DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

NATIONAL SCIENCE FOUNDATION [Docket No. 160810714–6714–01] RIN 0660–XC029

Comments Regarding the Incentives, Benefits, Costs, and Challenges to IPv6 Implementation

Written comments submitted by email to *ipv6@ntia.doc.gov*

C. M. Keliiaa, Sandia National Laboratories

SAND Number: SAND2016-11060 O

A. Internet protocol version 6

Request for Comment: NTIA invites comment on the following questions, in whole or in part:

Note that comments reflect the opinion and conclusions of the author through industry observation and experience.

Benefits:

1. What are the benefits of implementing IPv6? For example, what are the direct performance benefits of implementing IPv6 for end users, or for enhanced network security, as compared to IPv4?

Comments to *Benefits* Question 1: Enterprise deployment of internet protocol, version 6 (IPv6) aligns an organization with current Internet Engineering Task Force (IETF) standards. The American Registry for Internet Numbers (ARIN) internet protocol (IP), version 4 (IPv4) free pool was exhausted to zero on September 24, 2015. Subsequently the IETF obsoleted the IPv4 suite of standards on March 14, 2016. IPv4 is simply not sustainable for new information and communications technology (ICT) growth. IPv6 is the only sustainable IP solution for future internet growth and innovation. References: https://www.arin.net/vault/announcements/2015/20150924.html, https://tools.ietf.org/html/draft-howard-sunset4-v4historic-00.

Embedded IPv6 capabilities must be managed for function and cybersecurity. These capabilities are now in all modern platforms, operating systems, network equipment, and security products. Enterprise IPv6 adoption ensures continuity of internet and broadband information services, standards compliance, and competitive advantage amid unprecedented ICT industry growth. Reference: http://www.ipv6forum.org.

There are traffic performance efficiencies with IPv6 as compared to IPv4 due to consistent and smaller packet header size (40 bytes) as well as no need for fragmentation in route from source to destination. These efficiencies are beneficial to internet, enterprise, and mobile operations. An example of a market response to these efficiencies is the Apple, Inc. June 1, 2016 move to IPv6 only apps. References: https://datatracker.ietf.org/doc/draft-ietf-6man-rfc2460bis/, https://developer.apple.com/news/?id=05042016a.

Security is an interesting issue in comparison. First, ICT workforce IPv6 subject matter expertise must be at a level comparable to that of the IPv4 based knowledge, skills, and abilities (KSA) to architect, design, secure, deploy, and maintain a fully capable IPv6 enabled enterprise. Workforce KSA is the most significant enabler for cybersecurity. IPv6 like its predecessor is relatively agnostic to security in its simple and native implementation. But unlike its predecessor, new deployment of the IPv6 suite of technologies offer an unprecedented opportunity to have cybersecurity built-in as a design requirement, concept to disposition. Baked-in cybersecurity with IPv6 is a time sensitive proposition for public, private, and national security concerns. If IPv6 deployments reach maturity without cybersecurity as a design requirement we are left with bolt-on cybersecurity. Bolt-on cybersecurity is what occurred with IPv4 over the last 35 years, giving rise to a worldwide cyber threat and hence a cybersecurity industry. Reference: http://www.internetsociety.org/deploy360/resources/nist-guidelines-for-the-secure-deployment-of-ipv6/.

2. What are the expected or unexpected benefits of implementing IPv6?

Comments to *Benefits* Question 2: The predominance of IPv4 long delayed the adoption of IPv6 because dual-stack adds complexity, risk, and cost. Conversely, when the market penetration of IPv6 reaches predominance, as is already the case with major carriers, then moving to IPv6 only "single-stack" operations will reduce complexity, risk, and costs as compared with dual-stack operations. References: http://www.worldipv6launch.org/measurements/, https://www.youtube.com/watch?v=EfjdOc41g0s, https://code.facebook.com/posts/1192894270727351/ipv6-it-s-time-to-get-on-board/.

The IP transition for enterprise adoption of IPv6 is orthogonal to the mobile and internet of things (IoT) broadband adoption of IPv6. IP is a broadband technology that reaches across all critical infrastructure sectors, telecommunications and internet provider services, and enterprises requiring internet connectivity. In all cases a well-managed IPv6 only environment will realize new operational efficiencies with increased opportunities for ICT innovation and security. Reference: https://www.dhs.gov/critical-infrastructure-sectors.

Obstacles:

1. What are the biggest obstacles related to IPv6 implementation? For example, is it difficult to access adequate vendor support for IPv6 hardware and/or software? Does successful implementation depend directly on another service provider?

Comments to *Obstacles* Question 1: Internet service providers, telecoms, and enterprises are faced with a distinctly different suite of technologies with IPv6 that are vastly different in scale from its IPv4 predecessor. The key obstacle is ICT workforce KSA to expertly architect, design, deploy, secure, and maintain IPv6 operations.

