Before the
UNITED STATES DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Washington, DC 20230

In the Matter of:	**)**	
	)	
Deployment of Internet Protocol,	**)**	**Docket No. 040107006-4006-01**
Version 6	**)**	
	)	

MCI COMMENTS

WorldCom, Inc. d/b/a MCI (MCI) hereby submits its comments on the Department of Commerce's Notice of Inquiry (Notice) concerning issues implicated by the deployment of Internet Protocol version 6 (IPv6) in the United States.

The Notice was issued by the Department of Commerce in response to the President's *National Strategy to Secure Cyberspace*, which directs the Department of Commerce to "[f]orm a task force to examine the issues related to IPv6, including the appropriate role of government, international interoperability, security in transition, and costs and benefits."[1] The *National Strategy* emphasizes that the reliability and secure use of the Internet Protocol (IP) are essential to the security of the Internet infrastructure.[2]

The Task Force, which is co-chaired by the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA), has issued the Notice in order to solicit comments on (1) the benefits and possible

[1] *The National Strategy to Secure Cyberspace*, February, 2003 at 30.
[2] *Id*.

uses of IPv6; (2) current domestic and international conditions regarding the deployment of IPv6; (3) economic, technical, and other barriers to deployment of IPv6; and (4) the appropriate role for the U.S. government in the deployment of IPv6.[3] According to the Notice, any submitted comments will be used as input to the Task Force's interim report, which is to be discussed at a public roundtable meeting to be held in the first half of 2004.[4]

MCI's comments reflect its experience as a leading provider of IP-based services. Today, MCI offers IP-based services at speeds from dial to OC-48 over the farthest-reaching global IP network, a 98,000-mile global fiber optic network that spans more than 4,500 Points of Presence (POPs) throughout the world. MCI is also a pioneer in the deployment of IPv6, having offered IPv6 services over its very high speed Backbone Network Service (vBNS+) since 1998.

II. Benefits and Costs of IPv6

In order to assess the likely course of IPv6 deployment, the Task Force asks parties to compare the benefits of IPv6 to the costs of deploying IPv6, including the "transition" costs of introducing IPv6

A. Address Space

The most significant benefit offered by IPv6 is its capability to dramatically increase the number of computers connected to the Internet without relying on Network Address Translators (NATs).

---

[3] Notice at 1.
[4] *Id.* at 3.

As is discussed in the Notice, IPv4 address availability is limited by both the size of the IPv4 "address space" and by past address assignment practices. Although there has been considerable debate about the precise date on which the IPv4 address space will be depleted, the need to conserve IPv4 addresses has already had a signficant impact on the architecture of the Internet. In place of the "peer-to-peer" architecture envisioned by the IPv4 protocol designers, network operators have inserted NATs throughout the Internet in order to share public IPv4 addresses among multiple computers.

Although NATs have allowed the Internet to continue growing despite limitations on the availability of IPv4 addresses, the introduction of NATs has had a number of negative side effects. In particular, it has been MCI's experience that NATs make it more difficult to deploy new Internet applications: because NATs are tailored to existing applications, new applications can often be introduced only by reconfiguring NATs or through workarounds that may not work in all cases. Fundamentally, an Internet that relies on NATs is more complex and less flexible than an Internet in which each computer has its own unique address.

Because the IPv6 address space is so much larger than the IPv4 address space, a virtually unlimited number of computing devices could be connected to the Internet without the use of NATs. Such a significant expansion of the address space is likely to be necessary to accommodate the expected proliferation of wireless data devices, computers connected to "always-on" cable modem and DSL services, and other new types of computing devices. And by creating a NAT-free infrastructure, IPv6 would provide a flexible platform for the development of new applications.

B. Security and Other Benefits

In addition to the expanded IP address space, IPv6 offers a number of additional features. These features include simplified network management, more efficient routing, improved support for class-of-service, and improved support for mobile devices. The inclusion of these features reflects experience gained in operating IPv4 networks over the past two decades.

One of the features of IPv6 that has attracted significant attention is the potential for improved network security. In particular, the President's *National Strategy to Secure Cyberspace* cites the improved security features of IPv6 in its discussion of measures that could be taken to develop "secure and robust mechanisms that will enable the Internet to support the Nation's needs now and in the future."[5]

The network security improvements offered by IPv6 fall into two categories. First, IPv6 networks are potentially more robust than today's NAT-reliant networks. NATs are a point of vulnerability in the network: typically, if a NAT fails, all connections that are set up through that NAT are lost even if there is an alternate physical path. The vulnerability of communications to such NAT failures is at odds with the original objectives for the Internet, which was designed to allow communications to be routed around points of failure.

Second, IETF standards require that all implementations of IPv6 include IPsec, which is a suite of protocols that define mechanisms for authenticating and encrypting IP packets. Although IPsec is compatible with IPv4, the "mandatory" inclusion of IPsec in the IPv6 specification is expected to result in far wider distribution of IPsec-capable computers.

Moreover, "end-to-end" security protocols such as IPsec are difficult to deploy in many IPv4-based networks because of the widespread use of NATs in such networks.

