October 28, 2024

Alan F. Estevez
Under Secretary of Commerce for Industry and Security
Bureau of Industry and Security
1401 Constitution Avenue NW
Washington, District of Columbia 20230

RE: Comments of ACT | The App Association on the Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles [Docket No. 240919-0245]

Dear Mr. Estevez:

ACT | The App Association (App Association) writes in response to the Department of Commerce's (DOC's) Bureau of Industry and Security (BIS) request for comments on the notice of proposed rulemaking (NPRM) on securing the information and communications technology and services (ICTS) supply chain for connected vehicles.[1]

I. Introduction and Statement of Interest

The App Association is a global policy trade association for the small business technology developer community. 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. App developers like our members also play a critical role in developing connected vehicle innovations throughout ICTS connected vehicle supply chains. 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]

II. Connected Vehicles are Part of a Broader Digital Ecosystem of Applications and Services

The App Association appreciates BIS' request for input on the ICTS supply chain for connected vehicles (CVs) in the United States and shares the goal of realizing strong, sustainable, and secure ICTS supply chains across sectors. App Association members develop software and connected hardware at key points throughout ICTS connected vehicle supply chains. Connected vehicles leverage GPS, radar, photos, and other data points securely and

[1] 89 FR 79088.
[2] ACT | The App Association, State of the App Economy (2022), https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL.pdf.

appropriately collected, which App Association members often leverage to innovate and compete.

As BIS considers new rules for the security of the ICTS supply chain, the App Association urges consideration of the reality that connected vehicles are a part of the broader digital economy. Many connected vehicles on the road today have access to and make use of third-party applications and services, and this will only increase as the digital ecosystem around connected vehicles develops. BIS should be mindful that, while focused on security, its rules could amount to harmful digital trade barriers if not drafted with appropriate scope.

The small business innovators we represent prioritize the following general principles for policies affecting the international digital economy:

- ***Enabling Cross-Border Data Flows:*** The seamless flow of data between economies and across political borders is essential to the functioning of the global economy. Small business technology developers must be able to rely on unfettered data flows as they seek access to new markets.
- ***Avoiding Data Localization Policies:*** American companies looking to expand into new markets often face regulations that force them and other foreign providers to build and/or use local infrastructure in the country. Data localization requirements seriously hinder imports and exports, reduce an economy's international competitiveness, and undermine domestic economic diversification. Our members do not have the resources to build or maintain unique infrastructure in every country in which they do business, and these requirements effectively exclude them from commerce.
- ***Prohibiting Customs Duties and Digital Service Taxes on Digital Content:*** American app developers and technology companies must take advantage of the internet's global nature to reach the 95 percent of customers who live outside of the United States. However, the tolling of data crossing political borders with the purpose of collecting customs duties directly contributes to the balkanization of the internet. These practices jeopardize the efficiency of the internet and effectively block innovative products and services from market entry.
- ***Ensuring Market Entry is Not Contingent on Source Code Transfer or Inspection:*** Some governments have proposed policies that require companies to transfer, or provide access to, proprietary source code as a requirement for legal market entry. Intellectual property is the lifeblood of app developers' and tech companies' innovation; the transfer of source code presents an untenable risk of theft and piracy. Government policies that pose these requirements are serious disincentives to international trade and a non-starter for the App Association's members.
- ***Preserving the Ability to Utilize Strong Encryption Techniques to Protect End User Security and Privacy:*** Global digital trade depends on the use of strong encryption techniques to keep users safe from harms like identity theft. However, some governments continue to demand that backdoors be built into encryption keys for the purpose of government access. These policies jeopardize the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. From a privacy and security standpoint, the viability of an app company's product depends on the trust of its end users.
- ***Securing Intellectual Property Protections:*** The infringement and theft of intellectual property and trade secrets threatens the success of the App Association's members and

hurts the billions of consumers who rely on these app-based digital products and services. These intellectual property violations can lead to customer data loss, interruption of service, revenue loss, and reputational damage – each alone a potential "end-of-life" occurrence for a small app development company. The adequate and effective protection and enforcement of intellectual property rights is critical to the digital economy innovation and growth.

- ***Avoiding the Misapplication of Competition Laws to New and Emerging Technology Markets:*** Various regulators, including key trading partners, are currently considering or implementing policies that jeopardize the functionality of mobile operating systems and software distribution platforms that have enabled countless American small businesses to grow. Since its inception, the app economy has successfully operated under an agency-sale relationship that has yielded lower overhead costs, greater consumer access, simplified market entry, and strengthened intellectual property protections for app developers with little-to-no government influence. Foreign governments regulating digital platforms inconsistent with U.S. law will upend this harmonious relationship enjoyed by small-business app developers and mobile platforms, undermine consumer privacy, and ultimately serve as significant trade barriers.

III. BIS ICTS Rules Should Adopt Clear and Targeted Definitions

The App Association appreciates BIS's attempts to resolve vague definitions for connected vehicles, which could, if drafted broadly, include all segments of the automotive industry. We urge BIS to clearly and specifically define vehicle classes/supply chains to which it seeks to apply ICTS rules in order to provide clarity to the industry about impacted products, providing key use cases as guidance/to advance understanding.

IV. BIS ICTS Rules Should Avoid Data Localization Requirements

As discussed above, data and processing localization requirements ignore the efficiencies and security of distributed cloud computing and do not translate to assurances of data security, instead creating unnecessary barriers to trade and innovation. The App Association appreciates BIS's avoidance of local data storage or processing mandates in its rules. Such requirements would be inconsistent with connected vehicle industry leading standards for data collection and processing, which are deferred to by the U.S. Department of Transportation.[3]

V. BIS ICTS Rules Should Preserve the Ability to Secure Data and Supply Chains Using Encryption

Whether as contractors or as business partners, App Association members are required to share sensitive information with OEMs of CVs in the normal course of business using cloud computing services. They rely on risk management best practices and technical protection mechanisms to securely accomplish these vital interactions, which may include remote access and/or providing firmware or software updates. As it advances rules for ICTS connected

[3] https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

vehicles, BIS should maintain the ability to leverage these technical protection mechanisms such as encryption, without which the secure data flows that underpin secure supply chains could not exist.

VI. BIS ICTS Connected Vehicle Rules Should Align with Leading Risk Management Practices

The App Association also urges BIS to align with leading federal guidance from the National Institute of Standards and Technology (NIST) on cybersecurity and supply chain risk management[4] as well as sector-specific guidance from the National Highway Traffic Safety Administration (NHTSA),[5] when crafting its regulations, which enable the scaling of risk mitigation practices to the harms presented. Such an alignment will ensure that BIS rules enable the industry to most efficiently identify, assess, and mitigate the risks associated with the distributed and interconnected nature of ICTS connected vehicle supply chains across the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction).

VII. Conclusion

The App Association appreciates the opportunity to provide comments to BIS on securing the ICTS connected vehicle supply chains.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

Priya Nair
Senior IP Policy Counsel

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

[4] E.g., https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management.
[5] https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf.