July 17, 2013

The Honorable Hal Rogers
Chairman, Committee on Appropriations
U.S. House of Representatives
Washington, DC 20510

The Honorable Nita Lowey
Ranking Member, Committee on Appropriations
U.S. House of Representatives
Washington, DC 20510

The Honorable Frank Wolf
Chairman, Committee on Appropriations
Subcommittee on Commerce, Justice, Science and Related Agencies
U.S. House of Representatives
Washington, DC 20510

The Honorable Chaka Fattah
U.S. House of Representatives
Ranking Member, Committee on Appropriations
Subcommittee on Commerce, Justice, Science and Related Agencies
Washington, DC 20510

Dear Chairmen Rogers and Wolf, and Ranking Members Lowe and Fattah:

We write to express our strong concerns with Section 515 of the Fiscal Year (FY) 2014 Commerce, Justice, and Science (CJS) Appropriations bill being considered by the House Appropriations Committee. Section 515, which is identical to language included in the FY 2013 Continuing Resolution (CR), would prevent all Commerce, Justice, Science and Related Agencies from buying information technology (IT) systems that are produced, manufactured, or assembled by an entity that is owned, directed, or subsidized by China, with a very limited exception based on "national interest." Section 515 also bars any IT procurements until the Federal Bureau of Investigation has carried out an assessment of the risk of cyber espionage.

We commend the CJS Subcommittee Chairman for his interest in seeking greater security of federal government systems. However, since enactment of the FY 2013 CR, the effects of this

restriction have been detrimental to government security and to U.S. business both domestically and abroad. Consequently, we recommend that the Committee work with stakeholders on an alternative approach that would ensure the most effective solutions are available to the federal government.

Specifically, the provision is impeding the U.S. government's ability to protect its networks by requiring IT purchase assessments that substantially slow the federal acquisition process and put impacted federal agencies behind the security curve. This is particularly onerous for companies and government agencies that have partnered in performing mission-critical functions, but now face acquisitions that are currently being held in abeyance.

The provision focuses limited federal cybersecurity resources on a country-of-origin determination, rather than actionable cyber risks and threats, and the actual security profile of the IT product. Identifying a particular country-of-origin does not in itself determine the security of IT products. Rather, security is truly a function of how a product is made, rather than where it is produced.

Finally, at a time of heightened international attention to cybersecurity, the provision is compromising U.S. economic security, and has resulted in some foreign governments threatening—and in some cases taking—retaliatory actions against U.S.-based companies abroad. Because overseas sales account for a majority of the revenues of many U.S. IT firms, such retaliation puts at risk the jobs of thousands of American workers as well as the long-term competitiveness of U.S. companies.

For these reasons, we welcome the opportunity to work with you and your Senate colleagues to develop alternative approaches that advance the goals of IT product security without putting U.S. IT competitiveness in global markets at risk.

Sincerely,

BSA | The Software Alliance
Information Technology Industry Council (ITI)
SIIA – Software & Information Industry Association
Silicon Valley Leadership Group
TechAmerica
U.S. Chamber of Commerce
U.S. Council for International Business (USCIB)

CC: The Honorable John Boehner, Speaker of the House
The Honorable Nancy Pelosi, Democratic Leader
The Honorable Harry Reid, Majority Leader
The Honorable Mitch McConnell, Minority Leader
The Honorable Barbara Mikulski, Chairman, Senate Committee on Appropriations
The Honorable Richard Shelby, Chairman, Senate Committee on Appropriations
Sylvia Matthews Burwell, Director, Office of Management and Budget
J. Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, Executive Office of the President
Dan M. Tangherlini, Administrator, General Services Administration