April 4, 2013

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

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

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

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

Dear Speaker Boehner, Democratic Leader Pelosi, Majority Leader Reid, and Republican Leader McConnell:

The undersigned associations are writing to express our concern with language included in Section 516 of P.L. 113-6, the Consolidated and Further Continuing Appropriations Act for Fiscal Year 2013, which was signed into law by President Obama on March 26, 2013. This provision will bar the Departments of Commerce and Justice, the National Aeronautics and Space Administration, and the National Science Foundation from acquiring information technology (IT) systems unless "the head of the entity, in consultation with the Federal Bureau of Investigation or other appropriate Federal entity" has made a risk assessment of potential "cyber-espionage or sabotage...associated with such system being produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China." Given the expedited manner in which this provision was enacted, we ask the Congress to review the security implications and competitive impact of this requirement, and consider a more constructive approach to this issue. We also seek your support to ensure similar language is not included in other legislative vehicles.

Our associations represent thousands of U.S. technology companies. As designers, producers and consumers of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy and are aligned with the U.S. and other governments' goals to enhance cybersecurity. We understand and share Congress' concern about the security of the U.S. government's IT infrastructure.

The IT assessment requirements in Section 516, however, set a troubling and counterproductive precedent that could have significant international repercussions and put U.S.-based global IT companies at a competitive disadvantage in global markets. Fundamentally, product security is a function of how a product is made, used, and maintained, not by whom or where it is made. Geographic-based restrictions run the risk of creating a false sense of security when it comes to advancing our national cybersecurity interests. At a time when greater global cooperation and collaboration is essential to improve cybersecurity, geographic-based restrictions in any form risk undermining the advancement of global best practices and standards on cybersecurity.

We are concerned Section 516 could result in the following:

- Impede the U.S. government's ability to protect itself through use of the latest cutting-edge IT products. The requirement to assess every IT product purchase, absent any triggering threshold, will likely slow the federal acquisition process and put impacted federal agencies behind the security innovation curve because they would not be acquiring and using the latest security innovations.

- Put federal civilian agencies in conflict with the Department of Defense's (DoD) cybersecurity procurement reforms. The recent *Department of Defense Strategy for Operating in Cyberspace* recommended reforming the acquisition process, stating "DoD's acquisition processes and regulations must match the technology development life cycle. With information technology, this means cycles of 12 to 36 months, not seven or eight years."
- Fuel potential retaliation. The Chinese government may choose to retaliate against U.S.-based IT vendors by enacting a similar policy for screening IT system purchases in China.
- Encourage copycat legislation. Governments in other countries may seek to emulate this policy, harming U.S. IT vendors who wish to sell in those markets. Similar policies are already being pursued by some foreign governments. We are concerned this provision would severely undermine the U.S. government's efforts to contain these policies.

U.S. IT companies' significant global sales contribute substantially to the revenue we invest in domestic R&D, and new products and services. All of our members have a shared commitment to ensure their IT products and services reflect the latest and greatest in cybersecurity protection, and that cybersecurity policies advance this goal while maintaining our companies' innovative and competitive potential in global markets. Section 516 creates challenges that could undermine U.S.-based companies' global competitiveness.

Section 516 was not subject to committee hearings or markup, and was included in must-pass funding legislation that went through an expedited legislative process with limited opportunities for amendment. The global IT sector is committed to working with Congress and the Administration to consider constructive approaches that avoid geographic-based restrictions and focus instead on the appropriate and effective methods to meet our cybersecurity challenges. In the near term, we strongly encourage a meaningful bilateral dialogue between the United States and China to address cybersecurity concerns in a manner consistent with best security and trade practices.

Sincerely,

BSA | The Software Alliance
Emergency Committee for American Trade (ECAT)
Information Technology Industry Council (ITI)
Semiconductor Industry Association (SIA)
Software & Information Industry Association (SIIA)
TechAmerica
Technology CEO Council
Telecommunications Industry Association (TIA)
U.S. Chamber of Commerce
U.S. Council for International Business (USCIB)
U.S. Information Technology Office (USITO)

CC: J. Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, Executive Office of the President