Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Phone: 408 526-4000
Fax: 408 526-4100
http://www.cisco.com

May 15, 2014
President Barack Obama
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Mr. President:

This week a number of media outlets reported allegations that the National Security Agency has intercepted IT equipment while they were in transit from manufacturers to customers. While the reports included a photograph purportedly showing a Cisco product being modified, this issue affects an entire industry that depends on a global supply chain and global shipments. We ship our products from locations inside, as well as outside the United States, and if these allegations are true, these actions will undermine confidence in our industry and in the ability of technology companies to deliver products globally.

Confidence in the open, global Internet has brought enormous economic benefits to the United States and to billions of people around the world. This confidence is eroded by revelations of governments' surveillance, government demands that make it difficult for companies to meet the privacy expectations of citizens and laws of other countries, and allegations that governments exploit rather than report security vulnerabilities.

We simply cannot operate this way, our customers trust us to be able to deliver to their doorsteps products that meet the highest standards of integrity and security. That is why we need standards of conduct, or a new set of 'rules of the road,' to ensure that appropriate safeguards and limits exist that serve national security objectives, while at the same time meet the needs of global commerce. We understand the real and significant threats that exist in this world, but we must also respect the industry's relationship of trust with our customers.

Absent a new approach where industry plays a role, but in which you, Mr. President, can lead, we are concerned that our country's global technological leadership will be impaired. Moreover, the result could be a fragmented Internet, where the promise of the next Internet is never fully realized.

Mr. President, we appreciate the steps you took earlier this year on this important topic. We are asking your Administration to take more steps and a leadership role to ensure that guidelines and reforms are put into place that can be honored across the globe.

As a matter of policy and practice since our inception, Cisco does not work with any government, including the United States Government, to weaken our products. And when we learn of a security vulnerability, we respond by validating it, informing our customers, and fixing it as soon as possible. By adhering to these – and many other standards – we have built and maintained our customers' trust. Trust with our customers is paramount, and we do everything we can to earn that trust every day.

Please let me know if you have any questions. Our industry is ready to work with you and other governments around the world. We are not focused on how we got here, but rather what we will do to move forward. We are committed to playing any role that will contribute to the right outcome.

Sincerely,

John T. Chambers
Chairman and Chief Executive Officer
Cisco Systems

NSA slide below released 13 May 2014 by Glenn Greenwald for his book *No Place to Hide* showing Cisco shipping box being opened, probably the CIA-NSA Special Collection Service.

http://en.wikipedia.org/wiki/Special_Collection_Service

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon