Before the
Department of Commerce
National Institute of Standards and Technology
National Telecommunications and Information Administration
Washington, DC

Docket No. 040107006-4006-01

Request for Comments on Deployment of Internet Protocol, Version 6

COMMENTS OF
The Electronic Privacy Information Center

March 8, 2004

Pursuant to the Notice of Inquiry[1] published January 21, 2004 regarding the Request for Comments on Deployment of Internet Protocol, Version 6, the Electronic Privacy Information Center submits the following comments urging the Department of Commerce to shape IPv6 policy to promote security, privacy, and stability in emerging communication services.

The predecessor to IPv6, IPv4, formed the foundation for the Internet as we know it today.[2] However, weaknesses in security have allowed identity theft, third party surveillance, online fraud, and hacking, to become significant threats to Internet users. As the reach of the Internet extends with the capabilities of IPv6, further growth of the online community requires strong safeguards for the privacy and safety of persons online. Such privacy protection can safeguard people online by reducing these threats, and shield people from online exploitation.

As the replacement network protocol to IPv4, IPv6 provides an important communications framework for the next generation of network applications. IPv6 will extend the reach of the Internet into new areas and uses in the daily life of consumers; IPv6 has the flexibility to support mobile personal devices in wireless environments to high performance networking devices.[3] In light of the future growth of IPv6 networks, it is absolutely vital that IPv6 incorporate strong privacy protections for end users; these protections will lay a foundation of privacy and security services for use by end user applications.

Commitment to Privacy from the IPv6 Community

---

[1] Request for Comments on Deployment of Internet Protocol, Version 6, 69 Fed. Reg. 13, 2890 (Jan. 21, 2004).
[2] *See generally,* IETF, RFC 791, "Internet Protocol: DARPA Internet Protocol Program Specification"; IAB, RFC 2101, "IPv4 Address Behaviour Today".
[3] *See generally,* IETF IPsec Working Group (http://www.ietf.org/html.charters/ipsec-charter.html).

There is already a long-standing commitment within the IPv6 community to promote security and privacy. Historically, the Internet Engineering Task Force ("IETF") has attempted to increase the reliability, security, and privacy of computer networks. The Internet Advisory Board and Internet Engineering Steering Group Statement on Cryptographic Technology and the Internet called for the availability and development of stronger tools to protect security and privacy of network users and rejected limitations on computer security based on country requirements for interception.[4] From early in the IPv6 standard development process, the IETF has required support for Internet Protocol Security Architecture ("IPsec"), which provides services such as security, integrity, and confidentiality.[5] Further, as threats to privacy have been identified, IETF has taken steps to address the privacy vulnerabilities through technical privacy protection.[6] The European Commission IPv6 Task Force to the Data Protection Working Group has recognized IPv6 as a "potentially powerful tool to improve the possibilities of user privacy."

A key feature of IPv6 is IPsec, which provides security, integrity, and confidentiality services at the network, and further includes other features to facilitate the practical, efficient deployment of security technology.[7] While IPsec may be used over an IPv4 network, the IPv6 standard requires IPsec capability.[8] IPsec features protect the data flowing over an IPv6 network from interception and surveillance.[9] Because IPsec provides security at the network layer, end user applications are able to, and should, augment the services of IPsec with their own security to ensure robust privacy protection. These IPsec privacy features, if properly used and complimented by security architecture in end user programs, offer significant advantages over non-IPsec implementations of IPv4.[10] The DOC should strongly encourage the use of the IPsec features by end programs, and ensure that government networks and applications fully utilize the features of IPsec.

The importance of privacy to the IPv6 community is seen through the affirmative actions by the community to eliminate threats to privacy. As an example, early IPv6 implementations used an addressing scheme that threatened user privacy and online anonymity by tying a user's IPv6 address to the embedded network hardware access address.[11] This mechanism would have the effect of creating an unchangeable, unique identifier that could be used to correlate "seemingly unrelated activity" and allow a system and user to be traced across multiple unrelated

---

[4] RFC 1984, "IAB and IESG Statement on Cryptographic Technology and the Internet."

[5] For example, a consortium of Japanese companies has been working since 1998 on an IPv6/IPsec implementation. (www.kame.net).

[6] *See* Narten, Draves, RFC 3041, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6."

