Via email to
firstnetnoi@ntia.doc.gov

Before the

U.S. DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

On Behalf of the First Responder Network Authority

Development of the Nationwide Interoperable Public Safety Broadband Network

Docket No. 120928505-2505-01

COMMENTS OF CENTURYLINK ON NOTICE OF INQUIRY

I. INTRODUCTION

CenturyLink[1] hereby responds to the Notice of Inquiry (NOI)[2] of the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce, issued on behalf of the First Responder Network Authority (FirstNet), requesting "public comment on the conceptual network architecture presentation made at the FirstNet Board of Directors' meeting held on September 25, 2012," and inviting input on other network design and business plan considerations.[3] As stated in the NOI, FirstNet intends to use the information

[1] CenturyLink is the third largest telecommunications company in the United States and is recognized as a leader in the network services market by technology industry analyst firms. The company is a global leader in cloud infrastructure and hosted IT solutions for enterprise customers. CenturyLink provides data, voice and managed services in local, national and select international markets through its high-quality advanced fiber optic network and multiple data centers for businesses and consumers. The company also offers advanced entertainment services under the CenturyLink™ Prism™ TV and DIRECTV brands. Headquartered in Monroe, Louisiana, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations. For more information, visit www.centurylink.com.

[2] Notice of Inquiry, Federal Register, Vol. 77, No. 193, October 4, 2012, at 60680-60681.

[3] NOI at 60680.

received in response to the NOI to shape its efforts to establish a nationwide, interoperable public safety broadband network (Public Safety Broadband Network or Network), based on a single nationwide network architecture, as mandated by the Middle Class Tax Relief and Job Creation Act of 2012 (Act).[4] CenturyLink welcomes the opportunity to submit these comments and share its views with FirstNet as it embarks upon the very important task of fulfilling the Act's requirements and advancing the capabilities of public safety entities throughout the United States. Below, CenturyLink discusses the importance of FirstNet employing open and transparent public-private partnerships and leveraging the existing broadband infrastructure and services of wireline operators[5] that have demonstrated their ability to meet the requirements for the Public Safety Broadband Network as FirstNet proceeds to establish the Network. CenturyLink also comments on the architectural design of the Public Safety Broadband Network's core network (CN) component.

II. SOUND POLICY PRINCIPLES SHOULD GUIDE FIRSTNET

CenturyLink supports the Act's goal of establishing a single nationwide, interoperable public safety broadband network that enables first responders to effectively communicate and exchange data with and among each other during emergencies, leverages new technologies to improve response times, expands life-saving capabilities, and enhances the effectiveness of public safety entities. But, accomplishing an endeavor as ambitious as this in an expeditious and cost effective manner is only possible if open and transparent public-private partnerships are forged from the outset at the federal, state, tribal and local levels. Strong public-private partnerships at all levels that promote participation by all network services providers with a

[4] *Id. See also* Middle Class Tax Relief and Job Creation Act of 2012, Public Law 112-96, 126 Stat. 156 (2012).

[5] Wireline operators provide narrowband and broadband networks and services.

demonstrated capability for constructing and operating reliable and secure networks will best ensure that the elements, functions and equipment incorporated into the Network are based on commercial standards and that the network is capable of evolving with technological advancements – both of which are required by the Act.[6]

FirstNet, state, tribal and local governments should not fund the construction of new network facilities where commercial networks exist that can meet all reasonable network requirements adopted for inclusion in FirstNet's requests for proposals (RFPs) or the RFPs of state, tribal or local governments for their segments of the Public Safety Broadband Network. Leveraging existing fiber and other broadband-capable facilities will not only decrease the cost of deploying the Public Safety Broadband Network but will also allow for a more timely completion of the Network. Congress recognized the public benefits that accrue from the use of existing infrastructure that can support the functionality envisioned for the Network and the imprudence of unnecessarily overbuilding useful existing infrastructure.[7] The Act directs FirstNet to "enter into agreements to utilize, to the maximum extent economically desirable, existing – (A) commercial or other communications equipment; and (B) Federal, State, tribal, or local infrastructure."[8] There should be no deviation from this instruction.[9]

---

[6] *See* Section 6202(b) [47 U.S.C. 1422].

