May 15, 2017

TO:

Chinese Communist Party Central Leading Group for Cyberspace Affairs
Office of the Central Leading Small Group for Cyberspace Affairs
Cyberspace Administration of China
225 Chaoyangmen Nei Dajie, Dongcheng District, Beijing 100010

By CC to:
Standing Committee of the National People's Congress
No. 23 Xijiaominxiang, Xicheng District, Beijing 100805

Ministry of Commerce
No. 2 Dong Chang'An Avenue, Beijing 100731

Respected Leading Group Members:

As the June 1 implementation date of the Cybersecurity Law approaches, our organizations are writing to remind you of our significant concerns about various aspects of the law and to request a delay in its entry into force.

Our organizations represent companies across a wide range of industries, with deep, long-standing commercial ties with China. We appreciate the Chinese government acknowledgment of international industry groups' concerns regarding China's Cybersecurity Law and related pending cybersecurity regulations and measures – including in sector-specific measures – as expressed in our letter to Chinese Premier Li Keqiang on August 10, 2016 and in our letter to your Leading Group on November 11, 2016.

Our members are steadfast in their commitment to work with the Chinese government to find solutions that not only support China's security, economic, and social goals but also address the legitimate concerns of international industry. However, we are deeply concerned that current and pending security-related rules will effectively erect trade barriers along national boundaries that effectively bar participation in your market and affect companies across industry sectors that rely on information technology goods and services to conduct business. China's current course risks compromising its legitimate security objectives (and may even weaken security) while burdening industry and undermining the foundation of China's relations with its commercial partners. Indeed, our organizations remain concerned that China's current approach is leading to greater separation rather than integration among our economies. Further, at a time of significant political and social change globally, we are concerned such policies may exacerbate troubling trends in markets around the world that move China away from cooperative trade and the benefits of global trade.

We have been and remain hopeful that the Chinese government at the highest levels will take concrete, meaningful steps to implement its past commitments to work with foreign counterparts to promote pro-competitive and non-discriminatory information communication technology

(ICT) security policies. These commitments include ensuring that ICT security measures should be narrowly tailored, take into account international norms, be nondiscriminatory, and not unnecessarily impose nationality-based conditions or restrictions on the purchase, sale, or use of ICT products and services by commercial enterprises.

Regrettably, a number of recently-issued draft measures would place far-reaching restrictions on the export of data, restrict participation by foreign companies in China's cloud market, and institute onerous restrictions on commercial encryption products that could adversely impact billions of dollars in cross-border trade. These drafts suggest China is continuing to move away from its bilateral commitments, international obligations, and global norms, not toward them. They also underscore the asymmetry between the access that Chinese companies enjoy in other markets and the access foreign companies have in China. For example, Chinese companies are generally able to fully own and control data centers and cloud-related services around the world with no foreign equity restrictions or technology transfer requirements, and they can do so under their brand name and without any need to obtain a license. Yet it is impossible for foreign cloud companies to do the same in China. All countries have legitimate concerns over privacy and national security, but China is the principal country addressing these concerns by requiring foreign companies to transfer their technology and to surrender their brand and operating control in order to do business. Requirements that are being advanced by Chinese authorities as neutral and non-discriminatory are instead having the effect of excluding foreign competitors who cannot meet them because of technology transfer, encryption and other requirements.

It is critical that pending cybersecurity regulations—including those in sector-specific measures that promote or require the use of secure and controllable technologies as well as future implementing regulations and standards for the Cybersecurity Law—comply with China's World Trade Organization (WTO) commitments and encourage the adoption of international models that support China's development as a global hub for technology and services. We are concerned that these commitments are undermined by public statements, policies, plans, regulations and other forms of high-level guidance that call for indigenous and controllable substitution plans for information technology products and services.

Provisions in the new Cybersecurity Law and related measures that mandate broad data residency requirements and restrictions of cross-border data flows,[1] trade-inhibiting security reviews and requirements for ICT products and services, forced transfer of technology, and broad requirements for data sharing and technical assistance raise serious concerns for companies with global operations. These measures will add costly burdens, restrict competition and may decrease the security of products and jeopardize the privacy of Chinese citizens.

We therefore request that China delay implementation of the Cybersecurity Law and related measures until such time that they are consistent with President Xi's commitments in 2016:[2] ICT

[1] The recently-released *Draft Security Assessment Measures for Cross-Border Transfer of Personal Information and Important Data* is particularly troubling in that it expands the purview beyond critical information infrastructure owners, as outlined in the Cybersecurity Law, to all network operators and even individuals. This will pose numerous challenges for multi-national companies, both foreign and domestic, that must transfer data as part of daily business operations**.**

[2] https://obamawhitehouse.archives.gov/the-press-office/2016/09/04/fact-sheet-us-china-economic-relations

measures should be narrowly tailored, reflect international norms, be non-discriminatory and consistent with WTO agreements to which China is a party. In order to ensure compliance with international standards and best security practices, we further recommend that Chinese agencies consult and work closely with industry experts and other stakeholders throughout the regulatory and implementation process. As China prepares to implement its Cybersecurity Law it will become increasingly important that companies operating in China have a clear understanding of how the law will be enforced. We request China's assistance in this regard.

Our concerns encompass enormously consequential issues for China's economy, its relations with economic and commercial partners, and the global economy. We appreciate the challenges that regulators around the world face in managing new technologies and addressing legitimate security concerns. However, we respectfully urge that China's cybersecurity policies going forward better reflect a globalized information and communications technology sector, advance market competition, promote transparency, and allow commercial procurers to set their own requirements for the equipment and software they purchase. In our collective experiences, those economies that adhere to these principles will be both stronger and more secure than those that do not.

We appreciate your consideration of our concerns and look forward to working with you on approaches based on internationally-agreed standards, including those adopted by widely respected standards development organizations, to better ensure China's cybersecurity without sacrificing the benefits of global trade.

Signed,

ACT | The App Association
AdvaMed, the Advanced Medical Technology Association
American Chamber of Commerce in China
The American Chamber of Commerce in Korea
The American Chamber of Commerce in Shanghai
American Chamber of Commerce in South China
American Council of Life Insurers (ACLI)
American Insurance Association (AIA)
Arizona Technology Council
Australian Chamber of Commerce and Industry
Australian Industry Group (Ai Group)
Bitkom
BSA | The Software Alliance (BSA)
BusinessEurope
Canada-China Business Council
Coalition of Services Industries
Communications and Information Network Association of Japan (CIAJ)
Computer & Communications Industry Association
Computing Technology Industry Association (CompTIA)
The Council of Insurance Agents and Brokers (CIAB)
Danish Securities Dealers Association

DIGITALEUROPE
European Banking Federation (EBF)
European Services Forum
Financial Services Forum
Information Technology Industry Council (ITI)
Insured Retirement Institute
Internet Association
Internet Infrastructure Coalition / I2Coalition
The Japan Chamber of Commerce and Industry (JCCI)
Japan Electronics and Information Technology Industries Association (JEITA)
The Japanese Chamber of Commerce and Industry in China (CJCCI)
Japanese Information Technology Services Industry Association
Keidanren
Korea-China Business Council
Mexican Association of Insurance Institutions (AMIS)
National Association of Manufacturers
National Foreign Trade Council
PCI Property Casualty Insurers Association of America
Reinsurance Association of America
Securities Industry & Financial Markets Association (SIFMA)
Semiconductor Industry Association (SIA)
Singapore Chamber of Commerce & Industry in China (SingCham)
Software and Information Industry Association (SIIA)
Tech Titans
TechNet
techUK
Telecommunications Industry Association (TIA)
TheCityUK
The Travel Technology Association
U.S. Chamber of Commerce
United States Council for International Business (USCIB)
US-China Business Council
Washington Technology Industry Association