

**Questions for the Record for Mark Chandler, Cisco Systems, Inc.  
Senate Judiciary Committee  
Subcommittee on Human Rights and the Law**

**Senator Durbin Questions**

**1. You testified, “We support restrictions on the ability of companies to locate within an internet-restricting country electronic communications that include personally-identifiable information.” Does Cisco support H.R. 275, the Global Online Freedom Act of 2007? Please explain.**

*A1. Cisco believes that the U.S. government has an important role to play in protecting and promoting freedom of electronic information abroad. To focus these efforts, Cisco supports establishing an Office of Global Internet Freedom at the U.S. Department of State and appointing a U.S. Ambassador at Large for Internet Freedom. We understand that many companies that provide direct internet services to consumers, which Cisco does not, are voluntarily taking the step described in the question.*

**2. You testified that “employees would customize [Cisco’s] products in such a way as to undermine human rights would not be consistent with the code of conduct that we have.”**

**a. How would such customization be inconsistent with Cisco’s code of conduct?**

*A2a. Such customization would be inconsistent with Cisco’s core principles, embodied in our basic human rights guidelines adopted in Cisco’s Corporate Citizenship Report which guide the conduct of our employees. As stated in our Corporate Citizenship Report 2007, Cisco “support[s] the United Nations Universal Declaration of Human Rights” and, as outlined in our Code of Business Conduct and employee policies, we expect all our employees to “treat others equally and with respect and dignity.”*

*Cisco has adopted the following two principles from the UN Global Compact, as stated in the Report:*

*“Principle 1: Businesses should support and respect the protection of internationally proclaimed human rights; and*

*Principle 2: Businesses should make sure that they are not complicit in human rights abuses.”*

*The Report further makes clear that with regard to our products and the indirect customers of our products:*

- Cisco does not customize, or develop specialized or unique filtering capabilities, in order to enable different political regimes to block access to information.*

- *With respect to operating functionality, Cisco sells the same equipment in China as it sells worldwide.*
- *Cisco is not a service or content provider or network manager.*
- *Cisco has no access to information about individual users of the Internet.*

**b. Please provide a copy of this code of conduct and any other Cisco human rights guidelines or policies**

*A2b. See attachments.*

**3. At the hearing I asked you, “Does your company inform government clients, in writing or otherwise, that they will not assist in efforts toward censorship or repression?” You responded “our products do not do that.” You also testified, “Cisco does not customize, or develop specialized or unique filtering capabilities, in order to enable different regimes to block access to information...The tools built into our products that enable site filtering are the same the world over, whether sold to governments, companies or network operators. The features in our equipment are ‘off the shelf’ and not altered in any way for any market or region.”**

**a. Do you agree that Cisco’s off-the-shelf products, which you testified “enable site filtering,” can be used to enable different regimes to block access to information, even if they are not customized?**

*A3a. As I mentioned in my written testimony, the Internet can be and is disrupted by cyber attacks despite its redundant nature. Every major corporate and service provider network has experienced this. Attached to this letter is an article from the November 10 New York Times regarding the growing sophistication of attacks on public and private networks around the world.*

*Network management and security capabilities are essential to mitigate attacks and thus enable information flow. No network can be administered by our customers without the ability to manage and protect the information that flows through it. Without this capability, it would not be possible to operate the Internet, and the Internet would not exist as it does today.*

*Moreover, the technology that is used to manage and protect against hackers or viruses is the same generic technology used to filter or control Internet access by children, such as the parental control software that network operators are being urged to provide to all customers, or the illegal downloading of copyrighted material.*

*Network management software is a basic feature of Internet equipment -- Cisco’s and our competitors’ -- and fundamental to network functionality. Whether for security or the management of information, the technology is one and the same.*

**b. Do you stand by your testimony that “our products do not” assist in efforts toward censorship or repression in any circumstances?**

*A3b. Our products are designed to expand the reach of the Internet and to ensure the stability, safety and availability of communications networks; without these network management and security capabilities, the Internet could not function. Our products are not designed for censorship or repression.*

- c. Let me ask you again, does Cisco inform its government clients, in writing or otherwise, that they will not assist in efforts toward censorship or repression?**

*A3c. As I note in my answer to 2a above, our Corporate Citizenship Report, which is publicly available, states our corporate policy on human rights. It specifically notes that our company does not develop specialized technology to enable regimes to block access to information, nor do we have access to individual user information of private internet users.*

