

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications)	PS Docket No. 15-80
)	
)	
New Part 4 of the Commission's Rules Concerning Disruptions to Communications)	ET Docket No. 04-35
)	
)	
The Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers)	PS Docket No. 11-82
)	

COMMENTS OF COMCAST CORPORATION

WILLKIE FARR & GALLAGHER LLP
1875 K Street, N.W.
Washington, D.C. 20006

Kathryn A. Zachem
Mary P. McManus
COMCAST CORPORATION
300 New Jersey Avenue, N.W., Suite 700
Washington, DC 20001

LAWLER, METZGER, KEENEY
& LOGAN, LLC
1717 K Street, N.W., Suite 1075
Washington, D.C. 20006

Brian A. Rankin
Beth A. Choroser
Pamela S. Miranda
COMCAST CORPORATION
One Comcast Center
55th Floor
Philadelphia, PA 19103

Counsel for Comcast Corporation

August 26, 2016

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY.....1

II. BROADBAND NETWORKS ARE INHERENTLY ROBUST AND RESILIENT....3

A. The Further Notice Incorrectly Assumes that Broadband Networks Are More Susceptible Than Other Networks to Large-Scale Outages.....4

B. Comcast’s BIAS Network Is Dynamic and Capable of Preventing or Efficiently Mitigating Most Consumer-Facing Outages.....7

III. THE DEFINITION OF A REPORTABLE OUTAGE SHOULD BE STRAIGHTFORWARD, CONSISTENT, AND MEANINGFUL.11

A. Reporting Should Be Required Only for “Hard Down” Outages That Significantly Impact BIAS or VoIP Customers.11

B. A Performance Degradation Standard Does Not Make Sense, Would Be Overly Burdensome, and Would Not Provide Useful Information to the Commission. ...14

C. The Commission Should Apply the Current VoIP Reportable Outage Threshold If It Extends Reporting Obligations to BIAS Providers.18

IV. DEDICATED SERVICES SHOULD BE BEYOND THE SCOPE OF ANY NEW OUTAGE REPORTING RULES ADOPTED IN THIS PROCEEDING.....21

V. THE COMMISSION SHOULD ADOPT THE CURRENT TWO-STEP PROCESS FOR ANY AND ALL OUTAGE REPORTING OBLIGATIONS IMPOSED ON IP-BASED SERVICES.....23

VI. THE COMMISSION SHOULD AFFORD STRINGENT CONFIDENTIALITY PROTECTIONS TO OUTAGE REPORTS.27

A. Outage Reports Must Be Treated As Highly Confidential and Subject to Appropriate Safeguards.27

B. The Commission Should Not Share Outage Reports With States.30

VII. CYBERSECURITY ISSUES ARE BEST ADDRESSED THROUGH ONGOING PUBLIC-PRIVATE PARTNERSHIPS AND WORKING GROUPS.32

VIII. THE COMMISSION MUST ENSURE THAT ANY NEW REQUIREMENTS COMPORT WITH THE PAPERWORK REDUCTION ACT.....35

IX. CONCLUSION37

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Amendments to Part 4 of the Commission’s Rules Concerning Disruptions to Communications)	PS Docket No. 15-80
)	
New Part 4 of the Commission’s Rules Concerning Disruptions to Communications)	ET Docket No. 04-35
)	
The Proposed Extension of Part 4 of the Commission’s Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers)	PS Docket No. 11-82

COMMENTS OF COMCAST CORPORATION

Comcast Corporation (“Comcast”) hereby responds to the Further Notice of Proposed Rulemaking adopted by the Federal Communications Commission (“FCC” or “Commission”) on May 25, 2016, in the above-referenced proceedings.¹

I. INTRODUCTION AND SUMMARY

The Further Notice seeks comment on a wide range of issues that concern the possible adoption of outage reporting requirements for broadband services, as well as the potential expansion of the obligations that currently apply to interconnected Voice over Internet Protocol (“VoIP”) providers. Comcast respectfully submits that, in assessing those various proposals, the Commission should bear in mind four key principles:

¹ *Amendments to Part 4 of the Commission’s Rules Concerning Disruptions to Communications, et al.*, Report and Order, Further Notice of Proposed Rulemaking, & Order on Reconsideration, 31 FCC Rcd. 5817 (2016) (“R&O” and “FNPRM” or “Further Notice”).

(1) Outage reports should be useful and targeted to protecting public safety.

Comcast and other broadband providers already have strong incentives to ensure that their networks function optimally and avoid material disruptions to service. The competitive marketplace provides significant accountability if Comcast does not quickly address service outages that occur from time to time and take steps to ensure that major outages are avoided wherever possible. There is no compelling basis to conclude that burdensome reporting obligations are warranted for broadband Internet access services (“BIAS”), that more stringent obligations are necessary for VoIP offerings, or that any additional obligations at all are needed for dedicated services. Nor is there any reason to expand outage reporting to include cybersecurity issues, given that the Commission has not made (nor could it make) a well-grounded determination that ongoing public-private collaborations are inadequate to assist the Commission in making informed policy decisions in that area. Put simply, the Commission should limit and narrowly tailor any obligations it adopts in this proceeding.

(2) Any new outage reporting processes for packet-based services should be straightforward and should not impose substantial additional costs that are disproportionate to the anticipated benefits.

Contrary to the assertions in the Further Notice, the existing reporting requirements for VoIP provide a workable outage reporting model and should not be modified at this time. To the contrary, any additional requirements the FCC adopts for packet-based services should be consistent with today’s VoIP obligations, both in terms of: (a) the number and timing of the reports (*i.e.*, one notification within 24 hours and a final report within 30 days); and (b) the threshold metrics that constitute a reportable outage (*i.e.*, a “hard down” outage that impacts 900,000 user minutes and lasts for at least 30 minutes). The Commission must reject other, more expansive proposals that would impose large costs and burdens on broadband and VoIP providers. Notably, the value of the most burdensome type of reports contemplated in the

Further Notice – those concerning performance degradation – would be minimal or non-existent, while the burden of conducting such monitoring and producing such reports would be substantial. The Paperwork Reduction Act demands that the Commission carefully consider this imbalance.

(3) All outage information must be subject to strong confidentiality protections.

Outage reporting information necessarily includes network infrastructure data that is highly sensitive from both a competitive standpoint and a national security standpoint. The Commission must be careful to implement safeguards that are adequate to protect this information. In the event that the Commission expands reporting obligations to include cybersecurity attacks – which it should not – stringent confidentiality measures would be all the more important.

(4) A broadband outage should not be reportable unless it significantly affects BIAS consumers.

The idea that a reportable outage should be one that impacts customers is implicit in the *user*-minute reporting threshold that currently applies to VoIP and that should likewise apply to any BIAS outage reporting rules adopted in this proceeding. Many instances of infrastructure and network failures are absorbed seamlessly by broadband networks and applications without any consumer impact. This is a key aspect of broadband networks' architecture and design. It would be unduly burdensome to the industry and unhelpful to the Commission if BIAS providers were required to report network events that do not entail significant adverse effects on consumers.

