3. The Committee functions solely as an advisory body under the Federal Advisory Committee Act.

4. The Committee reports to the Director of the Census Bureau.

Membership

1. Members are appointed by and serve at the discretion of the Secretary of Commerce.

2. Members are appointed to the nine-member Committee for a period of three years. Members will be reevaluated at the conclusion of the three-year term with the prospect of renewal, pending Advisory Committee needs and the Secretary's concurrence. Committee members are selected in accordance with applicable Department of Commerce guidelines. The Committee aims to have a balanced representation, considering such factors as geography, gender, technical expertise, community involvement, and knowledge of census procedures and activities. The Committee aims to include members from diverse backgrounds, including State and local governments, academia, media, research, community-based organizations, and the private sector. No employee of the Federal government can serve as a member of the Committee. Meeting attendance and active participation in the activities of the Advisory Committee are essential for sustained Committee membership.

Miscellaneous

1. Members of the Committee serve without compensation, but receive reimbursement for Committee-related travel and lodging expenses.

2. The Committee meets at least once a year, budget permitting, but additional meetings may be held as deemed necessary by the Census Bureau Director or Designated Federal Official. All Committee meetings are open to the public in accordance with the Federal Advisory Committee Act.

Nomination Information

1. Nominations are requested as described above.

2. Nominees should have expertise and knowledge of the cultural patterns and issues and/or data needs of the Hispanic community. Such knowledge and expertise are needed to provide advice and recommendations to the Census Bureau on how best to enumerate the Hispanic population and obtain complete and accurate data on this population. Individuals, groups, or organizations may submit nominations on behalf of a potential candidate. A summary of the candidate's qualifications (résumé or curriculum vitae) *must* be included with the nomination letter. Nominees must have the ability to participate in Advisory Committee meetings and tasks. Besides Committee meetings, active participation may include Committee assignments and participation in conference calls and working groups.

3. The Department of Commerce is committed to equal opportunity in the workplace and seeks diverse Committee membership.

Dated: January 15, 2004.

Charles Louis Kincannon,

Director, Bureau of the Census.

[FR Doc. 04–1185 Filed 1–20–04; 8:45 am]

BILLING CODE 3510–07–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

National Telecommunications and Information Administration

[Docket No. 040107006–4006–01]

Request for Comments on Deployment of Internet Protocol, Version 6

AGENCIES: National Institute of Standards and Technology, National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice of inquiry.

SUMMARY: The President's National Strategy to Secure Cyberspace directed the Secretary of Commerce to form a task force to examine the issues implicated by the deployment of Internet Protocol version 6 (IPv6) in the United States. As co-chairs of that task force, the Commerce Department's National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA) invite interested parties to comment on a variety of IPv6-related issues including: (1) The benefits and possible 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. Comments should be submitted on paper and, where possible, in electronic form as well. All comments submitted in response to this Notice will be posted on the NTIA Web site.

DATES: Interested parties are invited to submit comments no later than March 8, 2004.

ADDRESSES: Comments may be mailed to the Office of Policy Analysis and Development, National Telecommunications and Information Administration, Room 4725, Attention: Internet Protocol, Version 6 Proceeding, 1401 Constitution Ave., NW., Washington, DC 20230. Parties should submit an original and five (5) copies. Where possible, parties should include a diskette or compact disk in ASCII, WordPerfect (please specify version) or Microsoft Word (please specify version) format. Diskettes or compact disks should be labeled with the name and organizational affiliation of the filer, and the name and version of the word processing program used to create the document. In the alternative to a diskette or compact disk, comments may be submitted electronically to the following electronic mail address: *IPv6@ntia.doc.gov.* Comments submitted via electronic mail should also be submitted in one or more of the formats specified above.

FOR FURTHER INFORMATION CONTACT: Alfred Lee, Office of Policy Analysis and Development, at (202) 482–1880. Media inquiries should be directed to the Office of Public Affairs, National Telecommunications and Information Administration, at (202) 482–7002.

SUPPLEMENTARY INFORMATION:

I. Background

A. The Internet Protocol

The Internet Protocol (IP) is a technical standard that enables computers and other devices to communicate with each other over networks, many of which interconnect to form the Internet. By providing a common format for the transmission of information across the Internet, IP facilitates communication among a variety of disparate networks and devices. This ability to communicate with a single, widely accepted format has been a key to the rapid growth and success of the Internet.[1]

The current generation of IP, version 4 (IPv4), has been in use for more than twenty years, and has supported the Internet's phenomenal growth over the last decade. A variety of stakeholders, through the guiding efforts of the Internet Engineering Task Force (IETF), have developed a newer version of IP, known as IPv6, which has several advantages over IPv4, including the availability of many more Internet

---

[1] *See, e.g.,* Barry M. Leiner, et al, ''A Brief History of the Internet,'' *http://www.isoc.org/internet/history/brief.shtml.* This document describes the development of the Internet and explicitly describes the original decision to use IP in a widespread manner. *See http://www.isc.org/ds/host-count-history.html* for statistics on the rapid growth of Internet hosts.

addresses and additional user features and applications.[2] IPv6 has also been designed to provide other features and capabilities such as improved support for hierarchical addressing, a simplified header format, improved support for options and extensions, additional auto-configuration and reconfiguration features, and native security features.[3]

B. Commerce Department Task Force

In light of the potential benefits of IPv6, especially the security implications, the President's National Strategy to Secure Cyberspace directed the Secretary 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. The task force will solicit input from potentially impacted industry segments.[4]

In response, the Commerce Department formed a task force to study IPv6 and to prepare a report of its findings and recommendations. The task force is co-chaired by the Administrator of the National Telecommunications and Information Administration (NTIA) and the Director of the National Institute of Standards and Technology (NIST) and consists of staff from these two agencies. The task force will operate in consultation with the Department of Homeland Security and with other federal offices and agencies, as appropriate.

The task force is in the process of gathering information from a variety of sources, including this request for comment, survey research, and a public roundtable meeting to be held in the first half of 2004. Prior to the public meeting, the task force intends to release an interim report, which will be discussed at the meeting.

C. Request for Comment

By issuing this request for comment, the task force wants to develop a record on the following broad questions, which are set forth in greater detail below: (1) What are the potential uses and benefits of IPv6; (2) what are the costs associated with deploying IPv6; (3) what are the current and projected penetration rates of IPv6; and (4) what is the appropriate role for the U.S. government in the deployment of IPv6?

In answering the questions posed in this request for comment, we urge commenters to provide specific, empirical data and underlying assumptions whenever possible. We also request commenters to supply us with any technical reports or economic analyses that they cite to or rely on in their comments. We further ask commenters, where appropriate, to address how their responses vary, if at all, among different customer markets for communications services and products (*e.g.,* small and medium enterprises, large enterprises, academia, civilian government, military, individual users, and any other relevant segments).

II. Potential Benefits and Uses of IPv6

We seek comment on the potential benefits and uses of IPv6. As described below, some of the potential benefits commonly associated with IPv6 include a significant increase in the number of available Internet addresses, a proliferation of new applications building on peer-to-peer communications, and improved security. We request comment on these and other possible benefits related to widespread adoption of IPv6. We request comment on the benefits accruing to both end users and system providers.

