Information Technology Industry Council
Innovation. Insight. Influence.

Question received from the Honorable Anna Eshoo, U.S. House of Representatives:

> *The GAO's report explores the concept of expanding the U.S. government's Committee on Foreign Investment in the United States (CFIUS) review process to include network provider purchases of foreign-manufactured equipment. The report notes a series of concerns that could result such as trade barriers, additional costs, and constraints on competition. Do you believe the benefits outweigh the drawbacks of expanding the CFIUS review process?*

Answer: No. ITI believes expanding CFIUS in this regard has numerous drawbacks that might outweigh any benefits. We concur with the findings in the May 2013 GAO report[1] that such an approach could result in trade barriers, additional costs, and constraints on competition. Such an approach also could negatively impact the security of U.S. communications networks.

Expanding CFIUS as proposed will decrease, not increase, security. The proposal is based on an incorrect premise that security is a function of where network equipment is manufactured and that equipment manufactured in a foreign country is inherently less secure. Product security is a function of how a product is designed, engineered, and maintained, not where it is manufactured. If forced to manufacture in a given country, companies lose significant flexibility to innovate in response to actual and emerging threats. A focus on where technology is developed, rather than how, fails to evaluate the actual security of the product and can lull buyers into a false sense of security. The global ICT industry encourages all governments to refrain from enacting policies that discriminate based on technologies' country of origin.[2]

Secondly, this proposal would impact nearly every information and communications technology vendor, including U.S.-headquartered ones, since nearly all network equipment is manufactured in foreign countries. By researching, developing, and manufacturing globally, companies gain global talent, resiliency/redundancy of suppliers, high-quality low-cost inputs, and manufacturing efficiencies. This leads to the affordable, leading-edge technology products, with the high level of security demanded by businesses, governments, and consumers. Thus, harms we foresee, enumerated below, will fall on U.S. and foreign companies alike.

Expanding CFIUS as proposed would harm our companies' competitiveness and trade. Other countries, interpreting our actions as an attempt to create barriers to foreign entry into U.S. markets, will emulate such proposals and pursue their own domestic requirements. A "race to the bottom" of such requirements would ensue, leading to a patchwork of conflicting

[1] GAO, "Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment," May 21, 2013.

[2] "Global ICT Industry Statement: Recommended Government Approaches to Cybersecurity," DIGITALEUROPE, ITI, and JEITA, June 2012, p. 2. ***Reconfirm title and insert footnote***

requirements from various governments, balkanizing the global ICT marketplace. This would significantly diminish the benefits—fast-paced innovation (new products with new and useful features), global interoperability, low cost, and constantly improved product security—that derive from our massive research and development (R&D) investments which we can only afford if we can serve a global marketplace. Being able to innovate in this regard is essential to our companies' survival. In fact, a recent Brookings report noted that government policies enacted in the name of "cybersecurity" could, if they are country-specific, impede the global flow of information technology products and services, harming information technology firms and vendors as well as importing countries.[3]

Unfortunately, we are already seeing other countries going down the path proposed. The most egregious cases include India and China. India's 2012 Preferential Market Access policy aims to impose domestic manufacturing requirements on telecommunications equipment sold in the commercial market. While China has long sought to keep foreign ICT products out of its market, recent China-focused policies coming out of Washington have increased motivation behind these exclusionary policies. Changing CFIUS as contemplated will be seen as a retaliatory measure towards Chinese companies, spurring China to move forward on its plans to set up a CFIUS-like Review Commission.

In addition to India and China, Indonesia, Nigeria, and other countries have domestic technology procurement requirements on the books. U.S. industry is working with the Administration to push back on these restrictions and our successes depend in part on being able to state that such approaches deviate from global norms. If the U.S. government begins to review commercial communications transactions, we will lose much of our bargaining power, which could result in foreign markets increasingly shut to our companies.

