



Cisco on Competitiveness and Innovation

It is becoming very clear that the United States can no longer take for granted our place as the global economic, technology, and innovation leader. There is much that government and industry can do to address this challenge, but we cannot be complacent in our response. We must recognize the challenge and take it head-on if we hope to be successful.

We need to focus on three areas to ensure global competitiveness and continued innovation.

1. Education - Education is the foundation of all innovation and the engine to economic growth. We must advocate policies that will create an educated workforce that is globally competitive to match America's future employment needs, specifically an educated workforce trained in math and science. In order for America's high tech industry to stay competitive, we need to invest in our workforce of tomorrow by giving them the tools necessary to compete for post-secondary education programs or careers in science, math or engineering. A domestic workforce educated in science, math or engineering will ensure that the American high tech industry continues to lead the world in terms of innovation and entrepreneurship. Moreover, an educated workforce will enable Cisco and other job producing companies to meet human resource needs. Further, in order to stimulate high-tech research and give companies certainty of investment, the R&D tax credit should be updated and expanded to maximize its impact in incentivizing companies to conduct R&D in the United States. Additionally, funding should be increased for basic R&D at government, university and private labs.

2. Appropriate Physical Infrastructure - The Internet, as we know it, was developed with government funds under the direction of the U.S. Advanced Research Projects Agency and, in 1969, became a reality with the interconnection of four university computers. The internet has now become the basis for efficiencies and productivity never thought possible. The deployment of broadband infrastructure is a key measure of success for a country and is crucial to the future growth of the innovation economy. We applaud President Bush's stated goal of having universal broadband connectivity in the United States by 2007 and we are looking forward to the FCC's leadership to making this goal a reality. Cisco believes that deployment of next generation broadband infrastructure should take priority over most competing interests when deciding regulatory policy. In Cisco's opinion, any national broadband plan should include policies to: 1) Incent private sector investment in broadband infrastructure; 2) Promote market-driven deployment of new technologies and applications; 3) Encourage innovation and entrepreneurship through clear, concise, minimally intrusive rules that create as much market certainty as is possible; and 4) Make spectrum available for wireless broadband services, including for first responders and ensure that communications technologies are interoperable.

3. Appropriate Legal and Regulatory Framework:

Patents - Patents ensure that inventors have the incentive to invest in further innovation, while at the same time promoting public access to new inventions. The threat of patent litigation, however, is becoming a drag on innovation while the current patent system is creating incentives for frivolous litigation. Legislation is necessary to reduce the disruptions caused by litigation and improve the quality of patents.

Intellectual Property - At Cisco, we believe our most important assets walk out the door every night. However, as we produce and own intellectual property and understand the vital importance of intellectual property to business development, strong intellectual property protection is necessary. The most effective role of government is to ensure adherence to existing laws and enforce penalties against transgressors.

Security - We all recognize how important security is to our economy, national security, and national competitiveness. Information security systems are moving from passive to active, and from point products to self defending networks using an adaptive, and interconnected, architecture-based approach. As the nature of security continues to change, public policy has to continue recognize the centrality of innovation, and continue to avoid technology mandates or regulation, which at the end of the day will always trail innovation, and make us less, not more, secure.