A. Increased Address Space

One of the most commonly cited benefits of IPv6 is the vastly expanded number of individual addresses that IPv6 will enable. IPv4 uses a 32-bit IP address scheme that allows more than 4 billion individual addresses to be identified on the Internet. With the explosive growth rate of Internet users and new applications over the last decade, concerns have been raised that the currently defined IPv4 address space may not be sufficient to meet the needs of the growing Internet user base.[5] By expanding the existing IP address field to 128 bits, IPv6 offers a vast pool (3.4 x 10^{38}) of assignable Internet addresses. As a result, IPv6 can enable an enormous number of new nodes and users to be connected to the Internet using their own unique Internet addresses.

The task force requests comment on the adequacy of IPv4 address space. Specifically, we seek estimates (and underlying assumptions) of how many IPv4 addresses have been allocated, how many are still available, and how long the remaining addresses will be sufficient to meet the needs of users in the United States, as well as users in other countries around the world.[6] We recognize that, because a large portion of the available IPv4 addresses have been allocated to North America, concerns regarding address availability may differ depending on the commenter's perspective. We therefore ask commenters to discuss how the purported limitations on IPv4 addresses will affect different geographic regions (*e.g.,* North America, Europe, Asia) and customer markets (*e.g.,* private sector, government, academia).

The task force also seeks comment on the potential uses for this greatly expanded pool of addresses. What new products, services, features, applications and other uses are likely to result from the additional addresses offered by IPv6? To the extent possible, commenters should provide estimates and underlying assumptions of the economic impact of these new uses and should identify which market segments will be affected by these uses.

The task force understands that the use of Network Address Translation devices (NATs) and the adoption of address conservation practices, such as

[2] Background information concerning the history of the Internet can be found at *http://www.isoc.org/internet/history/.* IETF efforts to transition from IPv4 to a successor protocol standard are described in S. Bradner, ''The Recommendation for the IP Next Generation Protocol'', RFC 1752 (Jan. 1995), *http://www.ietf.org/rfc/rfc1752.txt?number=1752.* Because of the vast amount of widely available resources that provide information on IPv6 and related topics, only representative citations are contained herein for the purpose of facilitating responses to this Notice. Commenters are requested to cite, as appropriate, specific references in support of comments submitted.

[3] For the purposes of this Notice, IPv6 can be defined with reference to IETF Request for Comments (RFCs) that contain the relevant standards. *See http://www.ietf.org* for updated information on this matter. Within the IETF, the IP Next Generation (IPng) Working Group developed IPv6, including the ''core'' draft standards approved in August 1998 (*i.e.,* RFCs 2460, 2461, 2462, 2463). To date, more than 70 RFCs comprise the suite of IETF documents that define IPv6. While the IETF continues to standardize IPv6, and a wide range of related efforts are being undertaken by other organizations (*e.g.,* the IPv6 Forum), the essential features of IPv6 appear to be well established and manufacturers already have a range of IPv6 compatible products available in the marketplace.

[4] The National Strategy to Secure Cyberspace, A/R 2–3, at 30 (Feb. 2003), *http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.*

[5] IETF RFC 1752 (*see* note 2, *supra*) estimates that IPv4 address space will be exhausted ''between 2005 and 2011'' and notes relevant assumptions underlying this estimate, which was made in 1993. While estimated dates for potential exhaustion of the IPv4 address space vary widely, a calculation made more recently by Christian Huitema purports to confirm the RFC 1752 timeframe projection. In his view, ''we are again facing a crisis. We must either deploy IPv6 or risk a strange evolution of the Internet toward a set of disconnected networks.'' Christian Huitema, *Routing in the Internet* 366 (2d ed. 2000). Information relating to allocation of IPv4 and IPv6 addresses is provided by the American Registry for Internet Numbers (ARIN). *See, e.g. http://www.arin.net/announcements/20031027_ipv4.html. See also Mark McFadden and Tony Holmes,* ''Report of the Ad Hoc Group on Numbering and Addressing'' (Mar. 2001), *http://www.icann.org/committees/adhoc/mcfadden-holmes-report-08mar01.htm.*

[6] *See, e.g.,* Geoff Huston, ''IPv4 Address Lifetime Expectancy—2003 *http://www.apnic.net/community/presentations/docs/ietf/200307/v4-lifetime-20030715.ppt.*

Classless Inter-Domain Routing (CIDR), have slowed the consumption of available IPv4 addresses. We seek comment on the accuracy of this understanding. While the adoption of NATs over the last decade has apparently slowed the consumption of IPv4 addresses, we understand that NATs have contributed to the development of separate, privately addressed networks that are interconnected with the public Internet. Because NATs act as gateways between the public Internet and users with private network addresses, each NAT device could potentially represent a single point of failure for traffic moving between a privately addressed network and the public Internet. We seek comment on the effects that NATs (as well as CIDR and other address conservation strategies) may have on network performance and network reliability.

B. Purported Security Improvements

The task force seeks comment on the ability of IPv6 to improve the security of information transmitted over IP networks. In general, we ask commenters to address any characteristics of IPv6 that directly or indirectly enhance network security compared to IPv4. Conversely, we also seek comments on any features of IPv6 that may degrade network security compared to IPv4.

We also seek specific comment on Internet Protocol Security Architecture, or IPsec, as it relates to an examination of the relative merits of IPv4 and IPv6. IPsec is a data security specification that is designed to protect the integrity and confidentiality of data traffic carried over the Internet.[7] We understand that while IPsec in IPv4 is functionally equivalent to that available in IPv6, IPsec support is optional in IPv4 networks. Because IPsec is a standard feature of IPv6, will IPsec be easier to use with IPv6 than with IPv4 and, therefore, more widely used? If IPv6 adoption leads to the elimination of NAT devices on the Internet, is it more likely that IPsec will work better as a widely used, end-to-end security mechanism? Are there critical IPsec implementation issues that are independent of the version of IP employed? To what extent will a successful IPsec implementation depend on the development of workable trust models that deal adequately with issues such as public-key management and the adoption of effective security policies? The task force requests comment on these and any other issues involving IPsec, relevant to the growth of IPv6.

We understand that IPsec also permits address authentication, thereby assuring the recipient that a particular message is actually coming from the purported addressor. We seek comment on whether this feature could potentially deter ''spoofing'' attacks or could facilitate tracing of undesirable messages.[8] Specifically, interested parties should explain how implementation of IPv6 or IPsec will accomplish those ends. As noted, moreover, IPsec is also available in IPv4. To what extent would deployment of IPv6 further national security and law enforcement interests over and above the security features and capabilities available via IPv4? The task force also understands that persons sending messages via the Internet can attempt to conceal their identities and addresses by, for example, operating through anonymous servers and relays operating at multiple protocol layers (*e.g.*, NATs, mailrelays, proxies). Assuming that ''network traceability'' is an important objective in cyber security, to what extent would adoption of IPv6 improve the ability of network operators and law enforcement officials to identify accurately the true source of malicious or illegal network activity?