- d. If not, will you consider adopting such a policy?**

*A3d: See answers to Questions 3(a) and 3(c) above.*

**Q4. You testified that the 2002 Cisco PowerPoint “Overview of the Public Security Sector” discussed at the hearing was the work of a low-level employee.**

- a. Did the reference in the PowerPoint to the Falun Gong as “evil” violate Cisco’s code of conduct or any other Cisco policies?**

*A4a. The statement in question does not reflect Cisco’s principles, policies or its sales and marketing strategy or approach. It is a quotation from a speech made by a Chinese government official in 2001. Reprinting a statement by a government official, even if the underlying sentiment is inconsistent with Cisco’s policies, does not by itself violate those policies.*

- b. If the response to question 4(a) is no, will Cisco change its policies and procedures to make clear that such a reference is unacceptable.**

*A4b. See answer to Question 4(a), above.*

- c. If the response to question 4(a) is yes, was the employee who authored the PowerPoint disciplined?**

*A4c. See answer to Question 4(a), above.*

- d. According to Cisco’s English translation, the PowerPoint described as one purpose of the Golden Shield project “Combat ‘Falun Gong’ evil religion and other hostiles.” Is it therefore accurate to conclude that Cisco knew in**

**2002 that one purpose of the Golden Shield was to combat Falun Gong and other religious or political dissidents?**

*A4d. The Chinese government's antipathy to Falun Gong has been long well-known. We regret that this quotation from a Chinese government official was reproduced in this 91-page presentation. The Golden Shield project, as we understand it, related generally to improved internal communication within the public safety departments. With respect to Cisco, Cisco sells the same off-the-shelf products in China as it does world-wide, consistent with U.S. law.*

**e. Has Cisco conducted an internal review to determine whether any documents similar to the 2002 PowerPoint exist?**

*A4e. No such review would be feasible or productive, given Cisco's size – 65,000 employees, operating in approximately 100 countries – and the fact that Cisco sells off-the-shelf products which are not customized. In no case does Cisco design products for repression or censorship. If contrary activity were to take place, Cisco would investigate any such report and take appropriate action.*

**f. If the response to question 4(e) is yes, please provide the results of this review, including any documents you discovered.**

*A4f. Not applicable.*

**g. If the response to question 4(e) is no, will Cisco conduct such a review and provide me with the results?**

*A4g. Literally tens or hundreds of thousands of documents globally describe the application of Cisco products to network implementation and modernization projects in the U.S. and around the world. We do not believe that such a massive review is feasible or productive, given that we sell standard equipment around the world which is not customized to enable different regimes to block access to information.*

**5.**

**a. What role did Cisco play in the development of the Chinese government's Golden Shield project?**

*A5a. To the best of my knowledge, Cisco did not play any role in the development of the Chinese government's Golden Shield project.*

*Cisco's standard switching and routing products have been acquired by various Chinese departments as part of their modernization programs, which could include, among others, the Golden Shield project. As noted above, Cisco does not customize its products to enable the blocking of information.*

- b. Has Cisco ever described Golden Shield as one of its success stories?**

*A5b. Not to my knowledge.*

## **6. Marketing**

- a. Can you assure me that Cisco does not in any circumstances market its product and/or services to government authorities in China or any other country on the basis of their usefulness in detecting, monitoring or censoring political dissent or expression that are protected under Article 19 of the International Covenant on Civil and Political Rights (ICCPR)?**

*A6a. As noted earlier, in a company with 65,000 employees located in approximately 100 countries, it is impossible to be certain whether any employee has ever violated any policy of the company, and this applies in this case as well. If such activities are detected, we will take appropriate action.*

*In any event, Cisco products are not designed or customized for the purpose of censorship or monitoring political dissent.*

- b. Can you be certain that no Cisco personnel market Cisco's products and services on this basis?**

*A6b. See answer to Question 6(a) above.*

- c. Will Cisco conduct a review to ensure that no Cisco personnel have engaged in this type of marketing?**

*A6c. See answer to Question 4(g) above.*

- d. What policies and procedures does Cisco have in place to ensure that Cisco personnel do not engage in this type of marketing?**

*A6d. See answers to Questions 2(a) and 6(a) above*

- e. Is this addressed in Cisco's code of conduct?**

*A6e. See answer to Question 2(a) above.*

## **7. Services**

- a. Can you assure me that Cisco does not in any circumstances assist or advise government authorities in China or any other country in using your**

**products for detecting, monitoring or censoring political dissent or expression that are protected under Article 19 of the ICCPR?**

