Before the
National Institute of Standards and Technology
National Telecommunications and Information Administration
DEPARTMENT OF COMMERCE

Comments on Deployment of Internet Protocol, Version 6
Docket No. 040107006-4006-01

Comments of VeriSign, Inc.

Mountain View, California

I. Introduction and Summary of VeriSign's Comment

VeriSign, Inc. (Nasdaq: VRSN), is pleased to provide its response to the above-captioned Notice of Inquiry: *Request for Comments on Deployment of Internet Protocol, Version 6*, as published in the Federal Register by NIST and NTIA on 21 January, 2004.

As a leading provider of Internet infrastructure services, VeriSign has a unique perspective from which our views on IPv6 are derived.

At the core, VeriSign believes the importance of the Department's inquiry is its potential to provide a basis for urgent attention to the Internet's protocol/standards process. Ten years have lapsed between the promulgation of the IPv6 protocol by the Internet's technical standards community, and the arrival of this moment at which the policy community has finally determined that it is appropriate to intervene into market processes, to assure that claimed benefits inherent in broad deployment of IPv6 can be achieved without further delay.

VeriSign believes that IPv6 should continue to be the subject of rapid deployment by all elements of the Internet community (NOI § IV B 1). But, our rationale for this prompt deployment is not grounded particularly in the often-claimed security benefits for the public Internet, which VeriSign believes are no longer uniquely compelling, or even the additional address space available in an IPv6 environment. Indeed, great care is required as IPv6 deployment goes forward, because paradoxical results, including, security impairment, are likely without significant controls and attention to the overall Internet technology environment. Deployment of IPv6 at this time is in VeriSign's view necessary, rather, to encourage the rapid completion of deployment of other essential public Internet infrastructure elements, to permit full realization of IPv6's benefits to private network operators, and to provide a homogeneous uniform platform on which to build the NEXT, post-IPv6 generation of Internet protocol advances.

The world and its utilization of the Internet are dramatically different than they were in 1995. The Internet has become recognized and enabled as an essential element of much of the planet's economic, social and governmental activity in the intervening years. To maintain that global utility, the process by which essential Internet technical

innovations are developed, vetted and deployed by the entire Internet community, promptly and pervasively must be similarly recognized and enabled by its infrastructure, governments and users.

VeriSign urges NTIA/NIST, without delay, to convene an interdisciplinary and international process, to collaborate with the Internet infrastructure, technology, user and standards communities to evaluate the present security environments as we transit to a more pervasive IPv6 deployment, to assess the changed, present and emerging threats to the public Internet and to make recommendations regarding security features and practices which should be developed, incorporated into the RFC/standards environment, and deployed pervasively, within the next 12 to 18 months. "IPvX" can not be allowed to consume the same amount of time from description to deployment as has IPv6.

Numerous elements of the IPv6 specification have in fact been overtaken by events in the intervening years. Specifically, claimed security benefits (NOI, § II B) have been in some regard been either mooted by the wide deployment of IPSec in IPv4 environments or been made irrelevant by the dramatic change in the nature of attacks and other security threats to the Internet, for which IPSec-based solutions are either unhelpful or, in some instances counter-productive.

Similarly, while a second major benefit of IPv6 deployment will be the availability of an almost inexhaustible supply of Internet addresses (NOI, § II A; III B 3), recent experience with telephone numbering schemes has taught that even "inexhaustible" inventories of technology addresses may be consumed more rapidly than expected, especially if allocation schemes do not prevent the warehousing of large address blocks, or other inefficient practices. While the mathematics of IPv6 numbering do not suggest this as a likelihood, few would have predicted that country code 1 area codes would be consumed (warehoused) at the rate they were during the wave of new area code introductions in the 1980s and 90s. VeriSign believes that achievement of IPv6's address space benefit will require not only uniform, pervasive deployment of IPv6-enabled tools and network elements, but an agreement among regional address authorities to utilize address allocation scheme(s) that incorporates both discipline and flexibility in a manner that reduces incentives to corporate users to "freeze" significant unused blocks of addresses or otherwise remove large blocks from available inventory.

II. VeriSign's Perspective on the Internet

VeriSign, Inc. is a leading provider of critical infrastructure services for the Internet and telecommunication networks. Since 1993, VeriSign, and its predecessor, Network Solutions, has been an essential provider of Internet infrastructure services. VeriSign was the first "registrar" of Internet domain names in the .com, .net and .org top level domains, and continues to operate the .com and .net registries under a cooperative agreement with the Department of Commerce and related contracts with the Internet Corporation for Assigned Names and Numbers (ICANN).[1] In addition, VeriSign operates two of the Internet's root servers, the A- and J- roots. As a consequence of these relationships, VeriSign has unique responsibilities, both explicitly detailed in the various contractual instruments, and implicit, as a result of our acceptance of the obligation of stewardship to the global Internet community. Our views on the deployment of IPv6 are thus necessarily colored by these roles and responsibilities.

