November 9, 2010

Mr. Mark Chandler
Senior Vice President, General Counsel and Secretary
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Dear Mr. Chandler:

We greatly appreciate your continuing positive efforts to work with us to identify and hopefully deal more effectively with many of the issues and concerns that we as shareholders have presented to you in connection with how Cisco Systems handles marketing, sales and export activities involving Chinese law enforcement agencies and operations.

Your letter of October 29, 2010 provided us with some of the additional information and material that we discussed with you and other senior Cisco officials in person on September 3, 2010. In that letter you indicated that you welcomed our input and information, and suggested that we provide to you any additional material and views that we might have along these lines. This communication is aimed at meeting this request, and serving as a basis for scheduling a third meeting with your senior management team immediately after the shareholders' annual meeting on November 18, although at our September 3rd meeting Ms. Graves suggested we meet in October. May we suggest the week of December 6 through 10 as the best time for this meeting, since that will give sufficient time to complete the annual meeting activities, and also would not conflict with the upcoming holiday season.

First, and most important, we would like to identify again some of the key concerns and points that we have covered in our prior communications with you that are most in need of additional exploration and discussion. Many of these points relate to your assurances in paragraphs three indicating your commitment to maximum and effective oversight and analysis of the potential human rights impacts of company policies and actions, and the assurances in paragraph two, bullet two of your letter that "Cisco sales are strictly in accordance with United States export control rules," as "informed by human rights concerns," limiting certain types of sales to China. We certainly share your concerns on this point, and while we believe, as you very forcefully and persuasively indicated at our meeting on September 3, and in your letter of October 29, that Cisco regularly reviews and makes assessments of human rights concerns at both the senior management and board of directors levels, without your providing us with any further details about how this process works, it appears to be an ad hoc system that may well not

meet the ongoing institutional assessment capability on these matters that the Department of Commerce Bureau of Industry and Security recommends in its Compliance Manual. We would welcome your providing us, and perhaps explaining to us in person at our next meeting, the details of how your assessment process works, and exploring with us how it might be made a more systemic means for assessing the potential negative impacts of proposed and actual Cisco policies and actions involving China and other highly repressive regimes. I am sure you agree with us and with the Department of Commerce that the methods used for making these assessments need to be institutionalized as an ongoing system, and we would be pleased to help you think through what may be required to make this human rights assessment capability a more permanent and regular part of Cisco's planning processes. If this type of regularized system had been in place, the highly controversial marketing and sale of Cisco's router equipment to Chinese law enforcement agencies in 2002 and 2003 as an integral part of Chinese law enforcement authorities' development of the Golden Shield Internet monitoring system, as testified to at the 2008 Senator Durbin Senate Judiciary Committee hearings, would not have occurred.

Second, the point you have made in paragraph two, bullet one of your October 29 letter regarding the "neutral" and standardized nature of Cisco's products needs considerably more discussion and exploration. As you correctly point out, the type and capabilities of much of the equipment and technology that Cisco sells and exports "by its very nature allows for the filtering of sites" on the Internet, and the monitoring and tracking of Internet communications. It is exactly that innate and inherent capability that concerns us, because by definition it provides Chinese security officials and agencies with the ability to monitor and track electronic communications, and to identify Internet users whose communications might be considered "undesirable" by Chinese law enforcement authorities. Indeed, this is exactly what has happened with the Golden Shield program and other more recent systems used by Chinese authorities to monitor and control the electronic communications of Internet users, and to punish those "misusing" their free speech and free association rights for purposes the government of China does not approve. If, as you suggest, Cisco's products enabled or facilitated these results because of their inherent tracking capabilities, questions do need to be explored as to why these products and technologies were marketed, sold and exported to China, since doing so did violate the Export Act prohibition against sending equipment to China that could be used, and in fact was used, for law enforcement purposes. Our main concern and goal is to work with you to assure that this highly negative and unlawful result does not occur again, especially given the inherent monitoring capability that Cisco's products provide as you very correctly acknowledge.