*A7a. Cisco is not a traditional communications service provider or a web portal; rather we sell our products to these service providers. (Cisco's Webex subsidiary does provide an on-line conferencing and collaboration service that is used for web-based business communications). Since we do not tailor our products to allow for censorship, we believe our business in China and elsewhere is conducted fully in accord with our corporate principles, noted earlier.*

*All Cisco customers globally have access to Cisco training and support. We provide service and support, either directly or, in many cases, through systems integration partners for our equipment. Cisco service and post-sales support is generally designed to replace faulty or defective products, provide training for the proper operation of network hardware and ensure that networks are stable and available 24 hours a day, including protecting our customer's networks from hackers and malware.*

**b. Can you be certain that no Cisco personnel provide such assistance or advice?**

*A7b. See answer to Question 6(a) above.*

**c. Will Cisco conduct a review to ensure that no Cisco personnel have provided such assistance or advice?**

*A7c. See answer to Question 4(g) above.*

**d. What policies and procedures do you have in place to ensure that Cisco personnel do to [sic] not provide such assistance or advice?**

*A7d. See answers to Questions 2(a) and 6(a) above.*

**e. Is this addressed in Cisco's code of conduct?**

*A7e. See answer to Question 2(a) above.*

**8. What policies and procedures does Cisco have in place to ensure that your products and services are not used by government authorities in China or any other country to detect, monitor or censor political dissent or expression that are protected under Article 19 of the ICCPR?**

*A8. As stated above, Cisco has adopted the principles of the UN Global Compact, including that businesses should ensure that they are not complicit in human rights abuses and should support and respect the protection of internationally proclaimed human rights. Our products are off-the-shelf and are not customized to enable different*

*political regimes to block access to information. Our products allow network administrators to manage and protect the information that flows through the network; without this capability, the Internet could not function.*

**9. You testified that “Cisco complies with all U.S. regulations informed by human rights concerns which control sale of our products.”**

**a. Has Cisco ever refused a business opportunity to avoid complicity in human rights violations in a case where no law prohibited pursuing the opportunity?**

*A9a. Cisco is not complicit in human rights violations.*

**b. Would Cisco support changing U.S. regulations or laws to prohibit the export to China of networking equipment that can be used for censorship and surveillance?**

*A9b. Cisco will abide by all relevant U.S. statutes and regulations.*

**10. What products has Cisco sold to the Chinese government?**

*A10. For reasons of business confidentiality, Cisco cannot publicly disclose the details of customer purchases. Cisco would be pleased to discuss this with the Committee in confidence.*

**11.**

**a. Please describe “Policenet” in detail. What products does it include?**

*A11a. Cisco does not currently have, nor has it ever had, a product or solution referred to as “Policenet.” It is our understanding that “Policenet” is a generic term used in many countries, including China, to refer to the concept of a networked police force.*

**b. What products and services does Policenet include?**

*A11b. Not applicable.*

**12. Would Cisco support an independent outside monitoring process, like the one that has been proposed for internet service providers, for companies that sell networking equipment to internet-restricting governments? Please explain.**

*A12. The business model for internet service providers and equipment vendors vary considerably, so I am not certain that what has been proposed would be appropriate. Cisco will abide by all relevant U.S. statutes and regulations.*

**13. Google’s Nicole Wong testified, “We support the development of tools that are intended to get around censorship on the Internet. We do that in a couple of ways,**

**both directly supporting developers in that area, and also providing a code base for building on top of that.”**

- a. Does Cisco support developers of anti-censorship technology? Please provide examples.**

*A13a. I am not aware that we have been approached by any anti-censorship technology developers for assistance. To the extent that technologies are innovative and broaden the reach of the Internet, we would support such technologies.*

- b. You testified about “the respect I have for the efforts that [Shiyu Zhou] undertakes to allow access to information that censors would otherwise preclude access to.” Will Cisco consider supporting the Global Internet Freedom Consortium?**

*A13b. The best way that Cisco can support the Global Internet Freedom Consortium is to continue to build our products to open, global standards and vigorously oppose attempts by some governments to balkanize the Internet by setting country-specific security requirements.*

## **Senator Coburn Questions**

**Q1. Please describe the efforts Cisco is making to ensure internet freedom to its customers around the world.**

*A1. As a global organization, Cisco has played a leading role in helping to make Internet technology ubiquitous. Doing this has enabled hundreds of millions of people in nearly every nation around the world to access information and ideas previously unavailable or inaccessible. We believe in maximum access to information and Cisco is proud of the role we have played in bringing the Internet to hundreds of millions of people around the world -- including by building open systems that facilitate efforts to overcome censorship.*