A secondary, although as important obstacle to IPv6 adoption is the lack of executive championship to enable the workforce.

Third, application developers should review and possibly rewrite code to meet current IPv6 standards. Reference: https://www.arin.net/vault/announcements/2015/20150708.html.

Fourth, Cybersecurity is not well understood at scale for IPv6. This is a particular concern due to the rate of change, ICT impact, and the scale that IPv6 provides for increased worldwide information services.

Lastly, Vendor functionality in some sectors may not provide sufficient industry standard-based IPv6 capability for cohesive integration needed for enterprise operations. For example, continuous diagnostics and monitoring (CDM). Reference: https://www.cisecurity.org/critical-controls.cfm.

2. How does an organization overcome those obstacles?

Comments to *Obstacles* Question 2: Workforce development should start early in the IPv6 planning phase to prepare the ICT workforce for the array of tasks associated with managing IPv6 operations. The two IP versions function independently from each other, so in effect a dual-stack enabled organization is running two logically separated network infrastructure foundations. At such time as the workforce is competent with IPv6 than IPv4 operations may be decommissioned to reduce the vulnerabilities and overhead associated with maintaining dual-stack operations.

An executive champion should enable the workforce to train and gain hands on experience through test and evaluation of the IPv6 technology suite with a directed cybersecurity protection posture specific to the organization. Professional advancement through industry certifications should be encouraged and rewarded. Those that establish themselves as technical leaders should be encouraged through financial incentives to mentor others. Reference: http://education.ipv6forum.com.

Vendors that do not provide sufficient functionality should be required to provide an IPv6 capability roadmap or be replaced with competitive vendor products that do provide sufficient IPv6 capability. This includes the full gamut of enterprise vendor offerings including cloud, mobility, software defined networks and network function virtualization (SDN/NFV), IoT, and cybersecurity products. References: http://5gmwi.committees.comsoc.org, http://sdnnfv.committees.comsoc.org, http://iot.committees.comsoc.org, https://www.ipv6ready.org, https://www.ipv6ready.org/db/index.php/public/?o=4.

Incentives:

1. What additional incentives would be helpful in a decision to implement IPv6?

Comments to *Incentives* Question 1: New IPv6 deployment provides the opportunity to engineer cybersecurity as a design requirement. Cybersecurity for IPv6 enabled infrastructure is a high concern due to increased risk levels introduced by complexities in the internet wide transition from the legacy IPv4 to IPv6. Cybersecurity research is necessary to understand the enterprise attack surface and to secure service, application, system, and network assets. Cybersecurity as a design requirement will increase the protection posture of an enterprise or provider to the benefit of improved enterprise information service continuity, mobile device security, mobile network security, and security in the developing IPv6 based IoT. References: http://prod.sandia.gov/techlib/access-control.cgi/2010/104766.pdf, http://www.sandia.gov/missions/defense_systems/cybersecurity.html.

2. If one factor made the crucial difference in deciding to implement IPv6, as opposed to not implementing IPv6, what is that factor?

Comments to *Incentives* Question 2: Cyber infrastructure modernization: IPv6 fundamentally enables next generation internet services comprising mobility, mobile networks, IoT, and distributed sensor networks that will instrument "smart" IP enabled critical infrastructure. Industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems integration with ICT is already impacting the Department of Homeland Security (DHS) defined critical infrastructure sectors. Cyber critical infrastructure modernization is rapidly occurring in: the IT sector with IPv6 enabled systems, network, and security products; the Communications sector with IPv6 enabled carrier infrastructure; the Healthcare and Public Health sector with telemedicine; the Emergency Services sector with mobile emergency communications and network management systems: Energy sector with smart grid; and the Transportation sector with mobile autonomous vehicles and unmanned aircraft systems (UAS). References: http://www.firstnet.gov. http://energy.gov/oe/services/technology-development/smart-grid, https://www.transportation.gov/AV, https://www.faa.gov/uas/, http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated, http://www.gartner.com/newsroom/id/3165317.

Motivation:

1. What is typically the driving motivation behind an organization's decision to implement IPv6?

Comments to *Motivation* Question 1: IPv6 provides an enterprise business continuity of information services to external business partners and internet based customer services. In addition, the predominance of IPv6 will accelerate its own deployment to meet market demand in mobile, IoT, and enterprise information services. References: http://pmimilehi.org/images/meeting/062216/ipv6_for_it_leaders_2016_06_22_v2.pdf.

2. What are the job titles and/or roles of the people within an organization typically involved in a decision to implement IPv6? What are those individuals' primary motivations when it comes to implementing IPv6?