Also, to support these infrastructure roles, VeriSign maintains facilities around the world, including a growing array (currently13) of top level domain server constellations to place DNS resolution capacity close to high concentrations of Internet traffic, and showcased by two operations centers in our California corporate headquarters and in Northern Virginia. Each contain physical infrastructure (servers, storage and related hardware) valued in the hundreds of millions of dollars.

VeriSign's substantial stewardship responsibility most importantly includes the provision of Internet service in a manner that supports the stabile, reliable availability to a user population today exceeding 1 billion globally. Each day, VeriSign's server constellations for .com/.net resolve more than 10 billion domain name requests, a level of traffic that is doubling every 18 months.

Figure A, below, depicts the location of the global constellation of .com/.net TLD servers under VeriSign's stewardship at the end of 2003.

[1] Cooperative Agreement NCR 92-18742, between the Department of Commerce and VeriSign, Inc., as amended 3 July, 2003.

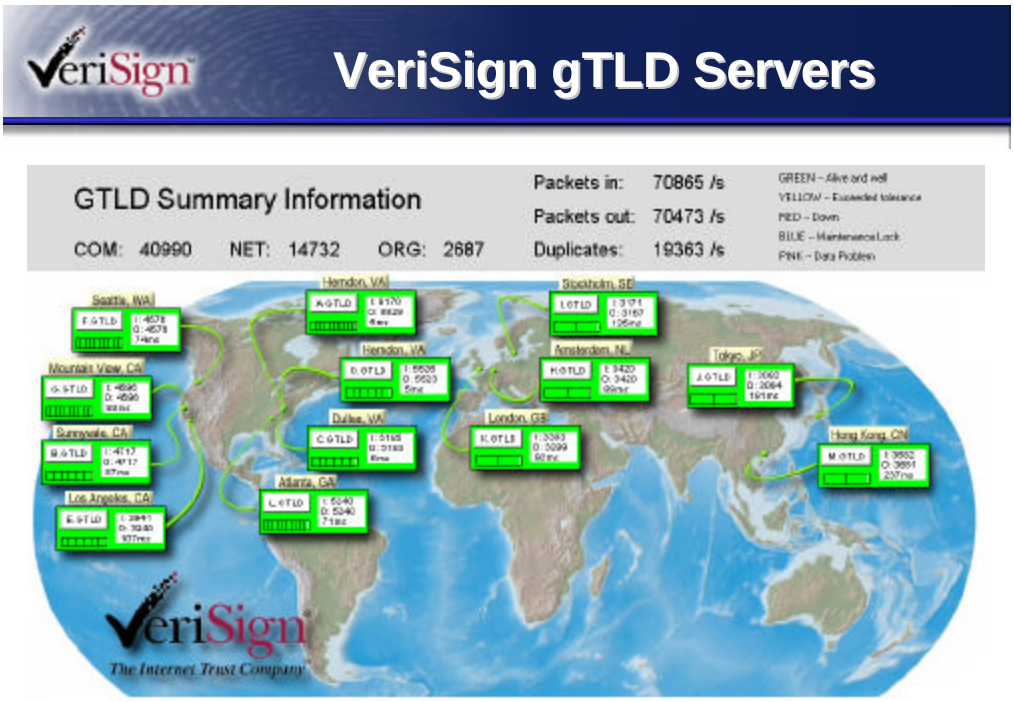

Figure A: LOCATION OF COM/NET SERVERS AS OF 12/2003

Accordingly, VeriSign has not only a unique perspective of the normal operations of the Internet and its naming and addressing functions, but a unique role in observing and responding to anomalous behavior on the network.

VeriSign is a participant in a range of Internet institutional activities, including standards bodies[2] and network monitoring activities[3] that place us in the midst of discussions about the present functional state of the Internet and its future availability and security. VeriSign's chief executive is one of the 30 members of the President's National Security Telecommunications Advisory Committee (NSTAC), and we also participate in the FCC-sponsored Network Reliability and Interoperability Council (NRIC), as well as numerous other Federal advisory committees dealing addressing Internet policy.

Frequently, when disruptions occur to the network, VeriSign's 24 hour watch centers are the first entity to observe an attack, hack, virus or outage, the first to respond, and the first to notify both other Internet infrastructure operators and the relevant agencies of government and the Internet community.