C. End User Applications

Apart from its expanded addressing capabilities and purported security improvements, we understand that IPv6 has also been designed to address other important user needs, including reducing network management burdens, simplifying mobile Internet access, and meeting quality of service needs. We ask commenters to explain whether and how IPv6 accomplishes these and other functions in a manner superior to IPv4. We also request that commenters explain the importance or value of the improved capabilities afforded by IPv6. To the extent possible, we ask that commenters provide examples of how these improved capabilities of IPv6 could benefit current users of IPv4 (*e.g.*, cost savings, time savings).

One potential benefit of IPv6 is that its increased address space may further an original vision of the Internet. The task force understands that the Internet address space was originally designed to be a unified open scheme, connecting all users and nodes (each with its own unique address), as defined by the IPv4 addressing convention. A central idea was to allow users to communicate and run applications (*e.g.*, Voice over IP (VoIP), gaming, or file exchange) with each other, across the Internet, on a peer-to-peer basis. Interested parties are encouraged to comment on the desirability and potential effort required to return the Internet to a unified open scheme as originally designed.

As noted above, the use of NATs has contributed to the development of separate, privately addressed networks that are interconnected with the public Internet. At the same time, various other devices are apparently being deployed throughout the Internet to increase network functionality. Such devices, often referred to as ''middleboxes,'' appear to be proliferating in response to demand for capabilities that may include not only network address translation, but also firewall protection, intrusion detection systems, and other features.[9] There is some concern that use of NATs and other middleboxes may block or inhibit the growth of peer-to-peer applications. Some observers assert that deployment of IPv6, by vastly increasing the available address space, will eliminate the need for NATs in particular, which, in turn, could lead to a proliferation of new peer-to-peer applications. On the other hand, NATs and other middleboxes may persist in an IPv6 environment because they may be useful for other reasons, including affording users some protection from hackers launching attacks across the public Internet. We request comment on these and any other issues involving NATs (or their equivalents) and middleboxes, related to the growth of IPv6.

---

[7] *See, e.g.*, Pete Loshin, ''Securing the Internet with IPsec (Internet Security Architecture),'' *Earthweb* (Sept. 9, 1999), *http://itmanagement.earthweb.com/erp/article.php/615921.* This article provides background information on IPsec and its operation with IPv4 and IPv6. The task force notes that IPsec is only one method of protecting the security of private communications. Interested parties are encouraged to comment on the availability of other data security specifications and their effectiveness at protecting the security interests of users, providers, and government, as compared to IPsec.

[8] ''Spoofing'' refers to the creation of Internet packets using someone else's Internet address. *See, e.g.*, Matthew Tanase, ''IP Spoofing: An Introduction,'' *http://www.securityfocus.com/infocus/1674.*

[9] *See, e.g.*, M. Lerner, *et al.*, *Middleware Networks: Concept, Design, and Deployment of Internet Infrastructure* (2000). In this document, the term ''NAT device'' refers to equipment that performs only network address translation. We use the term ''middleboxes'' in this Notice to describe a broader category of equipment, which could encompass NAT devices and other equipment that provide a variety of capabilities including, but not necessarily, network address translation. For a discussion of thee potential effects of NATs and middleboxes on end-to-end Internet connectivity, see David Margulius, ''The Threat to Universal Internet Connectivity,'' *InfoWorld*, Nov. 21, 2003, *http://www.infoworld.com/article/03/11/21/46FEtrouble_1.html.*

Notwithstanding the criticisms of NATs, some have argued that NATs will not preclude peer-to-peer devices and applications.[10] The task force requests comment on the accuracy of this assertion. Similarly, we seek comment on the effects of middleboxes on the availability and efficacy of peer-to-peer devices and applications. If NATs or middleboxes do interfere with peer-to-peer interactions, can ''work arounds'' be developed for particular applications? If work arounds can be developed, to what extent will they adversely affect the performance of the associated applications? Will those work arounds scale well (*i.e.*, continue to function seamlessly and efficiently as the number of applications and users increases)? As importantly, what additional costs (in time, money, and complexity) will firms incur to develop work arounds for particular applications in order to accommodate NATs and middleboxes?

D. Network Evolution

Although the task force requests comments on the potential benefits of IPv6, we understand that IPv4 networks can incorporate many of the features and capabilities commonly associated with IPv6. Thus, some observers have claimed that the increase in address space afforded by IPv6 is the only compelling reason for adopting the new protocol, not the availability of other capabilities.[11] The task force seeks comment on this assertion. Specifically, the task force requests comment on the ease with which each feature and capability associated with IPv6 can be implemented over IPv4 networks and whether IPv4 implementations will perform as effectively as IPv6 networks. Will IPv4 networks providing IPv6-associated features and capabilities suffer a performance penalty as compared to IPv6 networks? We request comment on whether any IPv6 feature or capability cannot be readily implemented over IPv4 networks. We ask commenters to identify the cost of implementing such features or capabilities on IPv4 networks, as compared to the cost of implementing IPv6 alternatives? We request comment on whether any IPv6 feature or capability, or set of features or capabilities is markedly superior to its IPv4 alternative, in terms of implementation cost or relative performance, such that an IPv6 implementation would be the clearly preferred choice over IPv4.

The task force also seeks comment on whether there are any potential performance impairments associated with the adoption of IPv6. For example, would the increased size of the IPv6 header have a significant impact on voice quality in VoIP applications, which are generally sensitive to latency? If, for example, IPv6 header compression schemes are used to mitigate potential performance issues (*e.g.*, increased transmission latency), do such schemes require more router processing effort resulting in increased end-to-end latency? To be widely implemented, does IPv6 require new routing technologies (*e.g.*, new versions of BGP–4) that could result in significant end-to-end system design and operational challenges? Are there any drawbacks due to inherent limitations of the IPv6 protocol design? Are there drawbacks resulting from immature or (currently) impractical hardware and software IPv6 implementation technologies?

We understand that the deployment of IPv4 networking infrastructure continues to evolve in ways that can effectively use existing and emerging transport and transmission system infrastructures (*e.g.*, multi-protocol label switching (MPLS), asynchronous transfer mode (ATM), Frame Relay, optical, wireless, digital subscriber line (DSL), ethernet). Does IPv6 deployment depend on modifications to these underlying networks or require new transport and transmission systems to be implemented? Will IPv6 be able to utilize presently underused capabilities of transport and transmission networks to support new types of applications or to provide more efficient networking services for existing applications? We also seek comment on any spectrum management issues that might arise when IPv6-based wireless and hybrid networks are used to support mobile and fixed applications. Because IPv6 offers new capabilities, do the transport layers (*e.g.*, transmission control protocol (TCP), user data protocol (UDP)) need to be modified to support both existing and new applications? Further, we request comment on whether and to what extent the transport layers need to be modified in order to realize the full capabilities of IPv6, including the potential for significantly improved IP network performance.

E. Other Benefits and Uses

The task force seeks comment on the range, attractiveness, and potential economic impact of new services that will emerge with the growth of IPv6. Specifically, what new service possibilities does IPv6 provide beyond those available using IPv4? We also ask commenters to identify other benefits and uses of IPv6 and to describe the potential economic and other impacts of such developments. For example, does VoIP represent the kind of application that could drive IPv6 adoption, and if so, how? Will IPv6 improve the performance of VoIP? Please identify other applications that could drive or benefit from the adoption of IPv6. Are there applications that could thrive with only a partial implementation of IPv6?