[7] Thayer, Doraswamy, Glenn, RFC 2411, "IP Security Document Roadmap." *See* Kent, Atkinson, RFC 2401, "Security Architecture for the Internet Protocol." *See generally* IETF IPsec Working Group (http://www.ietf.org/html.charters/ipsec-charter.html) ; NIST IPsec Project (http://csrc.nist.gov/ipsec/)

[8] RFC 2411.

[9] RFC 2401.

[10] RFC 2401, *See* Kent, Atkinson, RFC 2406, "IP Encapsulating Security Payload."

[11] RFC 3041.

networks.[12] This behavior is very much like that of an online "cookie," except while a "cookie" tracks usage on a web site and may be erased, the original IPv6 addressing scheme would have allowed the tracking of all online activity (*e.g.*, email, instant messaging, video conferencing, in addition to web traffic) through an unchangeable identifying number.[13]

To address this privacy and security threat, the IETF developed RFC 3041, "Privacy Extensions for Stateless Autoconfiguration in IPv6."[14] This aspect of the IPv6 standard increases end user privacy by enabling users to periodically randomize their IPv6 address as well as generate temporary addresses, thus preventing the creation of a unique, unchangeable IPv6 address assigned to a specific person.[15]

Further, this threat to online privacy also created a threat to network security. The early static addressing scheme that created unchangeable, unique IPv6 addresses could allow malicious users to map the "topography" of IPv6 networks, and locate key infrastructure, such as underlying subnet structures and mapping between networks, to focus their attacks.[16] The feature created to protect end user privacy in this situation also protects network security from malicious attack. Randomized addressing increases network security by allowing IPv6 systems to "hide" from attacks and threats. For example, the White House changed IP addresses of www.whitehouse.gov to dodge the "Code Red" denial of service attacks.[17] Thus, strong privacy protections also serve as important security safeguards, which help ensure the safety and stability of the Internet in general.

Recommendations for IPv6 Policy by the DOC

The U.S. government can play a vital role in encouraging the use of technical privacy enhancing technologies, and preserving those technical means of enhancing technologies against expansion of law enforcement access.

First, the DOC should join the EC IPv6 Task Force[18] in strongly encouraging that the technical privacy protections in the IPv6 standard are implemented by default by all vendors, and used regularly to protect end users. Specifically, the DOC should strongly encourage that all IPv6 implementations meet the requirements of RFC 3041, allowing users to generate a random IPv6 address to prevent tracking the network activity of a user across multiple networks. Further, RFC 3041 and other privacy enhancing technologies should be made readily available and accessible to consumers. Further, the DOC should recommend that vendors implement

---

[12] *See* RFC 3041 § 2.1
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *See Id.,* § 2.1
[17] *See* "Code Red Worm targets White House," July 19, 2001, *at* http://news.com.com/2100-1001-270272.html?legacy=cnet.
[18] EC IPv6 Task Force, Discussion document from the European Commission IPv6 Task Force to the Article 29 Dat a Protection Working Group, *at* http://www.ec.ipv6tf.org/PublicDocuments/Article29_v1_2.pdf.

technologies that automatically change IPv6 addresses, as specified by RFC 3041, on a regular basis to prevent third party surveillance or monitoring.

Secondly, the DOC should encourage commercial developers writing software for IPv6 to take advantage of the IPsec services, such as end-to-end encryption. Further, the DOC should ensure that all government networks and applications fully utilize the privacy and security safeguards of IPv6 to protect sensitive data and systems on the Internet against threats such as identity theft, hacking, and fraud.

Lastly, the DOC should ensure that IPv6's built-in security and other technical privacy safeguards are not compromised by an expansion of CALEA requirements to create security holes for law enforcement surveillance in the IPv6 data network. Extending CALEA surveillance capabilities from dedicated voice communications networks to information services such as IPv6 goes far beyond the intent of Congress and would pose significant threats to Internet security and stability. Imposing requirements that weaken technical privacy protections would compromise IPv6 security features by creating new vulnerabilities and thus diminish consumer user's privacy interests. Moreover, requirements that weaken technical privacy protection threaten the security of the nation's critical communications infrastructure, implicating national security interests. Given the international nature of IPv6, IPv6 systems weakened by surveillance features would be exploited by malicious non-law enforcement persons and by non-democratic governments to keep their populations under surveillance. Government action to extend CALEA to IPv6 architecture and security features would stifle both domestic migration to IPv6 and domestic software development of IPv6 applications.

We appreciate your consideration of our views.

Sincerely,

Marc Rotenberg
EPIC Executive Director

Michael Trinh
EPIC Policy Analyst