II. BROADBAND NETWORKS ARE INHERENTLY ROBUST AND RESILIENT.

The Further Notice appears to be premised on the notion that broadband networks are more susceptible to large-scale, customer-impacting outages than the public switched telephone

network (“PSTN”). This simply is not the case. To the contrary, broadband networks are designed and maintained to be redundant, resilient, and self-healing. Comcast’s own broadband network exemplifies these realities.

A. The Further Notice Incorrectly Assumes that Broadband Networks Are More Susceptible Than Other Networks to Large-Scale Outages.

In the Further Notice, the Commission asserts that “broadband networks’ interrelated architectural makeup renders them more susceptible to large-scale outages.”² This statement is incorrect. In fact, broadband networks’ architecture and design is exactly what makes them *less* susceptible than legacy networks to broad, consumer-impacting outages.

Because they use packet-switched technology, broadband networks have many built-in redundancies and few single points of failure.³

- “Packet-switched networks, by their very nature, are designed to be *resilient* and *reliable*.”⁴ Unlike circuit-switched networks that establish an end-to-end communications channel for the entirety of a transmission, packet-switched networks break up information into small data packets, which can and usually do travel over multiple routes before being reassembled at their destination.⁵ Routing and re-routing of

² See FNPRM ¶ 103.

³ See, e.g., Sam Biddle, *How to Destroy the Internet*, Gizmodo (May 23, 2012), <http://gizmodo.com/5912383/how-to-destroy-the-internet> (“The enormous, invisible truth of the Internet is that it’s enormously strong. There’s no main switch, no self-destruct button, no wire to be snipped for an easy blackout. The Internet, through a mix of chaotic serendipity and brilliant planning, is redundant to the point of near invincibility. Like a fiber optic hydra, you can hack off great expanses of it, and the thing will keep chugging. It’s smart – almost self-sustaining, able to repair and reroute its paths from one continent and country to another, making up detours on the fly.”).

⁴ Comments of Comcast Corp., PS Docket No. 10-92, at 4 (June 25, 2010) (emphasis added) (“Comcast NOI Comments”).

⁵ As the Commission explained in 1998: “Instead of maintaining an end-to-end channel of communications for the length of the information transfer, packet switching breaks the information up into small packets that are transmitted separately over the most efficient route available, and then reassembled, microseconds later, at their destination.” *Deployment of Wireline Services Offering Advanced Telecommunications Capability*, Memorandum Opinion & Order & NPRM, 13 FCC Rcd. 24011 ¶ 6 (1998); see also Comcast NOI Comments at 4 n.10 (citing same).

information occurs automatically to avoid congestion and failures in connectivity.⁶ If a network link does fail, routers are designed to detect the failure and send the message via a different route. If data is lost in transit, the receiving device can detect a missing packet and request that it be re-sent (in the case of the Transmission Control Protocol (“TCP”).

- Broadband networks are highly resilient and reliable because they are *redundant*. Redundancy is key to minimizing any single point of failure and avoiding sudden disruptions of Internet traffic flows. The modern broadband network contains a host of redundancies in its architecture to avoid outages, such as redundant fiber rings and optical node receivers.⁷ As discussed in more detail in Subpart B, virtually every element in Comcast’s broadband network upstream from the Cable Modem Termination System (“CMTS”) contains redundancies.
- Broadband networks are *self-healing*. They are designed to limit and contain harm both at the core and at the edge of the network.⁸ When they face physical damage or severe overload conditions, the network frequently is capable of fixing itself through a variety of means, including dynamic routing, backup power, and multiple access points to reach fiber and other facilities. As NCTA has explained, cable broadband networks have “the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.”⁹

While each broadband network is unique, they all share these key qualities, making them well-equipped to mitigate customer impact if and when outages occur.

The fact that broadband networks are innately strong and flexible does not mean that network providers can rest on their laurels. To the contrary, the communications industry has invested hundreds of billions of dollars to build state-of-the-art broadband networks that are innovative and durable.¹⁰ Indeed, since the Internet’s inception, stakeholders from all segments of the government and economy have worked in collaboration with each other to ensure the

⁶ See Comments of the Nat’l Cable & Telecomms. Ass’n, PS Docket No. 10-92, at 2 (June 25, 2010) (“NCTA NOI Comments”).

⁷ See *id.* at 2.

⁸ See *id.* at 5.

⁹ See *id.* at 2 (quoting U.S. Gov’t Accountability Office, *Critical Infrastructure Protection, Update to National Infrastructure Plan Includes Increased Emphasis on Risk Management and Resilience*, at 4, GAO-10-296 (Mar. 2010)).

¹⁰ See FCC, *Connecting America: The National Broadband Plan*, at xi (Mar. 16, 2010) (“Fueled primarily by private sector investment, and innovation, the American broadband ecosystem has evolved rapidly.”); Comcast NOI Comments at 2 n.4 (citing same).

survivability of the network of networks that comprise the Internet. The structural features and capabilities built into this ecosystem reflect years of risk assessment, analysis, and deployment of best practices by Internet engineers. Moreover, Comcast and other providers continue to undertake additional efforts to update their networks with even more advanced and more effective safeguards that will provide yet greater network resiliency going forward while simultaneously adding bandwidth.¹¹

Finally, contrary to implications in the Further Notice, there is nothing about a broadband network's architecture that makes it more likely to jeopardize 911 services than a legacy network. The Commission's suggestion that Next Generation 911 ("NG911") "sunny day" outages are indicative of broadband networks being inherently less reliable or more vulnerable to catastrophic failures is inaccurate.¹² The outages the Commission cites had nothing to do with mass-market, consumer-grade Internet access. Rather, the Further Notice incorrectly conflates the transition to IP-based NG911 – which relies on engineered, managed networks – with data transmitted over BIAS to end users.¹³ While the type of NG911 outages discussed in the Further Notice represents an important public safety problem, it is one that is separate from, and that will not benefit from, broadband network outage reporting.

¹¹ See, e.g., Mark Muehl, *Building a Smarter Network with OpenStack*, Comcast Voices (May 4, 2016), <http://corporate.comcast.com/comcast-voices/building-a-smarter-network-with-openstack> (announcing that Comcast's new platform, Comcast Elastic Cloud, will use Open Stack and enable the company to "deliver services to customers and architect our network to be not just bigger and faster, but smarter").

¹² See FNPRM ¶¶ 103-104 & nn.313-314.