III. Cost of IPv6 Deployment and the Transition From IPv4 to IPv6

The task force seeks information on the factors that may cause individuals and organizations to adopt IPv6 and, most importantly, the costs of doing so and the transitional issues presented. We encourage interested parties to provide us with specific detail, to the extent possible, on their IPv6 deployment strategies. What factors influence an organization's decision to adopt IPv6? For example, is there a certain level of IPv6-based traffic that will cause network operators or ISPs to convert their facilities to IPv6? Is there a critical point at which consumers' acquisition and use of IPv6-capable terminal equipment and applications will drive deployment of IPv6-capable infrastructure? To what extent, if at all, do these factors vary by provider (*e.g.*, network operator, ISP, equipment vendors, applications providers) and by market segment (*e.g.*, small and medium enterprises, large enterprises, academia, civilian government, military, individual users, and any other relevant segments)? As importantly, why are certain organizations choosing not to implement IPv6 at this time?

A. Cost of Deploying IPv6

The task force seeks specific data on the hardware, software, training, and other costs associated with implementation of IPv6. In responding to the questions below, we ask commenters to discuss the extent to which any of these costs may vary by market segment. They should also

[10] *See, e.g.*, Dan Jones, ''European IPv6 Plan Comes Under Fire,'' *Light Reading*, at 2 (Mar. 7, 2002) (citing statement of Paul Francis, inventor of the NAT).

[11] *See, e.g.*, Geoff Huston, ''Waiting for IP version 6'', at 9, *The ISP Column* (Jan., 2003); John Klensin, ''A Policy Look at IPv6: A Tutorial Paper,'' at 17 (Apr. 2003). *Contra* Latif Ladid and Jim Bound, ''Response by IPv6 Forum,'' *The ISP Column* (Jan. 2003). Claimed benefits of IPv6, including but not limited to resolution of IPv4 address depletion issues, are discussed in an IETF work in progress that outlines the business and technical case for IPv6. See S.King, *et al.*, ''The Case for IPv6 (Dec.1999). A wide range of potential IPv6 benefits are described in *http://www.ipv6forum.com/navbar/papers/IPv6-an-Internet-Evolution.pdf*, which was prepared by the IPv6 Forum, a leading global proponent of IPv6 deployment.

discuss whether and to what extent the costs might vary depending on the nature of the IPv6 implementation (*e.g.*, a ''greenfield'' implementation versus one that overlays or replaces an embedded IPv4 base)? To what extent do the IPv6 costs vary with the size of the embedded IPv4 base? In instances where IPv6 capabilities are already deployed, what factors must be present to ''turn on'' existing IPv6 functionality?

1. Hardware Costs

Deploying IPv6 on a national scale will require a substantial replacement and/or upgrading of existing IPv4 equipment. The task force solicits comments on the nature and magnitude of the costs of deploying IPv6, including the likely time period over which those costs will be incurred. For example, routers, hosts, servers, and terminal equipment presumably will have to be replaced or modified in order to originate, transport, and receive IPv6 traffic. If only modifications are required, will they involve hardware changes (*e.g.*, router line cards)? What are the likely costs of those changes? What additional costs will be incurred (*e.g.*, training/retraining costs, transition testing on operational functionality and performance)? Will the premises equipment that enables broadband transmission services (*e.g.*, DSL and cable modems) need to be replaced or modified in order to carry IPv6 traffic and, if so, at what cost?

As embedded IPv4 equipment reaches the end of its useful life, users will presumably need to acquire replacements. What are the useful lives of the various categories of such equipment (*e.g.*, routers, servers, premises equipment) and how has the duration of those lives changed over time? Are there differences between the technical and economic lives of particular equipment that may have a bearing on the decision to move from IPv4 to IPv6? When the time comes to replace existing IPv4 equipment, will the relative costs be such that users will tend to purchase IPv6-capable equipment? Or will the added direct and indirect costs (*e.g.*, operating, and administrative costs) of purchasing IPv6 equipment induce users to stay with IPv4-compatible equipment and applications? Will manufacturers continue to produce equipment and applications that can handle only IPv4 packets? What market conditions would persuade manufacturers to cease offering IPv4 equipment?

2. Software Costs

To what extent will the modifications to routers, hosts, servers, and terminal equipment mentioned above involve only software changes? What is the likely magnitude of those costs? Will various applications and Internet services (*e.g.*, search engines, content delivery networks, DNS) have to be modified to make them compatible with IPv6 transmission? What are the estimated costs of those changes? Will the necessary modifications to software and applications require extensive changes in the underlying coding and, if so, at what cost? Are there differences in the useful life and cost of software, as compared to hardware, that make it likely that firms will acquire and implement IPv6 software and applications before IPv6 hardware, or vice versa?

3. Training Costs

An organization's personnel will have to be trained in how to install, operate, maintain, and service IPv6 hardware and software. How much will that training cost? How do training costs compare (*e.g.*, in percentage terms) to the costs of IPv6 hardware and software? To what extent does the likely costs of training influence an organization's decision to adopt IPv6?

4. Other Costs

What are the opportunity costs of waiting to deploy IPv6? [12] To what extent will these costs vary by market segment (*e.g.*, small and medium enterprises, large enterprises, academia, civilian government, military, individual users, and any other relevant segments)? How will the transition path of the U.S., relative to the rest of the world, influence costs and prices of IPv6 equipment, services, and applications? For example, will costs and prices decrease over time as a function of the worldwide IPv6 installed base? Could waiting for international development and deployment of IPv6 lead to reduced R&D costs and fewer security problems for U.S. adopters? Would the U.S. benefit from lessons learned by early adaptors or will there be minimal knowledge spillovers? Conversely, will late entry into global IPv6 markets by U.S. firms have a significant long-term negative effect on market shares and economic performance? What is the impact of slow IPv6 deployment on the development of native IPv6 applications?

[12] The ''opportunity cost'' of an action or choice is the net benefits associated with the next best alternative to the course of action adopted. For a more complete discussion of opportunity cost, see Michael Parkin, *Economics* 10, 53–56 (1990).

B. Transition Costs and Considerations

1. Migration From IPv4 to IPv6 and the Coexistence of Dual Protocols

As our nation migrates from IPv4 to IPv6, there will be a period of time during which IPv4 and IPv6 operate simultaneously. The task force seeks comment on the costs and any other issues related specifically to this migration from IPv4 to IPv6. For example, what are the costs, burdens, and potential problems of ensuring interoperability between IPv6 and IPv4 networks? What are the incremental costs resulting from operating IPv6 and IPv4 concurrently? To what extent will various interoperability solutions continue to function efficiently and effectively as traffic increases? Does the operation of dual IPv4/IPv6 equipment impose significant costs relative to IPv4 or IPV6-only equipment? To what extent do measures to ensure interoperability reduce the performance of network routers, increase routing tables, or have other adverse effects?