[7] Companies such as CenturyLink can provide FirstNet and governmental entities at all levels facilities and equipment at the point the governmental entities are ready to deploy broadband infrastructure. CenturyLink has a robust national 207,000 route mile fiber network; 41 U.S. data centers; a comprehensive portfolio of IP-based data, cloud, security, voice, and integrated and managed solutions; and cybersecurity solutions to protect and defend national networks. CenturyLink's Carrier Diverse collocation facilities across North America, where carrier-to-carrier interconnections are established, provide 100% uptime to ensure that customers are operational even during the worst conditions.

[8] Section 6206(c)(3)(A) and (B) [47 U.S.C. 1426(c)(3)(A) and (B)].

[9] Although "economically desirable" is not defined, it is difficult to envision in the context of this massive and costly undertaking that securing cost efficiencies by maximizing the use of existing

The NOI solicits comments on several criteria for a reliable, ubiquitous, redundant, and interoperable broadband network for public safety users. Among the criteria is a requirement that the Public Safety Broadband Network:

> *Uses, to the extent possible, existing radio access network and* ***core network infrastructure installed by commercial mobile operators*** *in order to maximize the coverage and performance delivered to public safety while minimizing the capital expenditures; . . .* . [emphasis added]

CenturyLink is uncertain about how to interpret this criterion. CenturyLink believes that it would be a serious and costly mistake on the part of FirstNet if this criterion signals a bias in favor of commercial mobile operators as suppliers of the network infrastructure to be used to support the CN that is prescribed by the Act.[10] Section 6206(c)(3) is not so limiting in establishing FirstNet's responsibility to "leverage existing infrastructure." Wireline operators supply network facilities and services that are essential in the provisioning of today's commercial mobile radio services, and the network facilities and services of wireline operators will continue to be essential for the provisioning of commercial mobile radio services well into the future as greater reliance is placed on broadband facilities and services. In addition to delivering calls from Public Switched Telephone Network (PSTN) customers to the networks of commercial mobile operators and delivering calls from the networks of commercial mobile

---

broadband network facilities and equipment that meet established requirements would not be economically desirable. Accordingly, CenturyLink suggests that "economically desirable," as used in Section 6206(c)(3)(A) and (B), should be read to mean economically feasible. Credible concerns already exist that the $7B committed to fund the Public Safety Broadband Network will be insufficient to accomplish the task.

[10] The Act prescribes a CN that "(A) consists of national and regional data centers, and other elements and functions that may be distributed geographically, all of which shall be based on commercial standards; and (B) provides connectivity between – (i) the radio access network; and (ii) the public Internet or the public switched network, or both;" Section 6202(b)(1) [47 U.S.C. 1422(b)(1)].

operators to PSTN customers, the networks of wireline operators also provide backhaul[11] and backbone services for commercial mobile operators. Without wireline facilities and services, commercial mobile radio services would not be as robust, reliable or ubiquitous as they are today. Wireline operators have broadband network facilities available today that are fully capable of satisfying the requirements for the CN and supporting the broadband capabilities envisioned for the Public Safety Broadband Network.

As FirstNet considers the network design and specifications for the CN that will be contained in its RFP(s), it should not seek to narrow or limit the opportunities for wireline operators to participate in providing network facilities or services for the CN, or any other part of the Public Safety Broadband Network that wireline operators demonstrate their ability to supply or support on a cost-effective basis. Rather, FirstNet should avail itself of every opportunity to leverage the existing facilities and services of wireline operators and keep the door open for the use of the facilities and services that will be available from them as the Network evolves with technological advancements. CenturyLink encourages FirstNet to evidence a bias in its RFPs for opening the Public Safety Broadband Network procurement processes to all providers able to deliver the network capabilities sought by public safety entities in a manner that "ensure[s] the safety, security, and resiliency of the network, including . . . protecting and monitoring the network . . . against cyberattack[.]"[12]

III. THE CORE NETWORK ARCHITECTURE

A. A Converged Network Provides Benefits Over a Separate Network

There are high level design considerations that must be addressed in planning for the Public Safety Broadband Network. A fundamental consideration is whether the Network should

[11] CenturyLink had approximately 12,150 fiber-connected cell phone towers as of June 30, 2012.

