July 28, 2020

Megan Doscher
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725
Washington, District of Columbia 20230

RE: Comments of ACT | The App Association to the National Telecommunications and Information Administration regarding *Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers* (Docket No. 200609-0154, 85 FR 35919)

ACT | The App Association (the App Association) writes to provide input to the National Telecommunications and Information Administration (NTIA) in response to its request for public comments to inform the establishment of a program to share supply chain security risk information with trusted providers of advanced communications service and suppliers of communications equipment or services.[1] We support NTIA in its efforts to implement Section 8 of the Secure and Trusted Communications Network Act of 2019. The App Association agrees that the 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 internet of things (IoT).

The App Association represents thousands of small business software application development companies and technology firms that create the software apps used on mobile devices and in enterprise systems around the globe. Today, the ecosystem the App Association represents—which we call the app economy—is valued at approximately $1.7 trillion and is responsible for 5.9 million American jobs. Our members develop innovative applications and products to meet the demands of the rapid adoption of mobile technology (including the technologies at issue) that improve workplace productivity, accelerate academic achievement, monitor health, and support the global digital economy. App Association members reside throughout the value chain for communications networks and services (for example, increasingly developing network functions virtualization innovations), and will find themselves directly affected by NTIA's facilitate creation of a new program for the sharing of security risk information with trusted providers. We are committed to working collaboratively with all public and private stakeholders in these fora to ensure a secure cyberspace. For example, the App

[1] *Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers*, 85 Fed Reg 35919 (June 12, 2020).

Association co-chaired 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[2] and continues to develop voluntary assurance mechanisms around these recommendations and best practices. Further, the App Association is an active participant in both the Information Technology[3] and Health Sector[4] Coordinating Councils.

First, the App Association urges NTIA to clarify the relationship of its' new information sharing program to existing U.S. government cybersecurity information sharing constructs. A variety of public-private partnership (PPP) models currently facilitate information sharing, from the most formal to those more loosely organized, which are used by parties to improve their cybersecurity posture through the sharing of threat information and which should be leveraged to benefit NTIA is accomplishing its mission. For example, Information Sharing Analysis Organizations (ISAOs), which are envisioned in Executive Order 13691[5] 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), 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. These and other PPPs 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. NTIA should complement and build on these successful efforts and avoid duplication of them. NTIA's request for information makes no reference to existing information sharing efforts, so NTIA should also ensure that it addresses them and the role of this program in relation to them in its next steps.

[2] See https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-andinteroperability#block-menu-block-4.

[3] https://www.it-scc.org/.

[4] https://healthsectorcouncil.org.

[5] 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.

Second, we urge NTIA's new program for information sharing to seek to advance several concepts that should serve as the foundation for any information sharing construct:

- **Improving Organizations' Security Posture through Shared Situational Awareness:** It is far more likely that an organization will be targeted through an existing attack vector, making the experiences of others who have experienced the attack critical and timely knowledge. NTIA's information sharing program should minimize barriers to participation to enable the sharing of this key information that can allow organizations to prepare for, and to prevent and mitigate, new attacks before they happen. In this way, a successful information sharing program will help "all boats rise" with respect to security risk mitigation.
- **Benefitting from the Crowdsourcing Effect:** No organization, and smaller organizations like App Association members in particular, has the resources to monitor every threat and mitigate every risk. For many App Association members, the Chief Security Officer may wear a number of other hats. NTIA's program should enable organizations to tap into the pooled expertise of others and facilitate community collaboration and learning.
- **Timely Sharing to Improve Confidence and Resilience:** Because of the rapid way that supply chain risks evolve, App Association members prioritize staying informed about the latest developments as well as techniques for mitigating risk. NTIA's program should leverage economies of scale to deliver enhancements in supply chain security and improved safety against threats without bearing additional cost.
- **Better Supply Chain Security Innovation:** Supply chain risk awareness also improves an organization's ability to mature advanced threat warning systems. NTIA's program should ensure that security professionals can ensure their organizations are engaged and developing along with new challenges, standards, and best practices.

Third, the App Association urges NTIA to recognize that standardized processes for the security of supply chains already exist, several which the U.S. government itself has developed. These standards are based on extensive engagement with and contributions from both the U.S. government as well as leading private sector interests and represent leading approaches to supply chain risk management. Such standards include:

- ISO 28001 (Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance);[6]
- ISO/IEC 20243-2:2018 [ISO/IEC 20243-2:2018] (Information technology — Open Trusted Technology Provider Standard (O-TTPS) — Mitigating maliciously

[6] https://www.iso.org/standard/45654.html.

tainted and counterfeit products — Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018);[7]

- ISO/IEC 15408 Common Criteria;[8]
- National Institute of Standards and Technology (NIST) standards addressing supply chain security including:
  - The NIST Cybersecurity Framework;[9]
  - NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations);[10]
  - NIST 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations);[11] and
  - NIST 800-161 (Supply Chain Risk Management Practices for Federal Information Systems and Organizations).[12]
- Department of Defense (DoD) Defense Federal Acquisition Regulations (DFARs) Subpart 239.73 (Requirements for Information Relating to Supply Chain Risk).[13]

The App Association requests that NTIA's program align with and complement these leading standards and requirements that all include supply chain security risk management. Notably, these standards and others should inform many of the questions NTIA poses in its request for comment, including what information, if any, is unique to "supply chain risk information;" whether supply chain security risks beyond those Congress specified should be included in an information security program; how a "trusted" providers and suppliers should be determined; and others.

Further, the App Association requests that NTIA provide parties who attest to adherence to such standards with safe harbor from liability under this program; in the alternative, use of such standards should provide a strong presumption of compliance. Such an approach would maximize NTIA's valuable resources by allowing it to focus on areas of most concern and need in operating an information sharing program.

[7] https://www.iso.org/standard/74400.html.

[8] https://www.commoncriteriaportal.org/.

[9] https://www.nist.gov/cyberframework.

[10] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[11] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

[12] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[13] http://www.acq.osd.mil/dpap/dars/dfars/html/current/239_73.htm.

Fourth, we appreciate NTIA's proposal to structure that program primarily to promote the flow of risk information from the government to small and rural providers and suppliers. We urge NTIA to mitigate the barriers and risks, namely legal and financial, that small businesses face in receiving, sharing, and acting on timely supply chain security threat information. Further, NTIA's efforts to focus on small businesses should include a significant educational component targeted to this community, which the App Association commits to assist in any way possible.

The App Association appreciates the opportunity to provide input to NTIA on its future program to share supply chain security risk information with trusted providers of advanced communications service and suppliers of communications equipment or services.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

ACT | The App Association
1401 K St NW (Ste 500)
Washington, DC 20005
p: +1 517-507-1446
bscarpelli@actonline.org