Many observers assume that, regardless of the pace of IPv6 deployment, there will be significant ''islands'' of IPv4 for the foreseeable future.[13] There appear to be several transition mechanisms to allow interoperability among IPv4 and IPv6 hosts and networks, including dual stack, tunneling IPv6 over IPv4 networks, and IPv6-only to IPv4-only translation. What are the costs and benefits of each of these mechanisms? Is there a ''best'' or accepted approach that will provide for interoperability between islands of IPv4 and/or IPv6 and the Internet at large? What factors may determine whether and where alternative transition mechanisms will be available and applicable? Can alternative transmission mechanisms co-exist while still providing end-to-end interoperation among IPv6 and IPv4 networks? Does the embedded base of IPv4 equipment and applications function as a barrier that could isolate the U.S. from the benefits of foreign IPv6 deployments and/or testbeds?

The task force recognizes that industry groups have worked hard to ensure interoperability between IPv4 and IPv6 networks and applications. Will domestic and international market forces alone produce a level of network interoperability that maximizes overall social welfare, or will government intervention be needed to produce such

[13] 13 *See, e.g.*, Eric Carmés, ''The Transition to IPv6'' (Internet Society Briefing #6), *http://www.isoc.org/briefings/006/*, which describes transitional mechanisms for IPv6 and briefly discusses problems inherent with the coexistence of IPv4 and IPv6 networks.

an outcome? If government intervention is needed, what form should it take?

What problems, if any, may arise when existing IPv4 networks convert hardware, appliances and middleware to IPv6? Will applications that use IP services migrate easily? Are there estimates of the cost associated with these issues? On the other hand, implementation of IPv6 (as distinct from gains anticipated via the definition of the new protocol) could also yield substantial hardware and software advances. Currently, IPv4 operates on top of several protocol layers (*e.g.*, MPLS, ATM, frame relay, ethernet and wireless). Commenters are requested to explain how the technical requirements for these protocol layers and dependencies of protocol layers supported by IPv4 (*e.g.*, UDP and TCP) may be impacted by the use of IPv6.

The task force seeks comment on the adequacy of the existing set of IETF standards for IPv6. Is the current set of IETF standards for IPv6 technically complete enough to enable widespread commercial deployment of interoperable IPv6 (and IPv4/IPv6 transition mechanisms) networks, equipment and applications? Would it be helpful for the IETF standards-track RFCs to define ''mandatory'' services (*e.g.*, protocol capabilities) and ''optional'' services? What problems, if any, may arise in implementing IPv6, as embodied by the IETF standard set, in various types of equipment and software? Will the standards create undue hardship on equipment and software providers? Are additional industry or government specifications required to successfully realize the potential benefits of IPv6?

2. Security in Transition

Among the IPv6-related issues that the National Strategy to Secure Cyberspace directs us to study is ''security in transition,'' the need to ensure that security interests are protected during transition from IPv4 to IPv6. To what extent would the simultaneous operation of IPv4 and IPv6 networks and applications, potentially interconnected by a set of diverse transition mechanisms, compromise efforts to safeguard the integrity and security of communications traffic, or limit government's ability to protect legitimate security and law enforcement interests?

3. Other Transition Concerns

Proper Internet address allocation is achieved through a network of national (*i.e.*, the American Registry for Internet Numbers (ARIN)) and international (*i.e.*, Reseaux IP Europeens Network Coordination Centre (RIPE–NCC) and Asia Pacific Network Information Centre (APNIC)) organizations that are authorized by the Internet Corporation for Assigned Names and Numbers (ICANN) to administer numbering and addressing. Does the deployment of IPv6 create address allocation issues for any market segment? How will allocations to end users and end-user devices be affected by IPv6 deployment? Will small and mid-sized ISPs and IT firms have equitable access to the addresses they need? Are the existing national and international registries technically capable of handling administrative tasks required for IPv6 numbering and addressing? If not, identify the tasks and the costs for registries to be made capable of handling IPv6 related administrative tasks.

IV. Current Status of Domestic and International Deployment

A. Appropriate Metrics To Measure Deployment

Efforts to deploy IPv6 commercially are relatively recent phenomena. Notwithstanding the nascent nature of the IPv6 market, the task force seeks to develop an understanding of how the market is evolving across regions (both domestically and internationally) and among user groups (*e.g.*, government, industry, academia). What are the most appropriate metrics to gauge IPv6 deployment? Is the quantity of equipment purchased, the number of routers acquired, the number of addresses assigned, the number of hosts with IPv6 operating systems, the number of available applications that are IPv6 or IPv6/IPv4 compatible, or the amount of IPv6 traffic carried sufficient to properly define the IPv6 market? Are there other metrics or some combination of metrics best suited to characterize the domestic and international penetration of IPv6?

The task force is interested in an assessment of the total domestic and international deployment of IPv6. What is the known current volume of deployed native IPv6 and IPv4 network equipment (*e.g.*, hosts, routers, switches)? To what extent does the pace and extent of IPv6 deployment vary from country to country or region to region (*e.g.*, North America vs. Europe vs. Asia)? [14] How is that equipment deployed by market segment? What is the approximate domestic and global value of all deployed IPv4 and IPv6 equipment? What is the percentage (and proportion as compared to IPv4) of known IPv6 deployments by market segment?

B. Private Sector and Government Deployment Efforts

1. Overall Domestic Efforts

The task force seeks specific comment on the status of IPv6 deployment efforts in the United States. First, we seek comment on the availability of IPv6 products and services. Are technology suppliers producing the necessary hardware, software, applications, training, and any other products and services in sufficient quantity to meet the demand for IPv6 in the United States? We ask commenters to identify the relevant product and service categories and to describe the breadth and depth of offerings in those categories. For example, is the market for IPv6 routers characterized by multiple suppliers offering a variety of products, or does only a single supplier produce only a limited number of products? To the extent any relevant products and services are not available or are in limited supply, we seek information about their projected availability in the future, including analysts' estimates and suppliers' business plans.

Second, the task force seeks comment on the actual deployment of IPv6 products and services in the United States. To the extent possible, we ask commenters to provide specific information on the status of IPv6 deployment across product and service categories (*e.g.*, hardware, software) and across customer segments (*e.g.*, private sector, government, academia). For example, how many enterprise network routers are currently IPv6-capable? How many public or backbone network routers are IPv6-capable? How does U.S. router deployment compare with other countries? How many ISPs are currently capable of handling IPv6 traffic? What percentage of Internet access customers receive IPv6 capable services? What proportion of end-user equipment (*e.g.*, computers, wired and wireless end-user devices, cable modems, DSL modems, printers and other peripheral equipment, and other devices) is capable of handling IPv6 packets? To the extent that such capability is only provisioned in such devices, how easy/costly will it be for users to activate that capability? How many of the critical functions within an enterprise are IPv6 enabled (*e.g.*, DNS, wireless firewalls)?

Third, we seek comment on the projected growth of IPv6 products and services in the United States. We ask

[14] *See* Nokia's Chinese website for IPv6 which has compiled a list of IPv6 enabled applications. This information can be viewed at *http://www.ipv6.com.cn/technique/applications.html.*

commenters to provide all relevant assumptions and underlying data that support their growth projections. To the extent possible, we ask commenters to provide growth projections for specific products and services, as well as projections among customer segments.