[12] Section 6206(b)(2)(A) [47 U.S.C. (b)(2)(A)].

be physically separate or a part of a larger, converged network that also carries non-public safety traffic. CenturyLink submits that if properly implemented, a Public Safety Broadband Network that is a part of a converged network provides several important benefits over a physically separate Public Safety Broadband Network.

The first and most obvious benefit of utilizing a converged network design is cost. A converged network should result in lower overall costs than a physically separate network while enabling provision of the same services and capabilities. Other benefits derived from using a converged network design include higher network capacity during emergencies, higher availability and resiliency, and larger geographic coverage.

In order to obtain these benefits, a converged network needs logical traffic separation and multiple classes of service. All Public Safety Broadband Network traffic should be prioritized above other converged network traffic up to reasonable limits. Because all public safety traffic may not be of equivalent importance, there should be different classes of public safety traffic established to ensure that the highest priority public safety traffic reaches its destination. The converged network would be expected to protect and isolate routing and other critical protocols inside the Public Safety Broadband Network to ensure that non-Public Safety Broadband Network traffic does not interfere with or inhibit priority Public Safety Broadband Network traffic. Finally, ingress points must ensure that only appropriate Public Safety Broadband Network traffic enters and have safeguards in place for blocking malicious or non-appropriate network traffic. This last requirement would apply to a physically separate Public Safety Broadband Network as well.

B. Principles for the Design of the Core Network

CenturyLink envisions three networks that would comprise the CN that is prescribed by the Act – the Metro Core Network (MCN, the Backbone Core Network (BCN) and the Evolved Packet Core Network (EPC)). The EPC is the mobile core network for LTE and is not the primary focus of these comments. The MCN and the BCN would be used to provide full connectivity to radio access networks (RANs), the public Internet and the PSTN. The MCN would provide connectivity between radio towers and the EPC for mobile operators. The BCN would provide connectivity between multiple EPCs. The BCN could also be used to provide connectivity to the public Internet. By applying the following design principles, the same CN can be used by different mobile operators to enable the Public Safety Broadband Network.

High Availability

High availability is essential for the Public Safety Broadband Network. The availability of a network is only as high as its weakest element. Accordingly, all network elements for the CN should be carrier-grade equipment. Each network element should have dual power supplies and dual control planes with field-upgradable units. Network elements should be connected to the network with fully redundant links.

Class of Service

The CN should be able to differentiate traffic on a packet-by-packet basis so that public safety traffic and non-public safety traffic can be appropriately differentiated.[13] This will ensure that public safety traffic receives the highest level of priority and that delivery is assured. Public safety traffic on the CN should receive the highest designation among classes of service. It should have the lowest acceptable level of latency and no jitter.

[13] *See* the discussion of prioritization in Section III.A. at p.6.

Customer Differentiation

The CN should always be secure so that public safety traffic is not impacted by the traffic of other customers, and it should not be vulnerable to security vectors. The CN should also be able to separate the customers and their traffic from each other.

The MCN should be a carrier ethernet network as defined by the Metro Ethernet Forum. Since it is strictly a Layer 2[14] ethernet network, there should be no access from the public Internet to any of its network elements or to radio towers. Public safety traffic would be kept separate from the traffic of other customers through the use of virtual local area network tags.[15]

The BCN should be an Internet Protocol (IP)/Multi-Protocol Label Switching (MPLS)-based network. By using the MPLS standard, public safety traffic will be placed into its own virtual routed forwarding (VRF) technology.[16]

Network Management

The entire CN should be managed by a network operations center (NOC) that is operational at all times and is sufficiently staffed with skilled technicians who can respond to network events and resolve any problems that may arise in the CN. The Public Safety Broadband Network Command Center should be able to directly contact the NOC should it encounter CN-related issues. The NOC should also have a well-defined disaster recovery plan and geographically diverse locations so that its network monitoring functions remain operational during local or regional crises and disasters.

---

[14] Layer 2 of the Opens Systems Interconnection (OSI) Reference Model. Layer 2 is the Data Link layer.

[15] Virtual local area network tags are based on IEEE 802.3q standards for local and metropolitan area networks.

[16] VRF is based on Request For Comment (RFC) 4364. By placing public safety traffic in its own VRF, the traffic is separated from other customers' traffic and is secure as it travels through the network.

