to fill needs for unique communities large and small, sometimes across economic segments. ISAOs, as a complement to Information Sharing Analysis Centers (ISACs), are expected to help to 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 the Commission to recommend that these key fora are included in its guidance to federal agencies and stakeholders at large.

Further, small app companies and connected device makers are increasingly threatened by cyber attacks. With fewer resources than larger entities, small companies need clear guidance on where and how to share cyber threat information. Other key NIST efforts, such as the NIST Cybersecurity Framework[15] (and others influenced by NIST's approach) have embraced a scalable cybersecurity risk management approach, which lends to a feasible approach by smaller entities. As the digital economy continues to expand, powered by smaller organizations

[13] *See* https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability#block-menu-block-4.

[14] 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-cybersecurity-information-shari.

[15] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

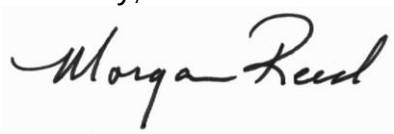
that develop software apps, fluid bi-directional sharing of information between and among these entities and the government will be crucial.

The Commission's Recommendations Should Address the Need for Enhanced Public Awareness and Education

End user education is a crucial aspect of improving cybersecurity in the digital economy because many cyber-based attacks are not sophisticated and are preventable. While we support the continued use of federal education efforts (such as the STOP.THINK.CONNECT campaign), many smaller businesses remain unaware of these resources. We therefore urge that the Commission 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 practiced. This will require a far greater resource commitment from the U.S. government than today.

ACT | The App Association appreciates this opportunity to provide input on the Commission's recommendations to enhance cybersecurity in both the public and private spheres. We stand ready to work with all stakeholders to realize a cyber-secure future for the United States, and encourage you to reach out with any questions.

Sincerely,



Morgan Reed
Executive Director
ACT | The App Association