Expanding CFIUS to commercial transactions also would be extremely costly and unwieldy. As described by GAO (pp. 9-10), communications networks in the United States are highly complex. Multiple network providers operate distinct regional and other smaller networks, including wireless, wireline, and cable access segments, which interconnect to a national backbone to form a national infrastructure. The entire network relies on hundreds if not thousands of types of products. Further, as GAO also highlights (p. 37), network providers conduct thousands of transactions a year. These purchases may serve to update one portion of a regional network, or be part of a phased-in national upgrade. It would be very time-consuming for both providers and vendors to file a CFIUS report on each of these transactions, a likely scenario given that each transaction would include foreign-manufactured equipment. In addition, detailing the country in

[3] Friedman, Allan, "Cybersecurity and Trade: National Policies, Global and Local Consequences," Brookings Institution Center for Technology Innovation, September 2013.

http://www.brookings.edu/~/media/research/files/papers/2013/09/19%20cybersecurity%20and%20trade%20global%20local%20friedman/brookingscybersecuritynew.pdf

which certain equipment is manufactured could be impossible from the vendor perspective. As described above, vendors have global supply chains. Further, vendors constantly change their sources of supply, based factors such as price. This would hamper any ability to cite prior filings related to the same type of equipment.

Mandating a review of each commercial transaction also would overwhelm the CFIUS process, which was not designed for that type of capacity. The number of CFIUS cases now averages from 100-200 per year.[4] Changing the CFIUS scope would result in a substantial—not marginal—increase in workload. This in turn is likely to lengthen the average review time, which at a minimum 30-75 days[5] already is quite long. Such a delay would raise costs for network providers, equipment vendors, and, ultimately, U.S. consumers (also pointed out by GAO, p. 36). It also would delay the roll-out of 4G LTE and other leading-edge networks in the United States, hampering the efficiency and productivity all U.S. businesses and consumers, and the U.S. government, enjoy from our communications networks. And these benefits translate into a significant impact on U.S. competitiveness and growth. Last year, Ericsson, Arthur D. Little, and Chalmers University of Technology, concluded that for every 10 percentage point increase in broadband penetration GDP increases by 1 percent.

In 2012, GAO released a separate report in which federal officials from the Director of National Intelligence (DNI), NSA, and the CIA provided reasons why the cost of tracking IT equipment's country of origin outweighed the potential benefits.[6] That report was focused on government procurement, but if these agencies feel that country-of-origin tracking was not a benefit for their own procurements, it is doubtful tracking for commercial telecommunications network purchases would be any more useful.

Both my May 2013 testimony (pp. 3-5) and the May 2013 GAO report (pp. 15-27) list a range of steps industry, network providers and equipment vendors, and the government are taking to address cyber-related risks in U.S. communications networks. U.S. government efforts should focus on:

- Creating incentives for the effective implementation of the President's February 12 cybersecurity Executive Order to continue. The Executive Order directs the General Services Administration and the Department of Defense to study the merits of incorporating global, industry-led cybersecurity standards into federal acquisition planning and contract administration. The ICT industry is deeply committed to improving

[4] ***(need footnote from Treasury website)***

[5] CFIUS includes a mandatory 30-day review, and CFIUS may institute a subsequent 45-day investigation (which can be extended). In addition, parties need time to get a filing complete before submitting it.

[6] GAO, IT Supply Chain: National Security-Related Agencies Need to Better Address Risks," March 2012, p. 27.

cybersecurity and, as such, we are deeply involved in this work and want to make it a success.

- Ensuring private sector participation in the supply-chain work within the Executive branch. As with any cybersecurity issue, public-private partnerships are critical. Currently

  there are various supply-chain efforts within the Administration. Although it has been challenging at times for the private sector to have input into that work, now both the IT Sector Coordinating Council and Communications Sector Coordinating Council have active supply-chain committees that are working closely with DHS and other government agencies to jointly review this work.

- Sourcing technology from authorized sellers and resellers. Federal purchasers and their contractors should procure ICT equipment directly from original equipment manufacturers (OEMs) or their authorized resellers and service partners, except when the item is discontinued or otherwise unavailable. This can help to minimize the chances that counterfeit or tainted products will be unintentionally acquired, mitigating a significant risk to government supply chain. Too often, we have seen government agencies procure technology products from companies that had no relationship with the products manufacturers, and had themselves bought the products from unverified sellers.

- Passing effective cyber threat information-sharing legislation.

These approaches are commendable and should be encouraged. Expanding CFIUS as proposed would hamper, not help, these activities and would negatively impact security, trade, innovation, and competitiveness as described above.