C. Relationship with other Internet Service Providers

The BCN operator must have public and private peering bi-lateral agreements in place with other Tier 1 Internet service providers (ISPs).[17] Each peering agreement must have additional language or criteria, usually 50% utilization, that triggers a circuit upgrade. The agreement must also have stringent acceptable use policies in place with all of the BCN's peering partners to ensure that the highest level of security is achieved and common Internet-based threats, such as denial of service (DoS) attacks, are mitigated. The BCN operator must support Government-assigned and Internet Network Information Center-registered IP addresses and domain names. All private peering arrangements must have redundant links for connections to private peering partners.

D. Relationship with the PSTN

Connectivity to the PSTN should be delivered in a series of converged and hybrid layers, consisting of both packet and circuit switched methodologies that incorporate a cooperative architectural design for resiliency. Having these layers will allow for the termination of voice and application traffic from the Public Safety Broadband Network to the PSTN, public safety answering points (PSAPs) and other support entities. This architecture will consist of emergency services IP networks (ESInets) and legacy selective router (LSR) arrangements for the delivery of traffic to PSAPs as well as a combination of legacy time division multiplexing and next-generation switches for the delivery of traffic to the PSTN. Each EPC will diversely peer with a legacy network gateway for convergence and circuit-switched delivery to the LSR and PSAP in a National Emergency Numbering Association (NENA) i2 arrangement and will diversely peer

[17] Enforceable agreements governing the exchange of traffic are necessary in order to secure assurances that expected service levels are met for traffic carried across the networks of multiple providers.

with an ESInet for packet-based delivery to a PSAP in a NENA i3 arrangement.[18] All PSAPs will be diversely connected to their primary and secondary service providers' ESInets. Alternate connectivity between service providers will be used when a primary service provider's connection to a PSAP is disrupted or degraded.

The PSTN should provide priority processing of Public Safety Broadband Network traffic where supported. Inter-carrier connectivity will be used for redundancy to accommodate overflow traffic in order to mitigate congestion in the PSTN. Redundant and alternate routing models should be exercised to ensure the delivery of Public Safety Broadband Network traffic to emergency services and support entities.

E. The Evolved Packet Core Network

All EPCs will be designed and placed in a geographically redundant configuration by region. Each regional EPC will be connected to its mated EPC utilizing alternate paths, CN elements and service providers. All EPCs and corresponding elements should be IPv6 compliant.[19] Each EPC, along with its subordinate systems and databases, should be configured to support localized and regional redundancy, based on manufacturers' and industry reliability and quality standards so that traffic can re-register and route to one or more alternate EPCs, and service not be interrupted, should an EPC become inaccessible. Public Safety Broadband

[18] NENA i2: NENA Interim VoIP Architecture for Enhanced 9-1-1 Services, NENA 08-001, Ver. 2. http://c.ymcdn.com/sites/www.nena.org/resource/collection/2851c951-69ff-40f0-a6b8-36a714cb085d/NENA_08-001-v2_Interim_VoIP_Architecture_i2.pdf?hhSearchTerms=i2;

NENA i3: NENA Detailed Functional and Interface Standards for the NENA i3 Solution (TSD), NENA 08-003, Ver. 1 http://c.ymcdn.com/sites/www.nena.org/resource/collection/2851c951-69ff-40f0-a6b8-36a714cb085d/NENA_08-003_Detailed_Functional_&_Interface_Specification_for_the_NENA_i3_Solution-Stage_3.pdf?hhSearchTerms=i3.

[19] It is expected that IPv4 interworking will be required for a transitional period.

Network traffic should have priority over non-Network traffic, and there should be a high likelihood of its completion at all times, especially during high traffic congestion conditions.

F. Ensuring Core Network Safety, Security and Resiliency

In addition to being a highly available network, the CN should also be very resilient and able to recover very quickly after a network event. The CN should have multiple network elements with each network element connected to other network elements using redundant links. These redundant links should have enough capacity to ensure that a fiber cut or other network-related events do not cause congestion or dropped packets for public safety traffic. During a network event, public safety traffic should not be interrupted for more than 50 milliseconds. Most applications, including voice-based applications, do not suffer service-affecting degradation as a result of an interruption of less than 50 milliseconds.

The CN should also be secure against attack vectors. The security should extend to physical, logical and cyber attack vectors. The operator responsible for the CN should follow RFC 3871[20] as the basis for its cyber security operating practices. The CN operator should also track US-CERT[21] alerts and Product Security Incident Report Team alerts from the manufacturers of the CN's network elements.