---

[2] e.g., IAB, IETF, IEEE, ANSI, ETSI, and ITU-t.

[3] e.g., IT/ISAC; CMU CERT, new U.S.CERT;

As will be developed further in this submission, these roles give VeriSign not insubstantial standing in the discussion of options and scenarios for the further deployment of IPv6 and the technical evolution of the Internet generally. While these views on IPv6 are not necessarily exclusive to us, nor delivered with any sense of special authority *ex cathedra*, derived from our unique role in serving the Internet, we do believe them to be informed by substantial experience, expertise and demonstrated commitment to responsible operation of the Internet for the benefit of the global user community, and VeriSign trusts they will be received in that spirit.

VeriSign professional technical staff have been closely linked to the evolution of IPv6 through their participation in the Internet's voluntary technical standards process, and as a result of VeriSign's participation in a range of industry initiatives.

For example, the sponsoring organization of the Internet's M- root in Tokyo, WIDE, has been hosting an IPv6 test bed since 1995, in which VeriSign has participated.[4]

VeriSign has routinely acquired IPv6 ready technology as it has become available on the market, and has experimented extensively in our laboratories to determine the operational characteristics of various network hardware and software elements in an IPv6 environment. Accordingly, our comments are illuminated not simply by dialogue or speculation, but by hands on experience in observing these elements in a deployed environment.

III Responses to Specific Issues in the Request for Comment

VeriSign will not address each issue raised in the NOI. Indeed, many of the issues posed as questions in the NOI are better analyzed and more thoughtfully addressed in the questions as framed than they have been elsewhere in much of the increasingly emotional and apocrypha-laden debate over IPv6.

Reform of the Internet Standards Process

VeriSign's position is that one of the—if not the singular—contribution of this proceeding may be to encourage a process of consensus that is inclusive and diminishes if not eliminates the potential that the next statements of technical specification (whether expressed as "RFC", "standards", or "best practices") that are broadly endorsed as being appropriate for deployment on the public Internet do not languish for a decade before serious efforts are made to assure their deployment. Said more concisely, we hope to avoid repeating the same mistake twice.

It is our belief that the process between initial drafts of "IP next gen" in the early 1990s and the present proceeding are ample evidence of the unfortunate result of such a

[4] WIDE Project: http://www.wide.ad.jp/wg/finish/014_ipv6.html

prolonged period. As we will set out in our responses, much of what is problematic about IPv6 at this moment is a result not of any inherent technological flaw, but rather, the simple passage of time. A significant number of the benefits claimed for IPv6 upon its initial publication have become mooted by intervening changes in technology, obsolesced by evolution in the mode of Internet infrastructure deployment and practice, or simply "overtaken by events" as a result of changes in the Internet environment, requiring updating, modification, or simply a new or different approach to an issue.

As a philosophical matter, one might speculate as to the extent of the next generation IP protocol's "obsolescence" potential. Would deployment of a new protocol in a one or two year—as opposed to ten year—deployment time frame (given Moore's law, the rate of technology advance and the rate of growth in the Internet user population) suffer less from obsolescence than has IPv6 ? Perhaps not.

Our concern about the process that has brought us IPv6, and brought us to this juncture in its deployment is NOT meant as a criticism of the protocol itself. Nor do we suggest that IPv6 NOT be fully deployed.

Rather, as we cite specific concerns with its benefits for address space enlargement and security, we wish to encourage an assessment that places as much or more emphasis on the process of protocol development and deployment as it does on the substance of the presently available tools embodied in IPv6 and related network elements.

And, more important, we hope to encourage a process that will embark from the present reality of uneven present IPv6 deployment, and a likely lengthy period of migration to "full" (or, at least, "general" IPv6 deployment) with the expectation that the future technical environment can not be rolled out in discrete "batches" as if the technology were a commodity. Rather, we believe we must evolve to an era where deployment of network improvements is a continuous process, subscribed to by all participants in the Internet's infrastructure, the collateral vendor communities of end-user service provision, large private and governmental networks, application and hardware vendors and individual users.

While the analogy to the highway system may be strained, some portions may also be illustrative of important basic hygiene necessary for the Internet. Our interstate highways have minimum speed limits; vehicles incapable of operating at those minimums are not permitted on the system. Vehicle safety inspections assure that basic operating necessities (brakes, lights, wipers, minimum tire tread) are present. Sub-system operators (i.e.—the states) who fail to uphold system-wide operating standards (speed limits) are excluded from economic support.