2. Domestic Government Efforts

The task force seeks comment on federal, state, and local government efforts to deploy IPv6 in the United States. For example, the Department of Defense (DoD) has announced plans to migrate its existing Global Information Grid Network to IPv6 by 2008.[15] Additionally, DoD recently initiated a multivendor testbed, known as ''Moonv6,'' to examine the interoperability of IPv6 equipment, software, and services under real-world conditions. Involving more than 30 networking vendors, testing vendors, and service providers, the project purportedly will be the most substantial test of the IPv6 standard set in North America.[16] We seek comment on any lessons learned to date from DoD's efforts to deploy IPv6 that could be applied to federal civilian agencies, state and local governments, academia, and the private sector. We seek similar comment on other IPv6 research efforts and testbeds, including IPv6 deployments in federal research networks (Fednets),[17] the Abilene backbone network,[18] and any other similar efforts. We ask commenters to identify the costs of these efforts and the expected effects these activities may have on the deployment of IPv6 within the United States?

What is the current state of IPv6 deployment by other federal, state, and local government agencies? What factors have various agencies considered in deciding whether and at what pace to deploy IPv6? How do factors like geographic location, population density and/or available expertise impact the costs/benefits for state and local municipalities that are considering IPv6 deployments? How will the recent DoD requirement that all Global Information Grid assets be IPv6-capable by 2008 affect the procurement plans and decisions of other federal agencies? The task force encourages states and local governments to describe any initiatives or studies that they have undertaken regarding the deployment of IPv6. What is the current state of IPv6 deployment by state and local government agencies? What factors have various agencies considered in deciding whether and at what pace to deploy IPv6? How do factors like geographic location, population density and/or available expertise impact the costs/benefits for state and local municipalities that are considering IPv6 deployments?

3. International Efforts

In addition to domestic IPv6 deployments, the task force seeks comment on international efforts to deploy IPv6. For example, we understand that governments and companies in Asia have been aggressively promoting and adopting IPv6, purportedly because of the growing demand for public Internet addresses in their countries. Japan and Korea plan to have IPv6 fully deployed before the end of this decade.[19] The European Union has developed substantial IPv6 plans and programs to ensure readiness and competitiveness when IPv6 is widely deployed.[20] Additionally, we understand that other countries such as Tunisia are engaged in substantial IPv6 deployments.[21]

The task force requests comment on the current and projected levels of IPv6 deployment across the globe, on both a regional basis (*e.g.*, Europe, Asia, South America) and on a country specific basis, where available. To the extent possible, we ask commenters to provide such information by product category (*e.g.*, hardware, software) and by customer segment (*e.g.*, government, private sector, academia). We also ask commenters to explain how particular initiatives or programs by foreign governments or foreign suppliers have helped (or hindered) IPv6 deployment. For example, have government commitments to reach a specific level of IPv6 deployment by a date certain helped spur deployment? Are governments devoting significant funding for IPv6 deployment efforts? Have government initiatives (of lack thereof) interfered with normal market forces and what are the consequences of those actions or inactions?

V. Government's Role in IPv6 Deployment

The task force seeks to build a public record that addresses two fundamental questions: (1) Should government be involved in fostering or accelerating the deployment of IPv6; and (2) if so, what actions should government undertake? In answering these questions, we ask commenters to build upon their responses to the questions above and to provide specific, empirical evidence, where possible, to support their assertions regarding the proper role of government in IPv6 deployment.

A. Need for Government Involvement in IPv6 Deployment

1. Reliance on Market Forces

As a general matter, government policymakers in the United States prefer to rely on market forces for the large-scale deployment of new technologies. In most cases, reliance on the market tends to produce the most efficient allocation of resources, the greatest level of innovation, and the maximum amount of societal welfare. Accordingly, we seek comment on whether market forces alone will be sufficient to drive a reasonable and timely level of IPv6 deployment in the United States. For example, given commenters' views on the current and predicted rates of IPv6 deployment, do commenters believe those rates demonstrate a sufficient uptake of IPv6 in the United States? We ask commenters to identify the specific reasons for their positions.

2. Potential Market Impediments

Notwithstanding the government's general preference for relying on market forces, there may be impediments in a particular market that warrant corrective action by the government. In this section, the task force seeks comment on whether some of the more common forms of impediments are present in the market for IPv6 products and services.

a. Technological Interdependencies and the ''Chicken and Egg'' Problem

The task force requests comment on whether a ''chicken and egg'' problem exists that could hinder efficient

[15] *See* U.S. Department of Defense, ''Internet Protocol Version 6 (IPv6), *http://www.dod.gov/news/Jun2003/d20030609nii.pdf.*

[16] *See* the Moonv6 Media page at *http://www.iol.unh.edu/moonv6/* to view a presentation that gives more detail about this particular program.

[17] Fednets are networks operated by the National Science Foundation, the Department of Defense, the National Aeronautics and Space Administration, and the Department of Energy. The Fednets coordinate closely to support participating agency missions and R&D requirements. *See* National Science and Technology Council, *High Performance Computing and Communications Information Technology Frontiers for a New Millenium: A Report by the Subcommittee on Computing, Information, and Communications R&D* (2000), *http://www.ccic.gov/pubs/blue00.*

[18] The Abilene Network is an Internet2 high-performance backbone network that enables the development of advanced Internet applications and the deployment of leading-edge network services to Internet2 universities and research labs across the country. *See* abilene.internet2.edu/about/.

[19] *See, e.g.*, a 2002 presentation by Toshihiko Shimokawa entitled ''IPv6 status of Japan,'' which describes the development of IPv6 in Japan, including information on government and private sector activities. This presentation is available at *http://genkai.info/2002–1004/materials/toshi.ppt.* For information about Korea's plans with respect to IPv6, see Gene Kowprowski, ''Internet Protocol for the Future: Ipv6 Poised for Adoption,'' *TechNews World* (Jul. 30, 2003).

[20] *See, e.g., http://www.europa-web.de/europa/03euinf/39INFTEC/ecresult.htm.*

[21] *See http://www.ipv6net.tn/.*

deployment of IPv6 (*i.e.*, disincentives for investment in supporting infrastructure until applications are deployed, matched by disincentives for investment in applications until supporting infrastructure is in place). In the case of IPv6, firms may be reluctant to build IPv6 networks (or to install IPv6 capability in existing IPv4 networks), or to develop and market IPv6 devices, if there are no IPv6 applications that prompt consumer demand for the underlying transmission infrastructure. Similarly, Internet service providers may be reluctant to install IPv6 in the absence of sufficient IPv6 applications. Applications providers, on the other hand, may hold off until the infrastructure is in place to make those applications usable by consumers. We seek comment on whether such a ''chicken and egg'' relationship exists between IPv6 applications and supporting infrastructure, and if so, how that relationship is manifesting itself in the market for IPv6 products and services.