As a general matter, security has three fundamental concepts that should be considered when assessing the risks to a network and the information that transits that network: availability, confidentiality and integrity. Cyber security also requires the consideration of these concepts.

[20] Operational Security Requirements for Large Internet Service Provider (ISP) Network Infrastructure.

[21] U. S. Computer Emergency Readiness Team.

Availability

Network availability should be one of the highest considerations in a public safety network. DoS attacks, for example, commonly occur in different manners. Sending large amounts of traffic that impact network capacity or critical services is the most common method of attack seen on the Internet. Another common method is attacking critical components or protocols in the network path that prevent traffic from reaching its destination. The CN should protect itself from these types of attack by separating and prioritizing public safety traffic over other network traffic. A properly designed network that provides logical traffic separation and prioritization will provide a higher traffic surge capacity for the same cost than a physically separate and dedicated network. The traffic surge capacity of a network is an important factor when considering a network's ability to withstand large scale DoS attacks.

Redundancy is critical for availability. As a result of a disaster, a portion of the CN could be physically damaged or impaired due to the disaster. Networks with higher capacity and more redundancy provide greater assurance of their availability.

The infrastructure of the CN should be appropriately hardened to resist common forms of attacks. Critical routing and name resolution protocols should be hardened and protected. Traffic entering the CN should be screened and possibly rate limited to minimize the amount of malicious traffic that can enter the CN. Traffic associated with routing protocols, domain name servers and network element management should be given the highest priority of any traffic on the Network. Strong network element management protections are very important. This includes strong authentication mechanisms, good code testing procedures and robust configuration management.

Confidentiality

Standard logical traffic isolation techniques, such as MPLS protocol, should provide more than adequate data confidentiality for the CN. Traffic that is especially sensitive should be encrypted from end point to end point to protect it across its entire path as it traverses access and core networks. Given the nature of public safety traffic, it usually does not necessitate traffic encryption in a core network.

Confidentiality attacks are most common at the end points and occur less often within access networks. Due to the traffic volumes in the CN, it is likely to be extremely difficult for an attacker to gain access to, identify, and capture traffic of interest for interception.

Integrity

Network traffic integrity is very important for the Public Safety Broadband Network. The altering of network traffic in the CN, especially if logically separated from other traffic, should prove difficult for an attacker. The protection of routing protocols, name services and network element management traffic provide the best defense against network traffic integrity attacks.

IV. CONCLUSION

The establishment of an interoperable public safety broadband network, based on a single nationwide network architecture, is an important and formidable undertaking. As FirstNet acts to fulfill its responsibilities under the Act to oversee the deployment of the Public Safety Broadband Network, it will face many challenges in accomplishing the Act's goal of providing public safety entities and their personnel with a seamless broadband communications platform for emergency response and recovery. Two of the most critical challenges faced by FirstNet will be to deliver the Network in an expeditious and cost-effective manner. CenturyLink believes

that meeting these challenges is possible if FirstNet forges open and transparent public-private partnerships and leverages the existing broadband infrastructure and services of wireline operators that have demonstrated their ability to provide and operate reliable and secure broadband networks which meet the requirements for the Public Safety Broadband Network.

The successful deployment and operation of the Public Safety Broadband Network will result from an alliance between mobile and wireline network operators. Both are needed. The networks of wireline operators provide access, backhaul and backbone services for commercial mobile operators, and without wireline facilities and services, commercial mobile radio services would not be as robust, reliable or ubiquitous as they are today. It would be a disservice to wireline operators to discount their importance in the current and future provisioning of commercial mobile radio services or the deployment and operation of broadband networks.

CenturyLink's position as a leader in the broadband network services, cloud infrastructure and hosted IT solutions markets makes it well suited to comment on the network design for the CN. CenturyLink requests that FirstNet consider these comments and take them into account as it develops its RFPs for the Public Safety Broadband Network.

Respectfully submitted,

CENTURYLINK

By: /s/ Lawrence E. Sarjeant
Lawrence E. Sarjeant
1099 New York Avenue, N.W.
Suite 250
Washington, DC 20001
202-429-3112
Lawrence.sarjeant@centurylink.com

November 1, 2012

Its Attorney