THE US-CHINA BUSINESS COUNCIL
美 中 贸 易 全 国 委 员 会

April 8, 2013

The Honorable Harry Reid
Majority Leader
U.S. Senate
Washington, DC 20510

The Honorable John Boehner
Speaker of the House
U.S. House of Representatives
Washington, DC 20515

The Honorable Mitch McConnell
Minority Leader
U.S. Senate
Washington, DC 20510

The Honorable Nancy Pelosi
Minority Leader
U.S. House of Representatives
Washington, DC 20515

Dear Majority Leader Reid, Speaker Boehner, Minority Leader McConnell and Minority Leader Pelosi:

I write today in opposition to Section 516 of H.R. 933, the 2013 Full-Year Continuing Appropriations Act, which covers appropriations through September 30, 2013. This provision bar the Departments of Commerce and Justice, NASA and the National Science Foundation from purchasing information technology systems without first conducting a cyber-espionage or sabotage risk assessment, including risks due to the product being "produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China." I urge you to ensure that similar provisions are not included in subsequent appropriations measures.

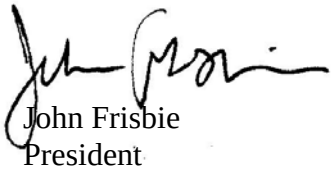
The national security of the United States is critical, but it must not be used as a means of protectionism. As colleagues at other associations have recently noted to you, product security is a function of how a product is made, used, and maintained, rather than by whom or where it is made. Imposing a country-specific risk assessment creates a false sense of security if the goal is to improve our nation's cybersecurity. For example, the White House completed its own investigation of one Chinese technology company in 2012, Huawei, and concluded there was no evidence of espionage, but that the company's products have flaws that could be more easily exploited by hackers. Based on that, it would be prudent for end users to be aware of those risks, but going a step further and stopping purchases of anything made in China goes beyond any reasonable security concern.

Cybersecurity is of increasing concern to US companies, regardless of the source, and it should be a priority for the US government to address. To do so, the US and Chinese governments should cooperate to address cybersecurity issues as they impact the commercial relationship,

starting with one fundamental premise: commercial espionage should not be tolerated and if it is not addressed, it could undermine a constructive commercial relationship.

As you consider legislation during this congress on cybersecurity, including in appropriations measures for FY 2014, I encourage you to work with American technology companies that are at the forefront of innovative technologies about what steps the United States should be taking to enhance its security in this area. Those steps should not be based on country-specific restrictions but instead on appropriate and effective tools to achieve that goal.

Sincerely,



John Frisbie
President