7035 Ridge Road
Hanover, Maryland 21076-1426

410 694 4500 phone
410 865 8001 fax

www.ciena.com

January 17, 2014

The Honorable Anna Eshoo
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Question:

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:

As part of our public policy advocacy efforts over the past several years, Ciena Corporation has given significant consideration to the role that CFIUS could play in network provider purchases of foreign-manufactured equipment. In our view, if the proposed expansion of the CFIUS review process were appropriately defined and tailored to adequately address the concerns set forth below and in the GAO report, then we believe that the benefits could potentially outweigh the drawbacks. If that were not the case, however, then we believe that the drawbacks would outweigh the benefits of expanding the CFIUS review process.

In order to make an effective assessment of any CFIUS expansion, Ciena believes that policymakers must consider the following:

1. Network providers have varying level of sophistication when it comes to testing and evaluating communications networking equipment. In our experience, some providers – typically the largest carriers and U.S. government agencies – have a deep understanding of and appreciation for the security benefits that are derived from our efforts to move our supply chain out of China. However, there are many private sector enterprise buyers of networking equipment that simply do not have the same level of sophistication or understanding of the security risks posed by equipment in their networks, or the same infrastructure resources with which to test and evaluate such equipment. Because some of these enterprises run enormous global networks, they may be unintentionally creating significant risks to their companies, customers and employees. In many cases, however, their networks are just as critical to our nation's well-being. At the same time, the scope of and breadth of network equipment today is quite significant. Not all network equipment functions in the same manner, operates in the same place in a network, or poses the same risks to security of the network. Accordingly, from a policy perspective, in order that the review net is

appropriately tailored to the relative risk posed by the transaction, there should be meaningful consideration given to the definitions of both "network provider" and "purchases" for purposes of triggering potential CFIUS review.

2. Under the current structure of the telecommunications industry supply chain, the vast majority of communications networking equipment – including equipment marketed and sold by Ciena – incorporates at least some components or subcomponents that are manufactured in a foreign country. As a result, broad policy proscriptions relating to "foreign-manufactured equipment" could theoretically impact every equipment purchase by network providers, which is not, in our view, the right policy approach. Instead, we believe that a more appropriate and practical approach would be to expand the CFIUS review to purchases of foreign-manufactured networking equipment from a subset of companies that may have interests adverse to those of the United States, both from a national security and a trade and economic perspective.

3. In light of the rapid transition of the communications industry to "software-defined networking" and "network function virtualization," the importance of software to current and future networks cannot be understated and is absolutely critical from a product integrity and product assurance perspective. By way of example, we have implemented strict controls over our software development, and the final testing and validation all of the software loaded onto our products is performed in North America. In so doing, we reduce the risk that the software can be tampered with or modified and thereby create network security concerns for our customers. Therefore, to the extent that any review process is created for network provider purchases of equipment, it must necessarily consider the integrity of the embedded software and any application software, where it installed, by whom, as well as who will conduct ongoing and routine maintenance and support of the software.

As a result of the above, Ciena continues to believe that the most important next step is a broad-based education program for enterprise purchasers of network equipment, particularly those enterprises with critical infrastructure. It would certainly be in the economic and security interest of the United States to find a way to routinely share information such entities so that they make more informed buying decisions.

Sincerely,

On behalf of Ciena Corporation

David M. Rothenstein
Senior Vice President and General Counsel