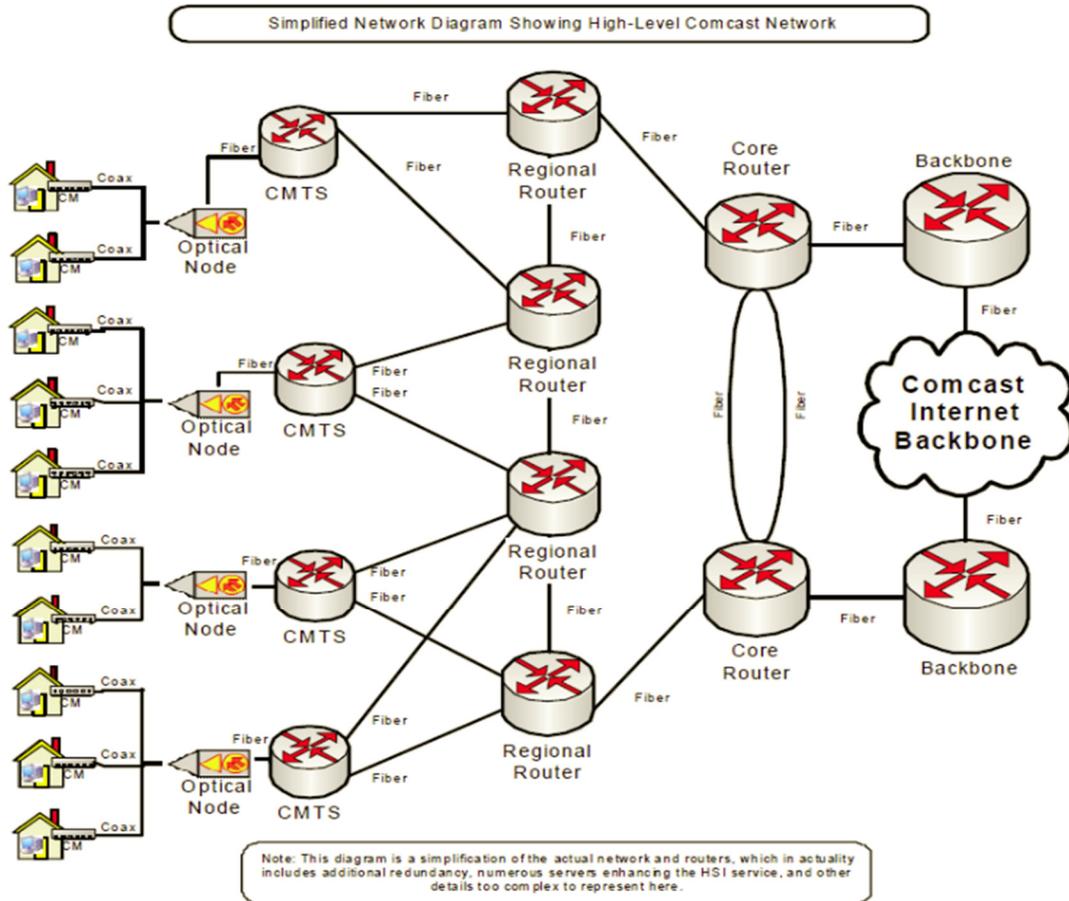
¹³ In fact, Emergency Services IP Networks ("ESInets") that provide NG911 are distinct from the public Internet and "must be designed to meet more stringent requirements for security and reliability service levels than most other IP networks." See NENA Emergency Services IP Network Design for NG9-1-1, NENA 08-506, Version 1, at 13 (Dec. 14, 2011), https://c.ymedn.com/sites/www.nena.org/resource/collection/2851C951-69FF-40F0-A6B8-36A714CB085D/NENA_08-506_Emergency_Services_IP_Network_Design_12142011.pdf.

B. Comcast's BIAS Network Is Dynamic and Capable of Preventing or Efficiently Mitigating Most Consumer-Facing Outages.

Comcast's network is designed to minimize single points of failure. When failures do occur, the network often is able to fix itself and reroute or take other actions so that the "failure" never results in customer-impacting disruptions. Comcast also takes other actions to guard against outages, such as ensuring there is sufficient backup power.

Comcast's Broadband Network is Highly Redundant and Has Few Single Points of Failure. As Comcast explained to the Commission in 2010, by building active redundancy into the network, Comcast is able to guard against virtually any unexpected failure of part of the network.¹⁴ Comcast's systemic redundancies exist at virtually every part of the network, which is organized as follows:

¹⁴ See generally Comcast NOI Comments.



The local portion of Comcast’s DOCSIS-based broadband network is a hybrid fiber-coax network, with coaxial cable generally connecting each customer’s cable modem (or other equipment) to the customer’s local neighborhood optical node,¹⁵ which is connected by fiber optic cables to a CMTS, which in turn connects to a regional network, and from there to the Internet backbone. As traffic moves away from customers’ homes, the redundancy of Comcast’s network increases. Each of Comcast’s more than 2,500 CMTS devices has routers with multiple ports that handle traffic coming from and going to various optical nodes. Routers at each CMTS are connected by fiber links into at least two different regional routers (or, occasionally, different

¹⁵ Comcast also has some customers who have direct fiber connections.

cards on the same router) located in the regional network. If any single router or card fails, traffic is automatically rerouted around the failed router or card.

The regional networks are generally built around a central fiber ring with at least two core routers. Each of these regional routers also is connected to a further string of routers by at least two independent fiber connections (*i.e.*, each router is “dual-homed” to the string of routers). The string of routers itself is dual-homed to the core routers, which are dual-homed to the backbone network. This design builds significant redundancy into the network. Thus, if one fiber link goes down, the traffic is simply rerouted over one of the other links. As in any network, however, there inevitably are points of failure for which redundancy is impractical, *e.g.*, the last mile. That is true of the local wires that connect subscribers to the CMTS, and it is also true of the CMTS itself, though some CMTS functions and interfaces are internally redundant. Because a CMTS is the aggregation point for traffic to and from optical nodes, a complete CMTS failure will affect the traffic for the optical nodes it serves and the customers served by those optical nodes. Taking this fact into account, Comcast has invested in high availability CMTS infrastructure to reduce the probability of customer impact. For example, each CMTS has multiple cards and ports that can serve as backups to one another. Other aspects of the high availability infrastructure include redundant power and cooling, uninterruptible power supply (“UPS”)/generator backup, redundant processors, and redundant network uplinks. To prevent CMTS failures, Comcast regularly tests and monitors CMTS performance, and upgrades or replaces CMTS devices as needed.

The Network Is Adaptive. Fiber and wire cuts, downed links, malfunctioning routers and switches, and similar network segment disruptions are events that any network operator must deal with in the normal course of business. Because Comcast’s broadband network is adaptive

and designed to route around any potential failure in the network upstream of the CMTS, however, such issues rarely impact Comcast's end users. Comcast also strives to find new ways to make all levels of its BIAS network more adaptive. For example, Comcast now relies on IP Anycast technology to access Domain Name System ("DNS") servers. Among other benefits, this technology allows a single, essentially virtual IP address to be shared across a large number of servers in a wide variety of locations.¹⁶ If and when one server – or even an entire data center – fails, the customer is routed seamlessly to the next best server or data center without disruption to her services.

In addition, Comcast's facilities are built to withstand extreme environmental conditions such as floods, hurricanes, and snowstorms – and when such events occur, Comcast often makes frequent and detailed reports to the FCC and Department of Homeland Security ("DHS") as part of the Commission's Disaster Information Reporting Service ("DIRS"). In addition, Comcast has almost completed the migration of its voice service to a next-generation IP Multimedia Subsystem ("IMS") architecture that is based on Packet Cable 2.0 standards. This new architecture increases network resiliency significantly because each IMS location has the capability to support up to six million lines (residential and enterprise).¹⁷ Similarly, customers still using soft switch technology benefit from an extensive voice switch recovery site.

¹⁶ Comcast added the IP Anycast capability for DNS to its network in order to protect against service disruptions, particularly the loss of one or more data centers where DNS servers are located. As the FNPRM notes, Comcast did experience a disruption on the west coast in 2015 related to DNS server overload. In the wake of that event, Comcast significantly increased the number of DNS servers and data center server sites to prevent this type of event from reoccurring. This type of design work is ongoing: Comcast regularly adds capacity via software upgrades and/or optimization, additional servers, additional DNS server sites, and other DNS design optimizations.

¹⁷ IMS locations are geographically diverse. Each site is redundant within itself and able to load share between one another in the event of a failure.

Finally, in the case of power loss to its facilities, Comcast has installed backup batteries and, in many cases, additional backup generators as well. (All voice-supporting headends, for example, have both battery backup and generator capabilities.)

III. THE DEFINITION OF A REPORTABLE OUTAGE SHOULD BE STRAIGHTFORWARD, CONSISTENT, AND MEANINGFUL.

If the Commission decides to extend outage reporting obligations to BIAS, those requirements should be easy to administer and designed to ensure that only outages that have a meaningful impact on consumers must be reported. As explained below, Comcast believes that these criteria militate in favor of extending the outage reporting regime that currently applies to VoIP to BIAS (and against expanding the obligations that apply to VoIP providers today). Pursuant to this system, only customer-impacting, “hard down” outages that satisfy the current VoIP reporting threshold of user minutes should be reportable. Furthermore, the use of other performance degradation metrics to determine reportable events would be needlessly burdensome and complicated (assuming such metrics could even be meaningfully crafted), require filings for incidents that had no material adverse effect on consumers, and fail to provide the Commission with any meaningful insights into the resiliency of critical network functions. The Commission likewise should reject the use of a throughput-based metric to identify reportable outages, which would be difficult or impossible to administer, and would improperly assign less importance to outages that affect lower-bandwidth consumers.

A. Reporting Should Be Required Only for “Hard Down” Outages That Significantly Impact BIAS or VoIP Customers.

To the extent the Commission extends outage reporting obligations to BIAS providers, it must do so in a manner that balances the agency’s desire to obtain useful outage information with the goal of minimizing administrative burdens on agency staff and service providers. The Commission similarly must weigh those considerations as it considers proposals to expand the

scope of the outage reporting requirements that currently apply to VoIP providers. Requiring parties to file outage reports only when a network suffers a “hard down,” customer-affecting outage strikes the appropriate balance by ensuring that the Commission receives reports regarding any significant disruptions affecting consumers without inundating the agency with worthless information.¹⁸

As an initial matter, limiting reportable events to “hard down” outages comports with the Commission’s stated aim of addressing network reliability concerns that may interrupt access to emergency response services and business connectivity.¹⁹ As explained below, use of the proposed service degradation metrics would provide the Commission with information about network events that may have no impact on the customer at all, much less an impact that would impede access to 911. As AT&T correctly asserted in a related past proceeding, a “hard down” standard would “provide[] the Commission with real *outage* data as opposed to flooding the Commission with useless . . . quality of service information.”²⁰

¹⁸ In the proceeding that resulted in the current VoIP outage rules, there was widespread support for a “hard down” outage reporting trigger. *See, e.g.*, Reply Comments of Sprint Nextel Corp., PS Docket No. 11-82, at 6 (Oct. 7, 2011) (“Sprint agrees with other commenters that argue outage reports should only be required when there is a total loss of service.”); Comments of Am. Cable Ass’n, PS Docket No. 11-82, at 10 (Aug. 8, 2011) (“[I]f the Commission imposes outage reporting . . . it should employ a standard that is based on a measure of whether a provider’s customers have a functioning connection to the Internet or not.”); Comments of CenturyLink, PS Docket No. 11-82, at 6 (Aug. 8, 2011) (The “definition of an . . . outage must be limited to the complete loss of service or connectivity.”); Comments of T-Mobile USA, Inc., PS Docket No. 11-82, at 12 (Aug. 8, 2011) (“[A]ny new outage reporting regime . . . should be limited to actual outages within the control of the covered provider.”); Comments of Time Warner Cable Inc., PS Docket No. 11-82, at 5 (Aug. 8, 2011) (“[P]roviders should be required only to report ‘outages’ that consist of actual losses of service meeting the relevant time and user thresholds, not attributes that amount to measures of *service quality*.”).

¹⁹ *See* FNPRM ¶ 159. Importantly, service disruptions potentially affecting 911 Public Service Access Points are already subject to specific outage reporting requirements. *See, e.g.*, 47 C.F.R. §§ 4.9(e)(5), (f)(4), (g)(1).

²⁰ Comments of AT&T Inc., PS Docket No. 11-82, at 24 (Aug. 8, 2011).

Adoption of this straightforward reporting standard also would “promote[] consistent outage reporting” and therefore “facilitate accurate analysis” of the data contained in providers’ reports.²¹ For example, the Commission would be able to assess the frequency of “sunny day” outages relative to those caused by environmental factors across an evolving array of technologies.²² Indeed, the “hard down” measure is the “only approach that w[ould] enable the Commission to accurately capture outages across the ever-changing variety of IP and telecommunications networks.”²³

Finally, use of a “hard down,” customer-impacting outage trigger would be less burdensome for all parties involved. As Vonage has noted, this “tailored approach would avoid the heavy burden represented by [quality of service] reporting while also conserving scarce resources.”²⁴ Conversely, a less efficient, more expansive reporting trigger would “impose significant, unnecessary costs on the industry . . . [and be] inconsistent with the Administration’s policy goals of regulatory flexibility, simplification of reporting and compliance requirements, and reducing regulatory burdens on businesses.”²⁵

²¹ R&O ¶ 36.

²² See FNPRM ¶ 103.

²³ Comments of Vonage Holdings Corp., PS Docket No. 11-82, at 11 (Aug. 8, 2011).

²⁴ *Id.* at 8.

²⁵ Letter from Am. Cable Ass’n, AT&T, CenturyLink, Comcast Corp., COMPTTEL, CTIA – The Wireless Ass’n, Frontier, Indep. Tel. & Telecomms. Alliance, Level 3 Commc’ns, LLC, Nat’l Cable & Telecomms. Ass’n, Sprint Nextel, Time Warner Cable, T-Mobile USA, U.S. Internet Serv. Provider Ass’n, US Telecom, Verizon, VON Coalition, Windstream, and XO Commc’ns, to James Arden Barnett, Jr., Rear Admiral (Ret.), Chief, Pub. Safety and Homeland Sec. Bureau, FCC, PS Docket No. 11-82, at 2 (Nov. 14, 2011).

B. A Performance Degradation Standard Does Not Make Sense, Would Be Overly Burdensome, and Would Not Provide Useful Information to the Commission.

In the Further Notice, the Commission proposes defining reportable outages to include cases of significant degradation and proposes a “series of metrics and thresholds” it believes could identify “outages” caused by such performance degradation.²⁶ The Commission should abandon these tentative proposals.

As an initial matter, the proposed metrics would lead to outage reporting for network events that do not adversely impact consumers, much less prevent them from using critical communications during an emergency. Reporting performance degradation also would provide no valuable insight to the Commission with respect to public safety or critical functions. Degradation that falls well short of a “hard down” outage – whether measured through latency, packet loss, throughput, or any other metric – simply does not affect critical 911 functions. Importantly, 911 calls made over an IP-based network can still be completed regardless of the ebb and flow of latency and packet loss.

Even if reporting on performance degradation would provide meaningful information to the Commission, trying to craft a useful metric would prove difficult, if not impossible. Packet loss and latency, for example, are not indicators of an outage. Many well-designed applications, services, and protocols have the ability to absorb levels of degradation. Indeed, some packet loss can actually *improve* the customer experience, as demonstrated by studies of bufferbloat and Active Queue Management (“AQM”).²⁷ This is because, under normal network conditions,

²⁶ See FNPRM ¶¶ 133-144.

²⁷ See, e.g., Greg White, *Active Queue Management Algorithms for DOCSIS 3.0*, CableLabs §§ 1.3, 1.4, 2-5 (Apr. 2013), http://www.cablelabs.com/wp-content/uploads/2013/11/Active_Queue_Management_Algorithms_DOCSIS_3_0.pdf (discussing how AQM techniques/packet drop decisions can alleviate bufferbloat-driven latency).

some packet loss allows interactive and/or latency-sensitive traffic to flow more quickly. For example, if Comcast were to configure or optimize its network for minimal or zero packet loss, then packets for a best efforts interactive application like an online game could get stuck behind large email attachments or file transfers that are not as time-sensitive. In some scenarios, this may even impair the quality of over-the-top VoIP and other real-time communication applications. By allowing some packet loss to the email attachment, the network can effectuate better real-time communication without creating discernible latency problems for the email packets. Through this flexible back-and-forth, the network maximizes throughput and minimizes delay. Thus, attempting to measure “degradation” in terms of government-imposed standards for acceptable packet loss, latency, or throughput would dampen or perhaps even functionally prohibit technical and engineering safeguards that actually make the network and applications that use the network perform better and create a better user experience.

In addition, the Internet community continues to invest in significant research, standardization work, and best practices development through organizations such as the Internet Research Task Force and Internet Engineering Task Force on the concepts of packet loss, AQM, and various forms of congestion control or marking, illustrating that this area is far from technically settled or mature enough for regulatory standards.²⁸

Furthermore, there is no apparent reason why the Commission needs to gather any information about latency and packet loss beyond that which it obtains via the Measuring

²⁸ In fact, the National Science Foundation and the Commission jointly held a Quality of Experience (“QoE”) Measurement Workshop in 2015 to debate what factors even impact end-user QoE. *Workshop on Tracking Quality of Experience in the Internet*, National Science Foundation and the Federal Communications Commission, Princeton, NJ, Oct. 21-22, 2015, <http://aqualab.cs.northwestern.edu/conference/276#program>.

Broadband America (“MBA”) program.²⁹ The MBA program already measures average latency and packet loss for each of the major BIAS providers.³⁰ Unsurprisingly, these reports call into question the use of these metrics in the outage reporting context. For example, the most recent MBA Report notes that “the differences in average latencies among terrestrial-based broadband services are small, and are unlikely to affect the perceived quality of [phone calls over the Internet].”³¹ With regard to packet loss, that same report finds that, although “[p]acket loss may directly affect the perceived quality of applications that do not request retransmission of lost packets, such as phone calls over the Internet[,] . . . packet losses of a few tenths of a percent are sufficiently small so that they are unlikely to significantly affect the perceived quality of [calls over the Internet].”³² Given these findings, there is even less reason for the FCC to impose performance degradation reporting obligations on BIAS or VoIP providers.

A throughput-based metric would fare no better as a performance degradation measurement tool.³³ A reportable outage threshold based on the drop of throughput below “normal” levels would vary as networks increase throughput, constantly shifting the benchmark for what constitutes “normal.” As a result, this type of benchmark would be nearly impossible to

²⁹ In its recent Notice of Inquiry regarding expanding the 706 broadband deployment inquiry, the Commission asks about expanding latency reporting, including via the MBA program. Setting aside the need for or feasibility of those particular proposals, these issues clearly more properly belong in that proceeding than in this network outage rulemaking. *See Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, Twelfth Broadband Progress Notice of Inquiry, FCC 16-100, ¶ 68 (Aug. 2, 2016).

³⁰ *See* FCC Office of Eng’g & Tech. & Consumer & Governmental Affairs Bureau, 2015 Measuring Broadband America – Fixed Broadband Report, at 17-19 (Dec. 30, 2015), <http://data.fcc.gov/download/measuring-broadband-america/2015/2015-Fixed-Measuring-Broadband-America-Report.pdf> (“2015 MBA Report”).

³¹ *Id.* at 18.

³² *Id.* at 19. The Report shows that Comcast’s average packet loss is barely above 0.1 percent. *Id.*

³³ *See* FNPRM ¶ 138.

administer on a going-forward basis. More problematic still, such a requirement would essentially penalize providers for upgrading throughput in advance of need, because any carrier that expands its capacity would then be responsible for maintaining the same percentage of a larger absolute capacity.

Finally, performance degradation reporting would impose substantial burdens and costs on providers that cannot be justified under cost-benefit analysis.³⁴ The rules on “hard down” outage reporting alone will increase costs significantly. But if BIAS and VoIP providers must report performance degradation as well, the costs would be even more substantial, especially if such performance degradation is measured on an end-to-end basis all the way to end users.

Because monitoring capabilities for these performance metrics are not built into cable modems today, both software and hardware would have to be replaced in every home. The devices themselves would become more costly. If providers were required to upgrade equipment today rather than at the end of the natural life cycle of the devices in question, costs would include the lost use of perfectly functional devices in favor of new, more expensive devices, labor, recycling, and administrative costs, as well as the many years this change would take to implement.³⁵

³⁴ See *id.* ¶ 94 & n.283 (seeking comment on potential costs and benefits associated with the proposals in the Further Notice).

³⁵ Verizon and Verizon Wireless provided an assessment of these costs to their network in 2011. See Comments of Verizon & Verizon Wireless, PS Docket No. 11-82, at 21-22 (Aug. 8, 2011) (“[A]dopting quality of service thresholds would impose considerable costs on providers as providers would have to install probes throughout their entire network to run these tests every five minutes, which themselves could cause network congestion. Even though Verizon has significant visibility into its broadband networks today and employs tools that test certain network functionality for its interconnected VoIP customers in frequent intervals, Verizon does not have probes in place today that can measure jitter, latency, and packet loss throughout its networks. Verizon estimates that installing these probes on every router could take over two years and would cost over \$75,000 per site, with a total cost well above \$100,000,000. These resources could be better used elsewhere, including efforts to upgrade Verizon’s networks or for future broadband deployment.”).

Notably, more limited performance degradation monitoring requirements also would prove excessively costly. Even if the performance degradation monitoring were to take place at the most highly aggregated level – at the backbone layer – Comcast estimates that it could cost millions of dollars to initially acquire and install the necessary monitoring equipment. Put simply, imposing such degradation monitoring equipment would increase Comcast’s cost of providing service to consumers, who would see no improvements whatsoever in their network or user experience.

In sum, performance degradation reporting is not only unnecessary, but also infeasible. This type of reporting would impose enormous costs on the industry and consumers while providing no useful information to the Commission, much less resulting in any concrete public benefits. Indeed, the metrics that the Commission suggests would not inform any performance degradation analysis at all, as these metrics would shed no light on whether critical services are being affected.

C. The Commission Should Apply the Current VoIP Reportable Outage Threshold If It Extends Reporting Obligations to BIAS Providers.

VoIP providers currently are required to report outages that potentially affect 900,000 user minutes and last at least 30 minutes.³⁶ Comcast favors continued use of this threshold for VoIP providers and recommends use of the same threshold if the Commission decides to extend outage reporting obligations to BIAS providers. A single, uniform reporting standard based on consumer impact is simpler and more equitable than the Commission’s proposal tied to the amount of bandwidth affected by a disruption. Moreover, given that the same events may sometimes give rise to both VoIP and broadband outages, it makes sense as an administrative

³⁶ 47 C.F.R. § 4.9(g).

matter to have a consistent reporting standard (though, as discussed below, two separate reports are warranted even when the same event leads to both a VoIP and BIAS outage).

In particular, the Commission proposes that a BIAS “outage event would become reportable when it resulted in 1 Gbps of throughput affected in which the event exceeds 22,500 Gbps user minutes.”³⁷ Using this type of metric would necessarily and inappropriately assign less importance to service disruptions affecting consumers subscribing to lower-bandwidth service, since 25 Mbps is pre-determined to be the baseline bandwidth input for this throughput calculation.³⁸ In contrast, an outage measured not in throughput user minutes but simply in user minutes would treat a user with a 10 Mbps connection, such as those who subscribe to Comcast’s Internet Essentials program, on equal footing with a user with a 100 Mbps or a 2 Gbps connection. The Commission’s overriding concern in establishing a BIAS reporting threshold should be the magnitude of the consumer impact, not the speed of the consumer’s BIAS connection.

Similarly, there is no basis for adopting a 1 Gbps throughput metric for interconnected VoIP offerings.³⁹ The Commission appears to assume, without explanation, that 25 Mbps is the standard connection speed required to place a voice call.⁴⁰ There is no basis in the record for this conclusion. To the contrary, the FCC’s Broadband Speed Guide notes that less than 0.5 Mbps is

³⁷ FNPRM ¶ 130.

³⁸ *Id.* ¶ 129. Comcast has suggested the use of a bandwidth-based metric for determining reportable outages affecting major transport facilities. *See* Comments of Comcast Corp., PS Docket No. 15-80, at 6 (July 16, 2015). Those outages, however, only involve high-capacity transmission links, not services that are directly user-facing. For Comcast, these links typically connect cell towers to Comcast’s network or are used for Ethernet transport. In those contexts, a reporting threshold based on bandwidth makes more sense than one based on user minutes.

³⁹ FNPRM ¶ 166.

⁴⁰ *Id.* at n.362.

needed to support a VoIP call.⁴¹ By adopting a throughput-based metric for VoIP, the Commission would no longer be able to monitor accurately whether a VoIP outage has impacted end users. Moreover, throughput rises rapidly each year, meaning that any measurement adopted into the rules would quickly become outdated.

In addition, the Commission's proposed approach raises a variety of implementation and administrative issues. For example, a bandwidth-based metric would require a BIAS provider to have an integrated system capable of monitoring, in real time, the size of the pipe and speeds that are provisioned to each and every end user, as well as the health of every dynamic connection. Further, as user speeds increase, BIAS providers would be forced to file reports about an increasing number of reportable events, even as the number of customers actually affected by each event declined. In turn, the Commission would begin to receive an ever-more expansive torrent of outage filings that would not prove helpful for increasing awareness of network resiliency.

In short, use of the existing 900,000 user minute threshold (for outages lasting at least 30 minutes in duration) would "better capture . . . the number of subscribers impacted" relative to the proposed throughput-based metric.⁴² Additionally, experience already has shown that this reporting threshold is workable for IP-based voice service. There is no reason to believe that it would prove infeasible or unduly burdensome if it were applied to other packet-based services.

⁴¹ Broadband Speed Guide, FCC, <https://www.fcc.gov/reports-research/guides/broadband-speed-guide> (last visited Aug. 26, 2016).

⁴² FNPRM ¶ 131.

IV. DEDICATED SERVICES SHOULD BE BEYOND THE SCOPE OF ANY NEW OUTAGE REPORTING RULES ADOPTED IN THIS PROCEEDING.

In the Further Notice, the Commission expresses its belief that “the public safety goals to be accomplished through Part 4 . . . can best be advanced” by extending the outage reporting requirements to all dedicated services.⁴³ While Comcast supports the Commission’s public safety goals, the Commission need not impose new outage reporting obligations on providers of dedicated services that are not already subject to such requirements.⁴⁴ The Commission’s previously articulated concern that outage reporting obligations are needed because “individual providers do not always take steps within their own operations to address reliability problems” simply does not apply to these dedicated services.⁴⁵

The Commission’s proposed definition of “dedicated services” makes clear that these offerings are typified by “prescribed performance requirements that include bandwidth, latency, or error-rate guarantees or other parameters that define delivery under a Tariff or in a service-level agreement.”⁴⁶ For example, certain Comcast business data services are offered with a variety of performance metrics and assurances, including contractual performance objectives.⁴⁷ The record of the Commission’s business data services proceeding is replete with additional examples of the types of service level agreements (“SLAs”) offered by providers today.⁴⁸

⁴³ *Id.* ¶ 109.

⁴⁴ Some dedicated transport services (namely, DS3 services) are currently subject to outage reporting obligations. *See* 47 C.F.R. § 4.9(f)(2).

⁴⁵ *Proposed Extension of Part 4 of the Commission’s Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers*, Report & Order, 27 FCC Rcd. 2650 ¶ 35 (2012) (“2012 R&O”).

⁴⁶ FNPRM ¶ 115.

⁴⁷ *See* Letter from Matthew A. Brill, Counsel for Comcast Corp., to Marlene H. Dortch, FCC Secretary, WC Docket No. 05-25 (Mar. 25, 2016).

⁴⁸ *See, e.g.*, Comments of Windstream Servs., LLC, WC Docket No. 05-25, RM-10593, at 13-17 (Jan. 27, 2016) (refiled Apr. 20, 2016) (noting that: (a) Verizon’s “Ethernet Dedicated E-Line +” service

In addition to guaranteeing high levels of network performance, these SLAs require providers to quickly remedy service degradations when they occur. For example, Verizon commits to a mean time-to-repair as brief as two hours, while XO includes a four-hour interval for its MPLS offering.⁴⁹ Customers of dedicated business offerings also typically demand and receive enforcement remedies (*e.g.*, financial penalties) that apply when providers fail to meet the established network reliability performance criteria, thereby creating strong economic incentives for providers to deliver service that meets the negotiated reliability guarantees contained in their respective SLAs.⁵⁰ Indeed, these types of contractual provisions are hallmarks that distinguish dedicated business services from other offerings, such as best efforts Internet services.

Despite these contractual guarantees that are designed to ensure network reliability, the Commission proposes reporting requirements that would force a provider to file up to three

provides a service availability standard of up to 99.999 percent, 99.995 percent service level of packet delivery, and frame jitter under 5 milliseconds; (b) AT&T offers business data services that can include a 99.995 percent packet delivery rate, latency of under 5 milliseconds, and jitter of under 3 milliseconds; and (c) Level 3 offers an MPLS IP virtual private network service that includes a packet delivery rate of 99.99 percent, jitter of under 3 milliseconds, and latency of 50 milliseconds); Letter from Level 3 Commc'ns, LLC and EarthLink, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 05-25, at 2 (Apr. 14, 2016) (“Ethernet-over-fiber and Ethernet-over-legacy loop services are typically offered subject to service level agreements . . . under which the service provider commits to jitter levels low enough to support real-time applications, such as video and voice applications. These SLAs typically require that the service provider pay penalties to customers if the service provider fails to meet the jitter commitment.”).

⁴⁹ See Verizon, Verizon Ethernet Dedicated E-Line +, at 2 (2014), http://www.verizonenterprise.com/external/service_guide/reg/cp_edeline_plus_sla.pdf; XO, XO Wide Area Network Services, Service Level Agreements and Associated Credits, at 2 (2012), <http://www.xo.com/WorkArea/DownloadAsset.aspx?id=10737418812>.

⁵⁰ See Comments of Windstream Servs., LLC, WC Docket Nos. 16-143, 05-25 & RM-10593, at 26-27 (June 28, 2016) (discussing how “high-level performance characteristics . . . commonly are enforced through Service Level Agreements . . . that impose financial penalties on a provider if the guaranteed performance levels are not met”); Comments of Birch, EarthLink, and Level 3, WC Docket Nos. 16-143, 15-247, 05-25 & RM-10593, at 67 (June 28, 2016) (“[M]ost PBDS providers offer services subject to service quality levels, memorialized in SLAs with different performance criteria.”).

outage reports *after* it has fully resolved an issue. In support of this proposal, the Further Notice fails to provide even anecdotal evidence regarding problems with outages for packet-based dedicated business services. This absence of evidence underscores the fact that additional reporting obligations for dedicated business services are unnecessary. Put simply, no purpose would be served by imposing new, unnecessary government reporting obligations that will have no effect on the quality of service that dedicated services customers will continue to demand and receive.

V. THE COMMISSION SHOULD ADOPT THE CURRENT TWO-STEP PROCESS FOR ANY AND ALL OUTAGE REPORTING OBLIGATIONS IMPOSED ON IP-BASED SERVICES.

Today, interconnected VoIP providers are subject to a two-step outage reporting process that requires them to file a notification with the Commission within 24 hours of discovering a reportable outage, followed by a final report within 30 days.⁵¹ In the Further Notice, the Commission seeks comment on whether to require all providers subject to the outage reporting rules, including providers of VoIP and BIAS, to comply with the more onerous three-step process that currently applies to other types of service.⁵² Most notably, this process would require providers to file a notification with the Commission within 120 minutes of discovering a reportable outage.⁵³ The Commission should reject this misguided proposal and instead use the current two-step process for reportable outages that affect VoIP and any other IP-based services subjected to such reporting obligations.

⁵¹ See 47 C.F.R. § 4.9(g).

⁵² See FNPRM ¶ 121.

⁵³ *Id.* In addition to filing a notification, providers would be required to file a report within 72 hours of discovering the reportable outage and a final report within 30 days of discovering the outage. *Id.*

As an initial matter, the proposal to extend the three-report requirement to VoIP and other IP-based services appears to be based on an incorrect premise. Specifically, the Commission seems to assume that requiring an initial notification within 120 minutes would give the agency greater “visibility into . . . outages” and enhance “its ability to take appropriate remedial action.”⁵⁴ This assumption ignores the fact that IP-based networks are more technically complex and resilient than the hierarchical, TDM-based networks for which the three-step reporting requirements were designed. As the Voice on the Net Coalition has noted, the existing three-step outage reporting system was “built for an industry where a failure would originate from infrastructure collapse, making it possible to determine the location and cause quickly.”⁵⁵

Determining the cause of an outage that affects an IP-based network, however, is far more challenging and time-consuming. In fact, in many situations, a BIAS provider will still be performing initial troubleshooting after 120 minutes. Pausing in order to report to the FCC could extend the mean time-to-repair, and information provided during that initial report may well be incorrect or contradicted later due to the nature of complex IP network troubleshooting. Indeed, such troubleshooting can involve extensive and detailed packet capture analysis or other extremely detailed and time-consuming research that is unlikely to be completed within two hours. As Time Warner Cable has indicated, “[r]equiring providers to submit reports within two hours of an outage can result in the diversion of resources away from the key priority of restoring service.”⁵⁶ In adopting the two-step process for VoIP outages, the Commission similarly

⁵⁴ *Id.* ¶ 162.

⁵⁵ Comments of Voice on the Net Coalition, PS Docket No. 11-82, at 10 (Aug. 8, 2011).

⁵⁶ Comments of Time Warner Cable Inc., PS Docket No. 11-82, at 6 (Aug. 8, 2011); *see also, e.g.*, Comments of Nat’l Cable & Telecomms. Ass’n, PS Docket No. 11-82, at 8 (Aug. 8, 2011) (“If there is time urgency associated with outages on the network, it is the urgent need of the interconnected VoIP

concluded that this approach would allow “more time for interconnected VoIP service providers to work the outage problem as opposed to reporting on the outage.”⁵⁷ In short, requiring the initial report within a two-hour period would add unnecessary cost and complexity without any reasonable promise of greater clarity in reporting to the Commission.

