December 10, 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
Ranking Member, Committee on Appropriations
Subcommittee on Commerce, Justice, Science and Related Agencies
U.S. House of Representatives
Washington, DC 20510

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

As you and your colleagues seek to finalize federal spending levels for the remainder of Fiscal Year (FY) 2014, we urge you to consider substituting Section 516 of the Consolidated and Further Continuing Appropriations Act of 2013, Pub. L. 113-6 (Section 516), with the language proposed in Section 515 of S. 1329, the FY 2014 Commerce, Justice, Science and Related Agencies Appropriations Bill as reported by the Senate Committee on Appropriations on July 18, 2013.

We are in agreement with members of Congress that improved security of federal government systems is a necessity. However, U.S. industry has suffered from significant unintended consequences as a result of the implementation of Section 516. We believe Section 515 of S. 1329 would accomplish the important goal we all share of advancing the cybersecurity of

government systems, without creating unintended consequences that have harmful implications for both federal government procurement and global trade.

Negative Impact of Pub. L. 113-6 (Section 516): Under Section 516 as written, agencies cannot prioritize security resources on riskier IT systems, which spreads these resources thinly at the expense of important mission-critical systems. Instead, the law 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 determine the security of IT products; rather, security is truly a function of how a product is made, rather than where it is produced.

Further, the law has unnecessarily slowed federal purchases of needed security technologies, putting key federal agencies behind the technology cycle and leaving them vulnerable. Some U.S. companies have had to cease, or interrupt, work at agencies with which they partner on projects significant to national security.

Finally, the provision is putting U.S. companies at risk of losing sales internationally, compromising U.S. economic security and U.S. job stability in our sector. Some foreign governments have used Section 516's country-of-origin discrimination to justify their own actions to keep U.S.-based companies out of their markets.

Security Benefits of Section 515: Opting for Section 515 of S. 1329 ensures the law will not undermine the long-term competitiveness of U.S. companies, and safeguards continued investment in U.S.-based research and development—including in leading-edge security products our government needs – while achieving the goal of a more assured government supply chain. Specifically, Section 515, indeed, would enable US agencies to prioritize security resources on IT systems. Moreover, by focusing on broad categories of cyber threats emanating internationally and domestically – rather than using a country-of-origin determination – Section 515 would avoid the unintended, but highly negative effects we gave seen in just a few months. These include: (1) the slowdown and cessation of IT procurements; (2) the interruption and halt of company work on key projects at critical agencies owing to burdensome, overly broad supply chain inspection requirements; and (3) the creation of incentives for some foreign governments to erect trade barriers or take other discriminatory actions that end up hurting US companies in one our nation's most dynamic and productive sectors.

For these reasons, we urge you to advance the cybersecurity of federal agencies and the economic security of the U.S. economy by including Section 515 of the S. 1329 in any continuing funding legislation that is considered by Congress.

Sincerely,

American Council of Engineering Companies (ACEC)
BSA | The Software Alliance
CompTIA
Financial Executives International (FEI)
Information Technology Industry Council (ITI)
IT Alliance for Public Sector (ITAPS)
Professional Services Council (PSC)
Semiconductor Industry Association (SIA)
Silicon Valley Leadership Group (SVLG)
Software & Information Industry Association (SIIA)

Technology Association of America (TechAmerica)
U.S. Chamber of Commerce
U.S. Council for International Business (USCIB)
U.S. Information Technology Office (USITO)

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
Ambassador Michael Froman, United States Trade Representative
Dan M. Tangherlini, Administrator, General Services Administration
Joe Jordan, Administrator, Office of Federal Procurement Policy
Steven Van Roekel, Federal Chief Information Officer
J. Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, Executive Office of the President
Alex Niejelow, Chief of Staff, U.S. Intellectual Property Enforcement Coordinator