*Since entering the China market in 1994, Cisco along with other leading technology businesses have participated in helping increase the number of Chinese people who have access to the Internet -- from 80,000 users in 1995 to over 253,000,000 in 2008.*

*Cisco remains committed to continuing to expand the reach of the Internet. To that end, Cisco invests billions annually in education, training and R&D to help bolster technology infrastructure and skills-development of people in emerging markets.*

*The Internet has been the greatest force in the world today for the dissemination of and access to information.*

**Q2. Is it Cisco's belief that its products are *not* being used by certain governments to further their censorship policies?**

*A2. Our products are not designed for censorship; they are designed to expand the reach of the Internet and to ensure the stability, safety and reliability of communications networks.*

## APPENDIX

[http://www.cisco.com/web/about/ac227/about\\_cisco\\_corp\\_citi\\_human\\_rights.html](http://www.cisco.com/web/about/ac227/about_cisco_corp_citi_human_rights.html)

### Human Rights

## Introduction

Cisco strives to treat employees, and the communities in which we serve, with respect and dignity.

A supporter of the [United Nations Universal Declaration of Human Rights](#) and [Global Compact](#), Cisco's codes of conduct, employee policies and guidelines substantially incorporate laws and ethical principles including those pertaining to freedom of association, non-discrimination, privacy, collective bargaining, compulsory and child labor, immigration and wages and hours.

Consistent with Cisco's culture and applicable laws, employees are encouraged to:

- promote a safe, healthy and supportive work environment where employees can contribute their skills; and
- participate with local stakeholders in addressing community well-being, social and economic development and environmental preservation.

Employees shall respect the human rights and dignity of others as outlined in the [Code of Business Conduct](#), employee policies, and guidelines or local laws applying and abiding within the scope of their individual roles and responsibilities to whichever sets higher standards.

[Read more about Cisco's responsible management and CSR governance](#)

[Read more about Cisco's human rights policy and freedom of expression](#) [TEXT FROM THIS LINK APPEARS BELOW]

Cisco engages with stakeholders in three primary ways: industry group stakeholder engagement, third-party facilitated individual interviews or convened groups, and ongoing conversations with established stakeholders.

Through these engagements, Cisco aims to gain perspective and insight regarding our corporate citizenship performance, specifically:

- To learn more about how Cisco's current corporate citizenship is perceived and where the company could be more transparent or change current practice
- To get forward-looking information from stakeholders with particular subject-matter expertise, industry knowledge, or insight into our lines of business and specified growth areas
- To provide Cisco leadership with a chance to listen to different perspectives and

build ongoing relationships with key influencers

The feedback from recent stakeholder engagements indicates that our stakeholders believe Cisco has made progress in areas of corporate social responsibility (CSR). Stakeholders view Cisco as a leader in CSR, as evidenced by our participation in the **Electronic Industry Code of Conduct (EICC)** and the Global e-Sustainability Initiative (GeSI), for example. In addition, stakeholders view Cisco as transparent, accessible, and a strong performer, and they feel our participation in external groups is broad-ranging.

For the future, our stakeholders look to Cisco to provide more nuanced data and metrics in support of our CSR activities, as well as to anticipate trends and continue to play a leadership role in addressing emerging CSR issues.

## Identified Issues

In addition to asking for feedback on Cisco's CSR performance, we actively solicit feedback on important emerging issues. The following issues were identified as most pressing:

- Individual rights to privacy, and how Cisco's products and services fit into that debate
- Data security and the development of technology solutions to address security
- Internet censorship and freedom of expression
- Cisco's position on Internet neutrality
- Cisco's CSR and corporate governance, particularly our internal implementation of policies
- China's policies toward the Internet
- Information on the management systems in place to meet our CSR goals
- Incentives for employees (and executives in particular) to meet our CSR goals and targets
- Political contributions

Cisco's 2006 report addressed stakeholder concerns for net neutrality, human rights, and privacy. This year we will address questions related to our responsible risk management, the relationships within our value chain, and our investigation of concerns raised by stakeholders concerning human rights and freedom of expression, and accessibility of the Internet, particularly in China

## Issues Spotlight: Human Rights, Freedom of Expression, and China

We maintain a specific corporate policy on human rights and other codes and policies addressing human rights for our employees and suppliers. With regard to our product and the indirect customers of our products:

- Cisco does not customize, or develop specialized or unique filtering capabilities, in order to enable different regimes to block access to information.
- Cisco sells the same equipment in China as it sells worldwide.
- Cisco is not a service or content provider or network manager.
- Cisco has no access to information about individual users of the Internet.