Comments to *Motivation* Question 2: Risk acceptance: A commitment is required from the risk managers of an organization, typically the Chief Information Officer (CIO) and Chief Security Officer (CSO), pending analysis of IPv6 impact to business continuity of information services. ICT professionals will be driven to update KSA's when corporate direction is clearly stated and supported. IPv6 is much more than a network issue and it underpins next generation information services comprising applications, systems, cybersecurity, and operational support systems. The ICT workforce as a whole should be involved in preparing for IPv6 adoption. Software developers should use the ARIN Preparing Applications for IPv6 guidelines; system administrators and cybersecurity professionals should become familiar with the National Institute of standards and Technology (NIST) IPv6 Security guidelines and develop secure configuration management for the enterprise; incident response professionals should be knowledgeable on the new features of IPv6; identity credential and access management (ICAM) professionals should understand how authentication services are facilitated in an IPv6 enabled environment; and network, operational support, and IP address management (IPAM) professionals should understand IPv6 functionality in the network and operational support systems. Emergent areas of communications, such machine-to-machine communications (M2M) should be identified for standards based market opportunities. Reference: https://www.ietf.org/mail-archive/web/smartobjectdir/current/pdfiZ5zTqvuNV.pdf.

Return on Investment:

1. What is the anticipated return on an IPv6-related investment? How quickly is a return on investment expected?

Comments to *Return on Investment* Question 1: A C-suite business case for the adoption of IPv6 is to be positioned for market opportunities in mobility, cloud, IoT, and smart infrastructure, and to reduce complexity, risks, and costs by eventually moving to a single stack IPv6 solution. Two years is anticipated for return on investment (ROI) of operational expenditures (OpEx) in workforce development that will continue to add value via IPv6 connectivity benefiting any organization for the foreseeable future.

2. Is return on investment a reason to implement IPv6, or is implementation considered a cost of doing business?

Comments to *Return on Investment* Question 2: Yes, ROI is a reason to invest in and implement IPv6. The primary ROI is market relevance and revenue realized in market opportunities in mobility, cloud, IoT, and smart infrastructure development including manufacturing and services. An initial investment is necessary for workforce development that when complete will continue as normal technology refresh and training included in the cost of doing business.

Implementation:

1. How long does the planning process for IPv6 implementation take?

Comments to *Implementation* Question 1: There is a steep learning curve for IPv6 that may take two to three years for ICT professionals to reach a level of IPv6 expertise equivalent to IPv4 based expertise. Progress will follow the learning curve and knowledge level of the ICT workforce. Executive championship is a key enabler for organizational priority and direction in terms of resource allocation to train, test, plan, and implement IPv6.

2. How long does actual implementation of IPv6 typically take? Is implementation a single event or evolutionary?

Comments to *Implementation* Question 2: The pace of deployment is associated with the KSA of the ICT workforce and the level of executive championship driving IPv6 implementation for an organization. IPv6 implementation will be enabled or impeded by the level of ICT expertise relevant to the needs of an organization. Time to deploy is estimated at two to five years depending on ICT workforce development and executive championship. IPv6 impact is indeed all things internet and therefore will be evolutionary with rigor pertinent to the size, needs, and complexity of an organization. Organic workforce development is recommended since IPv6 expertise in industry is developing and is difficult to buy or hire in.

Cost of Implementation:

1. What are the different types of costs involved in implementing IPv6? What are the typical magnitudes of each type of cost?

Comments to *Cost of Implementation* Question 1: Types of cost include OpEx and capital expenditures (CapEx). The CapEx investment has already been made by most organizations during the course of procurement cycles circa 2010. OpEx represents the initial workforce development investment necessary to manage embedded IPv6 capability that will eventually be absorbed into daily operational costs.

A test and evaluation lab should be established to provide hands on experience to the ICT workforce as part of the planning, initiation, and implementation phases of IPv6 deployment. The test bed can be equipped with reallocated ICT resources to minimize CapEx investment.

Time must be allocated to fulfill training duties. A focused OpEx investment to facilitate ICT workforce development may include in-house training for 25 students estimated at $30k per class; individual allowance for literature review $250.00 per annum; and conference attendance estimated at $2k per conference plus travel.

A concerted level of effort to organically build a knowledgeable ICT workforce of 100 with an average $50,000 salary, gross $24/hour, at a 10% training duty cycle (208 hours of 2080) is roughly estimated at: $5k per ICT professional per annum, $500,000 total; $120k for four in-house leader-led classes; $25,000 literature review; and $200k conference attendance, total estimate per annum is $845k.

2. How does an organization cover those costs?

Comments to *Cost of Implementation* Question 2: CapEx investment for IPv6 capable equipment is already sufficient for many organizations in the course of normal technical refresh and procurement cycles. Many organizations have, or should have continual ICT training requirements and IPv6 workforce development can be incorporated into existing training requirement costs. Strategic planning for information service delivery including business continuity concerns could supplement workforce development for IPv6. Tactical competitive advantage in the ICT industry could also be leveraged for investment, cost recovery, and ROI.