The ''chicken and egg'' problem seems to be most acute when the interrelated products are costly to develop and are highly interdependent (*i.e.*, the end product is a complex and capital intensive system). We seek comment on whether those characteristics are present for IPv6 infrastructure and applications. We also seek comment on how the expected degree of interoperability between IPv6 and IPv4 networks will affect this potential chicken and egg problem. Will the interoperability between IPv6 and IPv4 reduce potential impediments to the synchronized deployment of IPv6 infrastructure and applications, or will that interoperability merely serve to delay decisions to upgrade infrastructure and applications to IPv6? In some instances, government has responded to concerns over potential ''chicken and egg'' problems by playing an active role in the introduction of certain products and services, such as FM radio and HDTV. We request comment on how the deployment of IPv6 compares to other standards-based technology transitions and whether IPv6 presents the same or similar concerns that warrant government action.

b. Monopoly Power

The presence of a firm or group of firms, with monopoly power in the market for IPv6 products or services could create a potential impediment to the efficient deployment of IPv6 in the United States. Although we are not currently aware of any concerns regarding monopoly power, such a situation could arise from the existence of a dominant firm or group of firms in the relevant markets with the incentive to impede normal dissemination of IPv6, either by directly suppressing the technology or by setting excessive prices for IPv6 products and services. We therefore seek comment on whether any firm or firms have monopoly power for IPv6 products and services, and how the exercise of such monopoly power will affect IPv6 deployment in the United States.

To aid in this analysis, we seek comment on the extent to which IPv4 and IPv6 are direct substitutes. If IPv4 and IPv6 are direct substitutes (*e.g.*, if IPv6 equipment and applications compete directly with IPv4-based counterparts for market share), it may be unlikely that providers of IPv6 equipment, applications, and services will be able to charge excessive prices for their products (*i.e.*, prices that exceed any performance differential). Alternatively, if IPv6 builds on IPv4, enabling related but different applications, early entrants into the market may be able to establish sufficient market power to impede adequate competition. Economists, however, generally consider such temporary monopolies to be a normal phase of new technologies' evolution and thus such a pattern may represent an efficient deployment of a new technology and not a market failure. We request comment on these issues.

c. Network Externalities

The presence of network externalities or networking effects could also impede efficient deployment of IPv6.[22] The task force requests comment on whether and to what extent deployment of IPv6 is characterized by network externalities. If so, what is the magnitude of those externalities? In this regard, most observers believe that IPv6-based networks will be interoperable to a considerable degree with embedded IPv4 networks and, therefore, IPv6 users will be able to communicate with IPv4 users in many instances. To what extent does that affect the size or scope and timing of any network externalities associated with deployment of IPv6? Do network externalities arise, if at all, from all IPv6-based services and applications, or are they limited to specific offerings (*e.g.*, gaming services whose value to individual users likely depends on the number of potential opponents)? Given the early state of IPv6 deployment, is it premature to predicate a case for government intervention at this time on the possible existence of network externalities? How important are network externalities in the U.S. market for domestic firms who want to compete in global markets?

Network externalities increase uncertainty (and thereby deter efficient investment decisions) because the returns on a company's investment are dependent on the investment decisions of other companies.[23] In addition, if related applications, or applications and infrastructure are highly complementary, early entrants into a market that is not mature may not be able to realize returns on investment in an acceptable time frame. These factors increase market risk and impede the development and deployment of technologies. A lack of information and documentation regarding benefits and costs also increases market risk. The task force seeks comments on the importance of coordinating the timing of IPv6 migration for achieving efficient market penetration.

d. Other Impediments

In addition to the potential market impediments described above, we seek comment on any other potential market impediments that may hinder IPv6 deployment in the United States. To the extent possible, we ask commenters to provide specific, factual examples of any such impediments and to describe how those impediments are affecting IPv6 deployment.

3. Public Goods

An important role of government is to ensure the adequate provision of ''public goods,'' which market forces alone commonly cannot do.[24] Examples

[22] Network externalities arise from the fact that the value of a network to its users typically increases with the number of people that can access the network. Similarly, networking effects arise from the fact that the value of a network also increases with the number of individuals actually using the network. When a consumer decides whether to purchase and use a networked product or service (such as an IPv6-capable device), that person considers only the personal benefits of that purchase, and ignores the benefits conferred on all other users (*e.g.*, those users who may now have a new opponent in a IPv6-based gaming service). The individual may choose not to purchase the networked product or service, even though that purchase may have increased overall economic welfare. In consequence, deployment of the service (and the equipment and technologies that make that service possible) will be less than it ''should'' be. See Parkin, note 12 supra, at 504–510; Robert Willig, ''The Theory of Network Access Pricing'' in *Issues in Public Utility Regulation* 109 and n.2 (H. Trebbing ed. 1979).

[23] *See, e.g.*, Paul Stone, *The Economics of Technology Diffusion* (2002).

[24] Public goods are characterized by consumption nonrivalry, in that one person's consumption does not reduce the amount of the good available to others. More importantly, public goods are characterized by nonexcludability, in that no individual can be prevented from enjoying the

Continued

of public goods include national defense, law enforcement and clean air. Infrastructures, to varying degrees, also have the characteristics of public goods. Because standards are by definition used collectively by competing and partnering economic agents, they have infrastructure characteristics. In this section, the task force seeks comment on the public good characteristics of IPv6-capable products and services.

a. Security

In section II.B above, we seek comment on the potential security benefits of IPv6. To the extent that commenters believe IPv6 may directly or indirectly facilitate improved IP security, we seek comment on whether security benefits from IPv6 exist that can significantly further the delivery of public goods. For example, could the deployment of IPv6 advance important national security, national defense, and law enforcement interests, which are commonly understood to be public goods?[25] We understand that certain features of IPv6 (*e.g.*, expanded address space, auto-configuration) could enable the military to provide soldiers with equipment that could improve command and control capabilities in the field. Improved auto-configuration could also enable first responders to establish vital communications systems in the event of disaster or national emergency. Does the furtherance of those and any other security-related interests require government action to speed the deployment of IPv6 in the United States? In responding to theses questions, interested parties should explain the specific security interests to be furthered and how they would be advanced by wide scale deployment of IPv6.

The task force also seeks comment on whether the private sector may fail to sufficiently implement IPsec or other security mechanisms, and whether government action to accelerate the deployment of IPv6 could aid private sector security efforts. For example, what conditions could hinder private sector efforts to fashion key management systems and trust mechanisms needed to implement IPsec in an IPv6 environment? To what extent would federal government intervention be useful or necessary to overcome such obstructions?

b. National competitiveness

Given other nations' announced commitments to IPv6, is U.S. government action to support domestic IPv6 warranted and appropriate in order to preserve the competitiveness of U.S. businesses internationally? In this regard, we understand that U.S. firms are currently major providers of IP equipment, services, and applications. We also understand that many have developed or are developing IPv6 capabilities for their products and services. We further understand that some U.S. firms appear to be selling equipment in many of the countries (*e.g.*, Korea, Japan, China) that ostensibly are most committed to IPv6 deployment. Given these understandings, we seek comment on how the competitiveness of U.S. equipment firms and service providers would be adversely affected by slower deployment of IPv6 domestically?

We also understand that use of IPv6-capable networks and applications may increase the efficiency of users of IPv6 infrastructure, potentially allowing them to produce and market their goods and services at lower cost or with higher quality—both domestically and in international markets. Thus, lagging deployment of IPv6 in the United States (with consequent loss of economies of scale and scope) could conceivably reduce the competitiveness of American firms in various export markets vis-à-vis companies from countries that have deployed IPv6 more aggressively. We request comment on this supposition and, particularly, on the nature and magnitude of the cost advantages that use of IPv6 (as opposed to IPv4) may confer on a company in a global market context.