III. Status of IPv6 Deployment

Much of the groundwork has been laid for commercial deployment of IPv6. Although work continues on IPv6-related topics within the IETF, the core IPv6 specifications have been finalized and are sufficiently complete to support initial commercial implementations of IPv6. IPv6 has been tested extensively in a variety of research networks, both in the United States and around the world. Those testbeds have allowed researchers to investigate IPv6 protocol implementations and, more recently, operations and transition issues as well.

The translation of IETF standards and the experience gained from research testbeds into commercial deployment is slowly beginning to occur. For example, MCI offers IPv6 services to government customers over its vBNS+.[6] Software and network equipment vendors are increasingly implementing IPv6 in their products. Most key software vendors now include IPv6 implementations in their operating system software. And the availability of IPv6-capable routers and other network equipment is growing steadily.

In deploying IPv6, MCI is drawing on its years of experience providing IPv6 services over the vBNS+. A key consideration for MCI is ensuring that IPv6 services meet the performance requirements of commercial customers. In order to continue providing the service level agreements (SLAs) that commercial customers have come to expect, commercial IPv6

---

[5] *National Strategy* at 30.

[6] *See* http://www.vbns.net/; http://global.mci.com/us/enterprise/govt

services require not only upgrades to routers, but also upgrades to network management and monitoring. Moreover, commercial-quality services require careful attention to the interworking and coexistence of IPv4 and IPv6. MCI expects that IPv4 and IPv6 will coexist for many years to come.

IV. Government's Role

In the Notice, the Task Force asks whether government should be involved in fostering or accelerating the deployment of IPv6 and, if so, what actions government should take.

Although the deployment of IPv6 has occurred more slowly than was anticipated when the IETF began work on IPv6, there is no evidence of a market failure warranting government intervention. To a great extent, the current pace of IPv6 deployment reflects the normal weighing of benefits and costs that is associated with any technology deployment. Although IPv6 offers significant benefits over IPv4, particularly when the disadvantages of NATs are taken into account, it is clear that the use of NATs made access to the larger IPv6 address space less urgent. Moreover, the costs of IPv6 deployment are significant: as discussed above, the deployment of commercial-grade IPv6 services by ISPs is a complex undertaking. Similarly significant are the costs of developing new applications or porting existing applications to work with IPv6.

Notwithstanding these considerations, it is probable that demand for IPv6-based services will grow over the short- and medium-term and that deployment of IPv6 will accelerate as customers and service providers develop applications that make full use of

IPv6's capabilities. Of particular significance is the growing presence of IPv6 implementations in operating system software. As more and more computers become IPv6-capable, it becomes more likely that customers will develop applications that use IPv6's capabilities and will thus generate demand for IPv6 services. And as ISPs respond to that demand by expanding their IPv6 offerings, those expanded offerings will in turn spur the development of additional applications that take advantage of those offerings.

A second key trend that has the potential to drive demand for IPv6 services is the proliferation of wireless data devices and devices attached to "always-on" connections such as cable modems and DSL. The expected growth in the number of such devices, coupled with the fact that some potential applications for such devices require that each device be assigned a unique address, is likely to require the much larger IPv6 address space. For example, the wireless industry's Third Generation Partnership Project (3GPP) is making use of IPv6 in the 3GPP standards. Moreover, growth in the number of computers connected to "always-on" services such as cable modem and DSL is likely to drive demand for "end-to-end" security of the type offered by IPsec within IPv6.

Even without direct government intervention, the federal government will play a key role in influencing the pace of IPv6 deployment, in its capacity as a significant customer for IP-based services and equipment. As is demonstrated by the Department of Defense's recent announcement concerning IPv6, federal agencies may find that security requirements and other factors necessitate planning for IPv6. In its announcement, DoD explained that it found IPv4 to

be "incapable of meeting the long-term requirements of . . . DoD,"[7] and cited benefits of IPv6 such as improved security and "new enhancements to quality of service and easing system management burdens."[8]

Because of IPv6's improved support for IPsec, the early adoption of IPv6 by federal agencies would be fully consistent with the *National Strategy to Secure Cyberspace*. As the *National Strategy* emphasizes, "federal agencies should become early adopters of new, more secure systems and protocols where appropriate."[9]

Once IPv6 begins to be more widely deployed, the Task Force should assess whether that deployment is meeting the goals of the *National Strategy to Secure Cyberspace*. Although it is "mandatory" for IPv6 implementations to support IPsec, there is no requirement that IPsec actually be used. The extent to which IPsec is used will depend on a variety of factors, including the security policies adopted by the communicating parties, the availability of alternate security mechanisms, the interoperability of IPsec implementations, and the development of effective key distribution mechanisms. As part of its mandate, the Task Force should continue to monitor the deployment of IPv6 to determine the extent to which the potential for improved network security is being met.

[7] DoDD 8100.1 Global Information Grid Overarching Policy, September 19, 2002, at 1.
[8] *Id*.
[9] *National Strategy* at 43.

V. Conclusion

Although the deployment of IPv6 will involve significant costs, the benefits of IPv6 over IPv4 are sufficiently important that it is probable that demand for IPv6 products and services will grow in the coming years. It is also probable that federal agencies will play a significant role as early adopters of IPv6.

Respectfully submitted,
WORLDCOM, INC. d/b/a MCI

/s/ Alan Buzacott

Alan Buzacott
Senior Manager, Reglatory Affairs
1133 19th Street, N.W.
Washington, DC 20036
(202) 887-3204

March 8, 2004