A great hue-and-cry has developed both domestically and globally about the digital divide, and the failure of Internet-source countries and industries to take measures to assure the full availability of the network's benefits at every economic level in every country. In large measure, this criticism is well deserved; recognizing that, VeriSign and other technology vendors have taken steps to begin to respond to the concerns of lesser

developed countries, and access-deprived communities in our own country, to remedy that lack of full participation in the Internet age.

But an essential pre-requisite to any "bridging" of that divide is the presence of basic technology infrastructure to support network presence. This includes collateral infrastructure of electric power, network connectivity (wire, radio, satellite), a trained population of network managers and user support, the presence of access appliances—computers and other network devices—at the user level. And, while the chauvinists among us might suggest that, compared to the "nothing" that these communities posses now, even ancient 286 computers with dial-up modems would be a dramatic improvement, recent history—as with the deployment of cellular telephony in Eastern Europe after 1989—teaches us that both appetite and practicality dictate deploying the state-of-the-art as the Internet is brought to previously unserved communities.

Since that model of state-of-the-art deployment is likely to characterize the portion of new Internet users in the coming several years, there is little to bind them to a legacy of even IPv6 deployment, let alone IPv4. As new nodes on the network, they may freely deploy IPv6—or whatever the state of the art is at the moment the Internet is installed. More to the point, these communities, representing hundreds of millions of new users, dwarfing the North American Internet community in a very few years, --these new nodes --will have no reason NOT to demand not only IPv6 as their IP protocol baseline, but to insist on a process of continuous improvement in the condition of their own connectivity to the network, as well as that of all those with whom they seek to communicate.

It is therefore against this backdrop of dramatic growth in Internet users over the next several years that VeriSign suggests the critical importance of evolving the technical standards process in a manner capable of responding to such an enormous global environment.

Indeed, the very phenomena that characterize today's Internet environment-- expanding scale, accelerating deployment and exponential increases in the sophistication and pace of attacks--suggests that the legacy technical standards process that supports the Internet is incapable of being utilized "in vivo". The standards process and its endorsement of useful innovation must be overhauled if it is to be relevant and support the Internet of the future with tools that assure the network's simultaneous reliability, stability, availability, security and capacity for growth.

IPv6 Name Space Expansion and Allocation Issues

In both the discussion of the advantages in expanded name-space and the security benefits inherent in IPv6, we will treat the claimed benefits of both as if proven. VeriSign does not believe that the voluntary, industry-led, market driven standards process which produced IPv6 can be maintained as a credible artifact of the modern technological landscape if its work-product is subjected to post-hoc technical re-argument. The consensus of a broad array of technically skilled individuals produced IPv6; we do not believe it is necessary or appropriate to the instant proceeding to revisit the merits of their conclusions.

However, having said that, it is unquestioned that, because of the enormous lapse in time since the promulgation of IPv6 in 1995 and the instant proceeding, intervening events have introduced considerations, conditions and facts that did not exist ten years ago, and which may well be germane to the issue of the propriety of the IPv6 protocol, as specified, being deployed as contemplated in 1995.

In both the name space area and the security area, this is true.

In name space, as the NOI clearly describes, the much-feared exhaustion of available IPv4 addresses resulted in the utilization of both technical strategies (e.g.-NATing) and conservation measures (e.g.-CIDR) which dramatically slowed the rate of exhaustion of addresses. From the perspective of address space, these measures have provided some extension of the useful life of IPv4. Since present analysts disagree precisely on the length of that extended life, and, more importantly, events stimulating further exhaustion, such as the addition and expansion of top level domains continue, it seems futile to speculate on precisely when IPv4 address exhaustion might be approached.

Rather, VeriSign believes that the issue of importance in the address space area is assuring that allocation processes for IPv6 addresses are put in place by the regional address authorities that assure that artificial exhaustion will not be approached through allocation schemes that permit the warehousing of enormous numbering blocks without actually use.

The concern, even in the face of the astral-scale volumes of addresses enabled by IPv6, is not without precedent. One need only examine the recent history of U.S. area codes and their distribution in blocks of 10,000 numbers to appreciate the consequences of commercial "acquisitiveness"; when an entity "freezes" (indeed, is permitted by the allocation authority to freeze) 10,000 numbers in order to be assured of access to 900 of them, the rate of exhaustion is much greater than necessary. It might require only a few hundred thousand large entities in a region each receiving blocks of hundreds of billions of addresses (representing household electric outlets or vending machine container slots) to begin to consume address space at rates not contemplated by IPv6 draftsmen.

