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 The Internet Security Alliance
Arlington, Virginia

The Internet Security Alliance 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 trade association focused on improved cyber security and representing more than 50 corporate members serving various sectors of the economy on four continents, we believe we have a unique perspective to address the security aspects of this inquiry.

The Internet Security Alliance (ISAlliance) understands the desire, and in many cases, the need to deploy IPV6 protocol as a replacement for the current implementation of Internet Protocol (IPV4) from a network addressability perspective and for the merits that the expanded network feature set provides to the implementer.

IPv6 would be deployed to co-exist with and ultimately replace a set of IPv4 systems and protocols ***that have 20+ years of implementation and deployment experience***. The IS Alliance has concerns regarding the motivation for the deployment of IPv6 from the perspective of network security as outlined in the 3 broad areas below:

- Many security vulnerabilities result from software implementation errors and network configuration errors that continual inspection, due to real, everyday experience in production networks, has largely served to eliminate from the IPv4 code base. That said, after 20 years of IPv4, many implementation errors are found every year. The IPv6 code base will initially not have benefited from this vast degree of close scrutiny and consequently it is likely that the introduction of IPv6 will manifest many more security vulnerabilities during the early phases of production deployment than are currently seen with IPv4.

    - Industry, with assistance from the established security monitoring and alerting services, can and must use the systems

established during the development of IPv4 to expedite the security hardening of IPv6 implementations.

- The experience and perspectives gained from running IPv4 networks will certainly help to bring the security of IPv6 networks up to the levels of current IPv4 networks more rapidly, but during the transition a number of novel network solutions are likely to be required. Networks running IPv4 and IPv6 in parallel and using relatively untried transition mechanism may well suffer from additional unanticipated security vulnerabilities during the initial transition period.

    - Again the overall effect of such vulnerabilities can be minimized by rapid identification and promulgation of revised best practices by the industry assisted by government agencies that are running pilot programs.

- Many of the security weaknesses of IPv4 are inherited by IPv6, at least partially because of the desire to ease the learning curve for network operators during the transition and the desire to reuse the tried and tested tools of IPv4 to the greatest extent possible. Examples are insecure routing protocols, firewall implementations etc. Consequently there are areas of IPv6 where more secure solutions might theoretically be implemented but have not been. In many instances security will not necessarily be any better than is achieved by IPv4, at least during initial deployment.

    - There are areas where ultimately IPv6 has the capacity to improve on v4, and there are components that have been taken over from IPv4 that should be enhanced in the new more flexible environment that is offered by the IPv6 architecture.

    - The ISAlliance believes that the experience, expertise and systems put in place to build up the security of IPv4 can be applied to ameliorate the initial shortcomings of IPv6 implementations.

It is of major concern to the ISAlliance membership that organizations considering the deployment of IPV6 understand, very clearly, that implementations of IPV6 are not necessarily more secure than IPv4 despite the addition of IPSec capabilities to the protocol as a standard feature set. We believe that the deployment of IPv6 alongside IPv4 will throw up additional issues in security that have not been experienced in the single protocol environment of existing IPv4 networks. It is very important that all parties work together to deliver solutions and improved practices to overcome these problems.