

**Testimony of Stephen R. Du Mont
Vice-President, Global Public Sector Practice
Internet Business Solutions Group
Cisco Systems, Inc.**

**Hearing Before the
House Committee on Government Reform**

**“Beneficial or Critical: The Heightened Need for Telework Opportunities
in the Post – 9/11 World”**

July 8, 2004



Chairman Davis, Ranking Member Waxman, and other Distinguished Members: Thank you for the opportunity to testify today regarding the value of telecommuting and the important role it plays in helping our employees perform their jobs with a high level of efficiency, security, and customer satisfaction.

My name is Stephen Du Mont, and I am Vice-President and Managing Director of Cisco's Global Public Sector Internet Business Solutions Group (IBSG). This role provides me with the opportunity to collaborate with a global team of in-depth experts, to share best practices with government entities around the world and to assist these entities in developing technology related public policies and implement plans aimed at creating maximum public value. The common thread in my career has been developing strategies, facilitated by networking technology, which enable organizations to become more responsive at lower cost. This allows for continuous and accelerated improvement in productivity and can result in higher levels of customer and citizen satisfaction. Two years ago, our IBSG Team defined these strategies and identified successful usage models in a book entitled, "The Network Virtual Organization (NVO)".

During the past year, our Team has been collaborating with a number of global government leaders to explore the question: What will the next wave of e-Government look like? It is our conclusion that the comprehensive application of NVO strategies will form the basis for this next wave and we have just completed a book entitled, "The Connected Republic". There are a number of examples cited which demonstrate how leading governments are indeed starting to achieve greater mission accomplishment with less expenditure of taxpayer proceeds, by deploying robust broadband networks. These networks facilitate the redefinition of government processes to deliver superior service to citizens at lower cost, as well as, enabling progress in the area of e-Democracy.

Cisco's telecommuting policies and procedures not only reduce our overall cost of operations, but also afford us uninterrupted access to mission critical corporate data and resources in the event of a natural disaster, homeland security threat, or other

continuity of operations interruption. Our widespread acceptance and encouragement of telecommuting, or teleworking, for all eligible employees is not only integral to our overall business continuance plan, but also supports the President's goal of national broadband availability by 2007. Not only does teleworking help achieve the goal; it becomes a benefit of the goal.

Today, over ninety percent (90%) of all Cisco employees worldwide utilize residential broadband services and telework a portion of their time. In 2003, the financial impact of this capability was \$187 million dollars in increased employee productivity for the organization. That figure, coupled with the financial impact of Cisco's other employee and customer-facing network applications and services, resulted in over \$2.1 billion dollars to the organization last fiscal year alone or approximately ten percent (10%) of Cisco's annual revenues.

Today I will focus my comments on productivity gains through strategic technology deployment, specifically as it relates to teleworking, and its natural evolution as a key enabler of any continuity of operations plan.

Teleworking: A Practitioner's Approach

In 1992, Cisco's rapid growth was exerting pressures on both Recruiting and Facilities to accommodate staff expansions, and the expansions were expected to continue for several years. Our new product development initiatives required the hiring of many new engineers, and the local labor market in the Bay Area could not fulfill all of the company's needs. While many qualified engineers were available in other regions, these workers were not always willing to relocate. Consequently, a number of key engineers in remote cities were hired under teleworking arrangements, whereby they made major contributions while maintaining their current residences. At the same time, there were some key engineers who wanted to move to other locations. By offering them teleworking arrangements, we were able to retain their services at their new desired location. As a side benefit at the time, we realized major savings on relocation

expenses, office expenses, and improved the quality of life for many of its key intellectual capital contributors.

So in 1993, Cisco became one of the first companies in Silicon Valley to develop Telecommuting Guidelines for both managers and employees, as well as a Telecommuting Agreement to standardize policies and procedures for teleworkers. Today, over 20,000 our employees worldwide have high speed remote access for teleworking, and over 90% have some form of remote access and telework a portion of their time. Why is high speed remote access important to teleworkers, and what benefits does it deliver to the enterprise and the employee?

Extending Corporate Applications

Early Cisco telework initiatives offered employees traditional remote access to data applications, primarily using our Virtual Private Network (VPN) client solution. To those who only needed email and basic web applications, this proved to be a viable solution. However, many employees demanded access to the same applications in their home office as they had access to from their campus office. Applications including collaboration tools, IP Telephony (VoIP), audio conferencing, E-learning using video on demand, and executive video broadcasts using what we call the IP/TV® solution. These applications do not function optimally over a VPN client-based software solution. It was important that we extend corporate applications to the home, without compromising corporate security or IT management policies.

Challenges

Security: Protecting remote small offices and workers connected to the enterprise network requires the same degree of security as the main entrances. A 2003 security study conducted jointly by the Computer Security Institute and the FBI concluded that 78% of network attacks come through the Internet -- the remote mobile worker's primary method of network entry. End-to-end security is critical as remote employees may be opening up unguarded "back doors" into the corporate network. It is imperative to not

only have strong authentication features and policies to ensure who is accessing the network, but that the device accessing the network is healthy. Virus infection on data networks has become a serious problem and the health of the device must be established before network access is granted and viruses have a chance to be propagated.

Central IT Management: Typically, the mobile environment exists outside the control and sight of corporate management. This introduces complexity in remotely managing, supporting and applying policies over a network of widely distributed remote access points. In many cases, IT staff, wanting to do the right thing, will try to assist do-it-yourself users having problems even though the equipment is not supported. This can result in shadow IT projects, special configurations, and a significant drain on limited resources. The hidden cost can be substantial.

Enterprise Class Teleworker Trial Solves Challenges

In order to extend advanced applications to the home with Quality of Service, while incorporating end-to-end security and IT-management policies, Cisco deployed a pilot teleworker hardware solution. The trial consisted of approximately 600 employees with residential-class cable and DSL broadband access services, VPN routers, and IP Phones. Based on the results of this trial, we are rolling out this solution to employees worldwide this fall.

The router in the home provides advanced end-to-end security features, such as proxy authentication, which establishes the identity of the person logging in. In addition, Network Admission Control establishes the health of the device, before the user is granted access. This helps prevent viruses from propagating on the network. In addition, as legislation to protect personal data is on the rise, all data must be encrypted. The hardware device facilitates this encryption without causing jitter or delay for voice or video applications. IT can manage these remote routers and ensure that security policies are not left in the hands of individuals.

Business Results

Return on Investment / Lower Total Cost of Ownership:

- Participating groups reported an average cost savings of \$100 per month in phone charges per employee by using IP Telephony technology in the home
- Aggregated savings were almost \$430,000 per month with a payback period of less than two months
- Possible real estate savings were not calculated into the measurement, but prove considerable for other organizations that are new to supporting telecommuting in the workplace

Productivity:

- Participating trial users gained an average of 30 minutes per day based on no commute time
- Users also noted an additional four hours per day gained per month, as they were able to continue to work despite inclement weather, sick family members, or traffic delays

Policies that Facilitate Success:

- Employees are eligible for a monthly reimbursement up to \$100 for Internet Service Provider (ISP) access to telework. Employees can select the ISP of their choice
- Employees can expense up to \$500 for one-time installation and equipment fees associated with ISP access for teleworking
- Approval for teleworking and a monthly reimbursable account require a one-time Manager approval

Business Continuance: Our Experience

Teleworking is an essential and integral part of Cisco's Business Continuance or Continuity of Operations Plan. As an example, the major ice storms and snow last winter impacted one of our major Research and Development facilities in Raleigh, North Carolina. Our Cisco campus was without electricity for several days, resulting in the complete displacement of more than 2,500 employees until power was restored and roads were safe. Approximately 50 of the North Carolina employees, including several

members of the Technical Assistance Center (TAC), were participating in the teleworker pilot program. These employees found that when their homes had power, their teleworker setups were functional, offering them access to the full suite of corporate applications required to maintain business operations.

Some employees, when notified that their homes would be without power for an extended period, simply transported their hardware setup to a location with power and broadband service and continued working. The cost savings were measurable, tangible and substantial. Business continuity was not based on the number of employees who had four- wheel drive, but rather on a secure, managed and fully functional solution.

Business Continuance and the Federal Government

The Presidential Directive PDD 67, issued by President Clinton in October of 1998, directs all levels of government to plan for and be able to continue minimum operations in any potential national security situation. It assigns specific, essential functions to federal agencies based on their existing statutory authorities and capabilities. Each agency must publish a Continuity of Operations Plan; support the program by maintaining the necessary planning and budgeting processes; and ensure their ability to respond during a national emergency through training, testing, and evaluation.

In addition to PDD-67, the Federal Preparedness Circular 65, Federal Executive Branch Continuity of Operations (COOP), provides guidance for agencies as they plan for continuing essential functions when emergencies disrupt normal operations. EPA Order 2030.1, Continuity of Operations Plan Policy, establishes a uniform policy for developing and implementing COOPs within the Agency. It also ensures that Agency's internal organizations are able to continue essential operations during man-made, natural, technological, and national security emergencies.

Many Federal agencies are in the early stages of establishing teleworking capabilities that could easily integrate with a continuity of operations plan. The objective is to provide continuity of operations based on home broadband connectivity or telework

versus connectivity from a remote site or alternative disaster recovery site. The premise is that, in the event of a natural disaster or homeland security threat, a large number of government employees will 1) not likely be able to travel to an alternate site due to traffic congestion or 2) not wish to leave their families during the threat. Additionally, avoiding ever having all of the individuals capable of performing a particular function in the same physical location can dramatically reduce terrorist threat vulnerability.

Cisco is in discussions with organizations to develop workable demonstrations of this capability, modeled after our own deployed solution. The demonstrations leverage two critical components, residential broadband access and telecommuting solutions, to ensure access to the host organization's rich array of networked business applications including video for real-time command and control decision making. It also includes home office use of fuel cell technology which provides an alternative fuel source in the event of a power grid failure. So in the event of a man-made, natural, technological, or national security emergency, the host organization's internal employees will be able to continue essential operations from their home sites or alternate locations securely and under the control of the internal Information Technology department. The main tenets of PDD-67 as well as the Federal Preparedness Circular 65 and EPA Order 2030.1 will have been met.

Working with and Recruiting Employee Talent from Remote Locations

Cisco leverages talent in many locations and it is critical to the success of our business model for these employees to be able to work together seamlessly with their peers, colleagues, customers, and managers as a type of Networked Virtual Organization.

The U.S. Federal government, like many governments around the world, is facing a demographic challenge. Over half of the current federal team will be eligible for retirement in the next five years. The percentage in the area of IT professionals is even higher. It will be exceedingly challenging to recruit and retain adequate numbers of qualified individuals to overcome the anticipated talent losses. It is our experience that offering a robust telecommuting solution dramatically increases the attractiveness of

joining the team and would place the federal government in a much stronger position to compete for these resources. The higher level of productivity, which can be achieved with the right telecommuting solution, will also help in alleviating the replacement demands.

Providing employees with access to equivalent and common sets of applications and services in geographically dispersed locations creates a built-in backup plan to keep business processes functioning in unforeseen circumstances.

Summary

After more than ten years experience, our company still adheres to the same basic policy of using broadband technologies and teleworking to improve the productivity and quality of our workforce. Support for Telecommuting by business and government provides an additional incentive for Americans to obtain broadband services. The President has recognized the importance of universal broadband connectivity to our nation's security, productivity, educational achievement, and quality of life which is why he has called for universal availability of broadband by 2007. Enhancing the federal government's use of telecommuting can be an important driver in achieving the President's goal.

I would like to thank you, Mr. Chairman and other committee members, for inviting me here today. I am happy to answer your questions.