IPv6 Security Issues

Given VeriSign's role n the Internet's infrastructure, and the extent to which our function and professional staff's expertise have become viewed as a critical link in the Internet's security armor, we wish to be as unambiguous as possible in our discussion of IPv6 and security.

VeriSign believes the security objective implicit in the "broad deployment of IPv6" is essential to the future of the Internet. We also believe, unfortunately, that the objective of a truly secure Internet can not now be achieved by the simple broad deployment of IPv6. The goal now requires a much more complex process, supported by commitments from all key Internet user institutions to an unprecedented process of collaborative investigation and research.

At the time of its publication in 1995, the IPv6 protocol incorporated security features in the IPSec "module" that constituted significant positive improvements over then available native IPv4 security features. Had IPv6 been pervasively and persistently deployed in 1995, the benefits of its security features might well have altered the evolution of the network, and produced—from a security perspective-a different canvass against which this discussion is being painted.

But the reality is different. IPSec has been "liberated" from IPv6, and widely deployed in IPv4 environments. Nothing in IPv6's specification compels the utilization of IPSec features where they are present. Accordingly, the present environment is one which must be described, from a security perspective, as heterogeneous.

Thus the questions posed in the NOI (III, B) must be analyzed both from the capability end of the telescope, as well as the threat end of the telescope.

From the capability perspective, this security heterogeneity is risky. It makes deployment of some other IPv6-and-beyond features more difficult and more costly. It is indeed true that other critical IPv6 deployment issues related to resolution protocols and other key infrastructure elements are made more complex by this heterogeneity, even if they are technically "independent." Moreover, these risks and costs may be more evident in IPv6-capable network deployments in private enterprise environments than on the public Internet.

Indeed, an argument can be made that the essential locus of IPv6/IPSec deployment on the public Internet is at the point of greatest interface between users and the network—the ISPs. Were large ISPs that account for the largest number of Internet users to simultaneously deploy IPSec, or IPSec-enabled IPv6, one would expect that the number of potential "risk points" susceptible to an array of attack methodologies currently plaguing the Internet would go down significantly. Stated in IPv6 terms, the greater the deployment of the most advanced security features available, the less vulnerable the network SHOULD be.

This analysis must, however, now be flipped to the risk/threat end of the telescope. It is clear, as you are no doubt being frequently reminded in this proceeding, that 2004 is not 1995; that threats to the Internet have altered dramatically in their design, objective, technical method, and propagation speed. Risks for which IPSec was intended may no longer be substantial threats. A body of opinion exists that indeed, pervasive deployment of IPv6 on the public Internet without further attention to important security features would impose significant new security risks and degradation of network security posture, even though a much larger number of user nodes was nominally "upgraded" to IPv6.

Once this paradoxical potential for security degradation is understood, it is possible to cast the IPv6 debate more in terms of an "environment" than of a "technology." And indeed, as with biological ecosystems, the futility of attempting to predict discrete outcomes in the face of diverse, dynamic systems becomes apparent. Not only may assertions about the impact of deployment of one element of the IPv6 specification prove to be incorrect, but a

cascading array of consequences in the dynamic Internet environment may produce unintended harmful or paradoxical results requiring significant investments to cure.

Rather than fixate on the possible results from discrete IPv6 or IPSec deployment strategies, VeriSign believes the persistent threats to the public Internet demand a "leap-frog" strategy, which looks beyond the present uneven "heterogeneous" security environment, and accepts and attempts to anticipate the continuing growth in sophistication and aggressiveness of attacks to the Internet. Combining the global resources of the Internet technology community to assess the present security posture of the public Internet, evaluate the nature of present and emerging threats, and, as with IPv6, develop a set of tools and specifications capable of meeting these threats in a one-to-two year time horizon, would, if coupled with a broad based commitment to deployment by all key network elements (including large ISPs) stands, in VeriSign's view as the most promising strategy for moving beyond the IPv4-IPSec security environment and assuring a less risky Internet future.

Discrete elements of new initiatives directed towards network security assessment, risk assessment, and attack forensics exist across the Internet community. Collaborations encouraged by the National Strategy to Secure Cyberspace have begun in industry, government, and in cooperative environments between them. The traditional Internet technical community—especially the standards community—has been relatively silent since the 9-11 attacks in this regard, content to continue arguing for rapid resolution of efforts to finish secure BGP, authenticated BIND v. 9, and wide deployment of IPv6. VeriSign is of the opinion that these efforts, at this juncture miss the point. The expertise and energy reposing in these organizations must be turned collectively, and with coherent management of their common objective, towards the creation of a secure, stabile Internet capable of growing past 1 billion users in the next several years.

###