3. How does an organization justify those costs?

Comments to *Cost of Implementation* Question 3: Costs associated with IPv6 deployment may be derived from a business need for ICT industry relevance and cybersecurity. Cost justification includes business continuity of information services and standards based market preparedness for future business. Minimal CapEx and OpEx investment is anticipated for organizations that follow technical refresh and workforce development best practices. Cyber security must be designed and maintained by a knowledgeable workforce or risk information compromise through unmitigated risk exposure and compromise with asymmetric damages to public reputation, data loss, data integrity, and information service availability.

4. What considerations are there for cost-saving?

Comments to *Cost of Implementation* Question 4: Once workforce development is complete there are no significant hurdles to the ubiquitous deployment of IPv6. Facebook, Inc. and the Defense Research Engineering Network (DREN) are examples of large enterprise and infrastructure deployments that taken advantage of IPv6 efficiencies. References: https://www.youtube.com/watch?v=An7s25FSK0U, https://www.nitrd.gov/nitrdgroups/images/7/7e/IPv6-DREN3-Lessons-RonBroersma.pdf.

5. What implication does the size of an organization implementing IPv6 have on cost?

Comments to *Cost of Implementation* Question 5: The greater the size of the ICT workforce the greater the workforce development cost will be. These costs will eventually be absorbed into the cost of doing business.

Promotional Efforts:

1. What promotional efforts, if any, should NTIA take? What would have the most impact? cost?

Comments to *Promotional Efforts* Question 1: A national science, technology, engineering, and math (STEM) workforce development program specific to ICT would help to bridge the KSA gap. Industry organizations such as the North American IPv6 forum, Sysadmin, Audit, Network, Security (SANS) Institute, and the International Information System Security Certification Consortium $(ISC)^2$ should be utilized to advance and certify a national ICT workforce. Higher education and minority serving institutions should be incented to broaden curriculums to include IPv6 as a fundamental enabler for mobile, IoT, SDN/NFV, cloud, and smart infrastructure innovation. Lastly, federally funded research and development centers (FFRDC) could provide objective advisory to state, local tribal, and territorial efforts to modernize cyber critical infrastructures. References: https://www.sans.org, https://www.isc2.org, https://www.dhs.gov/enhanced-cybersecurity-services.

2. What promotional efforts, if any, are being led by the private sector? Have they been effective?

Comments to *Promotional Efforts* Question 2: The large carrier space is predominantly IPv6 capable. Additionally, the North American IPv6 taskforce (nav6tf) has contributed in the private sector. References: https://www.youtube.com/watch?v=EfjdOc41g0s, http://www.nav6tf.org.

3. Which additional stakeholders should NTIA target? What is the most effective forum?

Comments to *Promotional Efforts* Question 3: Federal, state, local, tribal, territorial, and private sector critical infrastructure stakeholders should be targeted in a collaborative and inclusive national effort toward anchor institution and critical infrastructure modernization.

4. Should NTIA partner with any particular stakeholder group?

Comments to *Promotional Efforts* Question 4: Federal, state, local, tribal, territorial, and private sector stakeholders. Reference: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

Additional Issues:

1. NTIA invites commenters to provide any additional information on other issues not identified in this RFC that could contribute to NTIA's understanding of the considerations that organizations take into account when deciding to proceed with IPv6 implementation, as well as future IPv6 promotional efforts that NTIA may undertake.

Comments to *Additional Issues* Issue 1: IPv6 is a broadband technology. National broadband expansion and the internet wide IP transition coincide amid tremendous ICT sector growth. Enterprise adoption of IPv6 follows large carrier deployments, which are predominantly using IPv6 today. The growth of expanded broadband services in rural areas including state, local, tribal, and territorial jurisdictions indicates that small rural internet service and telecommunications providers will have to adopt IPv6 to develop and deploy new broadband internet services to serve areas and population groups that have lacked sufficient internet access. Rural area impacts include critical services that depend on mobile capabilities as part of the communications portfolio. It is important to note that dual-stack is not the goal, rather native IPv6 functionality and turning off IPv4 is the goal. Once IPv4 is turned off than IPv6 native functionality will yield broadband advanced internet services to areas and groups that have under-utilized broadband technology. Reference: https://transition.fcc.gov/cgb/consumerfacts/broadband_initiatives.pdf.

Comments to *Additional Issues* Issue 2: Cybersecurity research is necessary for developing secure IPv6 enabled services. This a concern as 5G mobile capabilities and IoT develop to support "smart" infrastructure in the IT, Emergency Services, Energy, and Transportation critical infrastructure sectors. Reference: https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf.