February 4, 2015

The Honorable John Kerry
United States Secretary of State
U.S. Department of State
Washington, DC 20037

The Honorable Jacob J. Lew
United States Secretary of the Treasury
U.S. Department of the Treasury
Washington, DC 20005

The Honorable Penny Pritzker
United States Secretary of Commerce
U.S. Department of Commerce
Washington, DC 20230

The Honorable Michael Froman
United States Trade Representative
Executive Office of the President
Washington, DC 20508

Jeffrey Zients
Director, National Economic Council and Assistant to the President for Economic Policy
Executive Office of the President
Washington, DC 20508

Dear Secretary Kerry, Secretary Lew, Secretary Kerry, Ambassador Froman, and Director Zients:

The undersigned associations, representing a wide range of the U.S. business community, request your immediate action to work with Chinese officials to reverse an alarming number of troubling, new Chinese government policies impacting the information and communications technology (ICT) sector. If implemented, these policies will have a significant negative impact on U.S. ICT companies' market opportunities in China by imposing sweeping indigenous production and control burdens on ICT products based on "cybersecurity" justifications. These rules also raise serious questions regarding China's international trade commitments and its bilateral commitments to the United States. We request your prompt engagement with the Chinese government to reverse these policies and halt their implementation.

To date, China has issued specific measures requiring the deployment of "secure and controllable" technology and software in the banking sectors. To qualify as "secure and controllable," ICT products and services must, among other things, undergo intrusive security testing, contain indigenous Chinese intellectual property (IP), implement local encryption algorithms, and comply with country-specific (Chinese) security standards. The same policies also mandate that vendors disclose source code and other sensitive and proprietary information to the Chinese government and engineer their products so as to restrict the flow of cross-border data. According to official Chinese government statements, many of these policies will be reviewed and potentially expanded to telecommunications and other sectors during an upcoming annual meeting of the Central Leading Small Group for Cyberspace Affairs, which is chaired by Chinese President Xi Jinping.

If fully implemented, these policies threaten the ability of U.S. ICT companies to participate in the $465 billion ICT market[1] in China. Our companies' losses in turn will translate into decreased research and development (R&D) investments in the United States, harming U.S. jobs and innovation. The policies also

[1] http://bits.blogs.nytimes.com/2014/12/02/in-2015-technology-shifts-accelerate-and-china-rules-idc-predicts/

will likely have a significant adverse impact on additional U.S. industry sectors invested in China, ranging from energy to finance, telecommunications and other services. The policies' requirements that ICT products restrict cross-border data flows will also likely have a clear impact on the manufacturing sector. The policies are regrettably indicative of the increasingly negative investment climate for foreign ICT companies in China, create another market barrier for foreign financial services and telecommunications companies, and call into question China's international trade commitments. Contrary to the stated goals of Chinese authorities, these policies likely will not strengthen, but will rather decrease, cybersecurity in China because they will restrict the flow of leading-edge security technologies into that market.

We have raised our concerns directly with the leadership in Beijing in the attached January 28, 2015 letter to the Chinese Communist Party Central Leading Group for Cyberspace Affairs. We also have discussed this issue with your staff, who have swiftly and substantively engaged with us. We would appreciate your prompt attention to these extremely troubling developments as well as an opportunity to meet with you to provide additional details of the disruptive impact of these policies on U.S. commerce with China.

cc: J. Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator at the National Security Council.
Ambassador Robert Holleyman, Deputy United States Trade Representative.
Alex Niejelow, Chief of Staff to the U.S. Intellectual Property Enforcement Coordinator, Executive Office of the President.

Sincerely,

American Chamber of Commerce in China
American Chamber of Commerce in Shanghai
BSA | The Software Alliance
Coalition of Services Industries (CSI)
The Consumer Electronics Association (CEA)
Emergency Committee for American Trade (ECAT)
Information Technology Industry Council (ITI)
National Association of Manufacturers (NAM)
National Foreign Trade Council (NFTC)
Semiconductor Industry Association (SIA)
Software and Information Industry Association (SIIA)
Telecommunications Industry Association (TIA)
TechAmerica, powered by CompTIA
TechNet
United States Council for International Business (USCIB)
U.S. Chamber of Commerce
United States Information Technology Office (USITO)

Attached: Multi-association letter to Chinese Communist Party Central Leading Group for Cyberspace Affairs, January 28, 2015