B. Nature of Government Action

In light of commenters' answers provided to the preceding questions, we now seek comment on the type of action or actions, if any, that the government should take regarding IPv6 deployment. Traditional government support for new technologies and technology infrastructures have included R&D support, incentives for investment in equipment, government procurement, and facilitation roles with respect to standards development and deployment. We emphasize that the list of government actions discussed below is not exhaustive, nor are such actions mutually exclusive. We therefore request that commenters provide specific details for any course(s) of action they propose, together with the estimated costs of such action(s).

1. No Government Action

To the extent commenters believe the aforementioned trends and potential market conditions suggest a timely deployment of IPv6 in the U.S., one possible U.S. government action would be to let market forces guide the diffusion of IPv6 into existing and future markets. The task force requests comment on the appropriateness of this non-intervention approach. Commenters should address the potential costs to the U.S. economy if government inaction results in a domestic implementation of IPv6 that lags other industrialized nations.

2. Options for Government Action

We discuss below specific actions that government could take to further deployment of IPv6. As noted above, the approaches discussed are not exhaustive, however, and interested parties are encouraged to identify and outline other potential avenues for government action. If the federal government should elect to spur deployment of IPv6 within the U.S. economy, we also request comments regarding how, when and in what form such action should take. What factors and market information should government consider in order to determine that the market-driven rate of IPv6 deployment in the U.S. is insufficient, thereby necessitating government intervention? Should government intervene early to stimulate deployment? Should it allow the market to drive deployment forward, and concentrate government efforts on assisting or encouraging those individuals and enterprises that are the slowest to adopt IPv6? To what extent, if at all, should the timing of government intervention differ with respect to private sector deployment of IPv6, as compared to its adoption by federal, state and local government?

a. Government as Information Resource

Rather than actively promoting deployment of IPv6, the government could establish programs to assist public and private sector entities in making their deployment decisions. It could, for example, create an information clearinghouse that gathers and disseminates IPv6-related information among government agencies and interested private sector firms. Such information could include data concerning the potential benefits and costs of deploying IPv6, the purchasing decisions made by other public and private actors, and guidelines to aid

---

benefits provided by a public good. Nonexcludability creates the problem of "free riders," who can enjoy the benefits of a public good without paying the costs of providing it. Moreover, the producer's inability to exact payment from free riders may prevent the producer from fully recovering costs. For these reasons, market forces alone tend to "under produce" public goods. *See* Parkin, note 12 *supra*, at 499–503.

[25] *See* Joseph Stiglitz, *Economics of the Public Sector* (1988).

interested parties in making IPv6 procurement decisions. What would be the costs and benefits of such an approach? What would be the essential elements of an effective clearinghouse program?

b. Government as Consumer

We seek comment on whether the government should use its position as a large consumer of information technology products to help spur IPv6 deployment. For example, working through its procurement process, should the federal government purchase only IPv6-compatible products and services? Should state and local governments adopt similar procurement policies? What would be the cost to the government of adopting IPv6 procurement policies compared to not adopting such policies? Could the government's adoption of IPv6 procurement policies have any unintended, adverse effects on the market for IPv6 products and services? If so, please define and assess the likelihood and magnitude of such effects.

To the extent commenters support government IPv6 procurement policies, we seek specific comment on how they should be implemented. For example, when should such policies become effective? Should such policies apply to all government entities, or are there specific classes of agencies that should adopt these policies before others? How should government fund any additional costs (if any) associated with the adoption of IPv6 procurement policies?

c. Government Support for Research and Development

As discussed above, testbeds and experiments by the Fednets and Abilene [26] have provided early working experience relating to the deployment and use of IPv6. Those activities have also helped to train a corps of IPv6 technicians that could be available to facilitate private sector deployment of IPv6. Furthermore, the Internet2 program has established an IPv6 Working Group that interacts with users, university networks, and Fednets to explain IPv6 deployment and transition issues and to provide hands-on experience to those entities concerning implementation, maintenance, and use of IPv6. In light of these activities, we seek comment on whether the government should provide additional support for IPv6 research and development. Are current research and development efforts sufficient? Does the government possess research and development tools or resources for IPv6 that are not readily available to the private sector? If the government does provide research and development assistance, what form should it take (*e.g.*, use of government facilities, tax incentives, matching grants, direct funding)?

d. Government Funding of IPv6 Deployment

Aside from research and development projects, we also seek comment on whether the federal government should attempt to spur the growth of IPv6 networks, applications, and services through direct funding of IPv6-related activities. For example, the government could provide direct assistance to entities desiring to purchase IPv6-capable equipment, whether in the form of tax incentives, matching grants, or direct funding. The task force seeks comments on the need, feasibility and wisdom of these approaches. How should such programs be structured and how much would they cost? Could existing policies and programs be used to provide such funding, or would new legislative authorization be required? Where the federal government provides funding to state and local governments for emergency communications equipment and networks, should the federal government require state and local agencies to purchase IPv6-capable equipment to ensure interoperability among equipment and networks in neighboring communities?

e. Government IPv6 Mandates

Although imposing government mandates on the private sector to deploy IPv6 is perhaps the least preferred role for government, the task force nonetheless seeks comment on this option to ensure that we develop a complete record. Specifically, we seek comment on whether the government should require suppliers of IP products and services to provide those products and services in an IPv6-compatible version by a date certain. To the extent commenters support such an approach, we ask them to explain the specific authority under which such a mandate could be imposed (legislative or administrative), the timeline under which the mandate would operate, and the benefits and costs of imposing such a mandate.

Dated: January 14, 2004.

Arden L. Bement, Jr.,

Director, National Institute of Standards and Technology.

Michael D. Gallagher,

Acting Assistant Secretary for Communications and Information, National Telecommunications and Information Administration.

[FR Doc. 04–1154 Filed 1–20–04; 8:45 am]

BILLING CODE 3510–60–P

[26] *See* Section IV.B.2 *supra.*

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 010604A]

Taking Marine Mammals Incidental to Specified Activities; Port of Miami Construction Project (Phase II)

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of receipt of application and proposed authorization for an incidental take authorization; request for comments.

SUMMARY: NMFS has received a request from the U.S. Army Corps of Engineers-Jacksonville District (Corps) for renewal of a one-year Incidental Harassment Authorization (IHA) to take marine mammals, by harassment, incidental to deepening the Dodge-Lummus Island Turning Basin in Miami, FL (Turning Basin) and an application for the promulgation of regulations governing the incidental take of marine mammals for the same activity over a 5–year period. Under the Marine Mammal Protection Act (MMPA), NMFS is requesting comments on its proposal to reissue a 1–year IHA to the Corps to incidentally take, by harassment, bottlenose dolphins (*Tursiops truncatus*) as a result of conducting this activity and the Corps' application for regulations.

DATES: Comments and information must be received no later than February 20, 2004.

ADDRESSES: Comments on the application should be addressed to Michael Payne, Chief, Marine Mammal Conservation Division, Office of Protected Resources, NMFS, 1315 East-West Highway, Silver Spring, MD 20910–3225. Comments cannot be accepted if submitted via e-mail or the Internet. A copy of the application may be obtained by writing to this address or by telephoning the contact listed here. Publications referenced in this