Third, closely related to the second point, is the issue related to your statement in paragraph two, bullet one of your October 29 letter that Cisco does not "customize" its products in any way that would

"facilitate censorship" or other human rights abuses, and your statement in the first sentence of paragraph two, that Cisco's policy of providing "standard" Internet equipment and of "opposing efforts of governments to 'balkanize'" or regulate electronic communications, provide the best means for preventing Internet related human rights abuses and assuring "freedom of expression" on the Internet. Further joint discussion and analysis are needed on whether resistance and opposition to "balkanization" and regulation of electronic communications can be effectively maintained and carried out, and the goal of freedom of expression secured. Given the inherent monitoring capabilities of Cisco's equipment, and the unfortunate reality that many security and law enforcement customers in highly repressive countries like China fully and openly intend to make use of Cisco's products for censorship and monitoring purposes, we need more careful attention and analysis of the potential impacts of projected sales and exports. The fact that Cisco may not want or intend to have its products used in these negative ways does not prevent that unwanted result from taking place without further action of some type being taken. That is one of the major points made in the Bureau of Industry and Security's Compliance Manual, that requires a more organized and systematic set of procedures to be in place to assess end use and end user impacts before sales and exports take place.

Fourth, we respectfully disagree with and are deeply concerned of your statements in paragraph five. The fact is that, besides the American public, the Chinese people also hold a very negative image of Cisco's business in China. Since I attended Cisco's shareholders meting in 2008, some Chinese people have urged me to take firm actions, some have expressed an appreciation when they heard the progress at our September 3rd meeting. You can find one such report of Radio Free Asia at http://www.rfa.org/mandarin/yataibaodao/si-09102010110801.html. There is also a typical strong condemnation of Cisco from China in this report. "我是一名刚刚毕业的中国大学生，是计算机网络专业的。 对我来说，我深刻感到中国的网络封锁越发到了发指的地步。我利用了复杂的技术手段得以来到这民主之地，但同时还有千千万万的同胞处于网络恐怖之下。无数网络警察，网络秘密调查员遍布中国各地，利用他们购买的CISCO和其他公司的设备，监控网民的合法行为。我抗议思科公司提供给中国政府价值数百亿美元的网络设备，用于封锁中国数亿同胞的基本人权与言论自由，这些设备被用于制造迫害。思科公司对此负有不可推卸的责任。" (I am a new graduate in China of Computer Network major. I deeply feel that China's Internet blockade is beyond description. I used a complex of technical means to come to this land of democracy, but at the same time there are millions of people under the terror of network. Numerous network police and secret investigators all over China are using Cisco and other companies ' equipments to monitor legal actions of Internet users. I protest against Cisco providing the Chinese Government network devices of billions dollar used for the blockade of fundamental human rights and

freedom of expression of hundreds of millions of people in China. These devices are used for creating persecution. Cisco has an inescapable responsibility.) You can see that the situation of Cisco's PR in China is much more serious than you understand or believe, and we are here to help the company understand the business consequences of its actions in both China and the U.S.

Finally, with respect to the listing of other companies involved in Internet and electronic communications in China that you have compiled and have very kindly provided to us, we would welcome further discussions with you about how the activities of these companies relate to the concerns we have been expressing. We have expressed our determination to help any company in this regard at our September 3rd meeting. Among the companies in the listing, I have submitted proposals to HP and Intel for next year's shareholders meeting. I also have Brocade's shares, but Huawei is a private company and ZTE is traded in Hong Kong not in the U.S. stock market. We are carefully monitoring these companies (and IBM and Juniper in the future).

As we have discussed, as shareholders with the unique background and direct experience that we have had with China's repressive policies, we believe that we can assist you in analyzing and brainstorming further about these issues in a positive and constructive way designed to help you formulate and implement the best and most effective policies and institutional mechanisms to achieve the goals you have articulated of opposing and preventing "a less open Internet," and promoting a system of electronic communications that is free and not subject to restrictions and control. We look forward to hearing from you about scheduling the next meeting and discussions with you that we propose to take place the week of December 6 through 10, as we have noted above.

Sincerely,

Jing Zhao

cc: Ms. Laura Graves, Morton Sklar, Esq.