Mr. John Lindquist
President and CEO
Electronic Warfare Associates
13873 Park Center Road, Suite 200
Herndon, VA 20171

The Honorable Anna Eshoo

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 equipmet. 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?

Expanding the Committee on Foreign Investment in the United States (CFIUS) review process to include network provider purchases of foreign-manufactured systems will be significantly burdensome on all concerned because there are no manufacturers of telecommunications equipment in the United States. Furthermore, the bulk of the components (board level and below as well as software and firmware) integrated into telecommunication systems are also manufactured outside the United States. More to the point, all manufacturers of telecommunications equipment, including software and firmware, have significant developmental and production facilities in the Peoples Republic of China as well as other nations that, from time to time, might find it in their interest to subvert or disrupt U.S. networks. In light of the global nature of the network providers supply chain, CFIUS would be in a position of evaluating the entire supply chain on a continuous basis. That becomes extremely difficult because the pedigree of the components and software routines used in the systems are often extremely difficult, if not impossible to determine which in turn makes it very difficult to assess the risk associated with the components and, therefore the risk to the system.

The CFIUS review process is designed to determine who can be trusted. The nature of the supply chain makes it nearly impossible to know who was involved in the development and manufacture of a network system or its components. If one can't know who is involved, one can't know who to trust.

A more productive, and less disruptive approach, would be to develop an independent review process, similar to the process put forth in a recent CFIUS mitigation agreement. The agreement requires a detailed analysis of hardware, firmware, and software so as to provide an acceptable level of assurance that the system is free of components and subcomponents designed or corrupted to enable malicious exploitation. In addition, the agreement requires a trusted delivery process that ensures that the system delivered is exactly the same as the

system evaluated. The result is that the network provider, and in turn the U.S. government, can decide whether or not to trust the system based empirical evidence rather than on the country in which the manufacturer has located its headquarters. Since all components have a great likelihood of manufacture outside the U.S. by non-U.S companies, it might serve the Committee's goals more effectively, to review the High Assurance Analysis and Trusted Delivery Processes as well as the Independent Evaluator implementing those processes. This approach would limit the complexity of the CIFIUS Review Process, and avoid many of the feared trade economic and political drawbacks, and dramatically increase the security posture of the network system.