Comcast’s experience in reporting VoIP outages under the current rules aptly illustrates this point. The company has devoted thousands of hours and millions of dollars to the development and deployment of an extensive, sophisticated system for identifying outages and quickly restoring service. Nonetheless, Comcast frequently cannot verify whether a service disruption was a reportable event within 24 hours. Given this uncertainty, Comcast often files an outage notification within 24 hours, only to withdraw the filing when it subsequently determines that the disruption did not reach reportable levels. Indeed, Comcast estimates that up to *fifty percent* of its notifications are withdrawn under the current system. To chop the initial notification period from 24 hours to two hours for IP-based service outages would dramatically increase both this percentage and the overall number of reports filed with the Commission for events that turn out to be non-reportable disruptions, thereby inundating the Commission with filings that contain no useful information. No public interest goal would be served by such a reporting requirement.

By contrast, maintaining the current procedure for reportable IP-based outages would permit Comcast and other providers to focus their resources solely on addressing the cause of the outage and restoring service during the initial hours after discovery. In addition, continuing to allow IP-based providers to file initial notifications within 24 hours would facilitate service

provider to *fix* the problem – a task that will only be hampered by diverting resources and attention to reporting obligations.”).

⁵⁷ 2012 R&O ¶ 95.

providers' ability to report more accurate and complete data, thereby fulfilling the FCC's goal of "provid[ing] the Commission with the information it needs while reducing the reporting burden on the providers."⁵⁸

In light of these considerations, there can be no serious doubt that the three-part outage reporting system simply is "not a good model" for IP-based services.⁵⁹ Accordingly, to the extent the Commission wishes to adopt a single outage reporting process,⁶⁰ it should eliminate this more burdensome process entirely and instead require *all* providers to file a notification within 24 hours and a final report within 30 days.⁶¹ There is broad support in the record for this approach. As AT&T has noted, "two general themes [from prior submissions] are clear: (1) the reporting deadlines need adjustment because they are unrealistic and (2) there are too many reports."⁶² By applying the two-step VoIP outage reporting regime to all providers subject to these obligations, the Commission ultimately "will improve the quality of outage reporting data

⁵⁸ *Id.* ¶ 101.

⁵⁹ Comments of Verizon & Verizon Wireless, PS Docket No. 11-82, at 10 (Aug. 8, 2011).

⁶⁰ *See* FNPRM ¶ 127 (seeking comment on "whether all reporting . . . should be adjusted to a two-step process").

⁶¹ *See* 47 C.F.R. § 4.9(g).

⁶² Reply Comments of AT&T Inc., PS Docket No. 11-82, at 4 (Oct. 7, 2011); *see also, e.g.*, Comments of Alliance for Telecomms. Indus. Solutions, PS Docket No. 15-80, at 4 (July 16, 2015) ("ATIS NRSC recommends that: (1) the deadline for notifications, other than those for outages to 911 special facilities, should be extended from 240 minutes to 24 hours, similar to the existing reporting requirements for interconnected VoIP providers; and (2) the requirement that service providers submit initial reports within 72 hours of the discovery of an outage should be eliminated."); Comments of Sprint Corp., PS Docket No. 15-80, at 5 (July 16, 2015) ("[T]he Commission should consider modifying the reporting timeframes for cable, wireline and wireless providers to make them consistent with those of interconnected Voice over Internet Protocol . . . providers."); Comments of AT&T Inc., PS Docket No. 11-82, at 21 (Aug. 8, 2011) ("The 120-minute notification requirement is unnecessarily burdensome and disruptive.").

submitted to the Commission and standardize rules across providers, all of which benefits the public interest.”⁶³

Finally, adoption of a uniform outage reporting system for all services will improve the Commission’s ability to compare the “reliability and resiliency” of various services, provided it requires each service to report disruptions separately. For example, if the Commission adopts outage reporting obligations for BIAS, providers should be required to file separate reports for BIAS outages and disruptions affecting other IP-based offerings, such as VoIP. Although VoIP and BIAS applications both are provided over IP-based networks, these networks are designed so that each service can operate independently of the other. Consequently, a reportable outage affecting one service does not mean that the other service also suffered a reportable disruption. Maintaining separate reports for distinct services will provide the Commission with more granular data that accurately reflects the frequency and magnitude of the outages affecting each offering.

VI. THE COMMISSION SHOULD AFFORD STRINGENT CONFIDENTIALITY PROTECTIONS TO OUTAGE REPORTS.

A. Outage Reports Must Be Treated As Highly Confidential and Subject to Appropriate Safeguards.

The Commission proposes to extend its existing “presumptive confidential treatment to any reports filed under rules adopted pursuant to this [FNPRM], including broadband outage reporting filings.”⁶⁴ Comcast supports this approach. In the same breath, however, the Commission questions whether it should *loosen* these protections and potentially remove any

⁶³ Reply Comments of CenturyLink, PS Docket No. 15-80, at 5 (July 31, 2015); *see also, e.g.*, Comments of Verizon & Verizon Wireless, PS Docket No. 11-82, at 14-17 (Aug. 8, 2011) (“A two-report system would still provide a measure of ‘situational awareness’ to allow the Commission to become involved in significant outages early should it so choose. Final reports would still give the Commission the opportunity to obtain the full details within the same timeframe as it does so today.”).

⁶⁴ FNPRM ¶ 145.

such presumption “as networks, and consumer expectations about transparency, [] evolve.”⁶⁵

This would be a serious mistake. If the Commission makes any changes, it should be to *strengthen*, not relax, the confidentiality protections afforded to outage reports, particularly if the collected data includes broadband network information. Broadband data is highly sensitive in nature, is routinely kept from the public, and could be incredibly harmful if placed in the wrong hands. Moreover, such information could highlight vulnerabilities in networks, thereby raising even stronger public safety and national security concerns with respect to disclosure than the voice data currently included in outage reports.

In adopting the Network Outage Reporting System (“NORS”) in 2004, the Commission determined that any potential consumer benefits of public disclosure of network outage information are “substantially outweighed by the potential harm to the public and national defense that might result from disclosure.”⁶⁶ More specifically, the FCC found that:

Given the competitive nature of many segments of the communications industry and the importance that outage information may have on the selection of a service provider or manufacturer, we conclude that there is a presumptive likelihood of *substantial competitive harm* from disclosure of information in outage reports. In addition, under FOIA exemption 4, we are also obliged to consider any adverse impact on the Commission’s ability to implement its statutory responsibility under section 1 of the Act to *ensure that communications services are adequate to protect “the national defense” and promote “safety of life and property.”* The record in this proceeding, including comments of the Department of Homeland Security, demonstrate that *the national defense and public safety goals that we seek to achieve by requiring these outage reports would be seriously undermined if we were to permit these reports to fall into the hands of terrorists who seek to cripple the nation’s communications infrastructure.*⁶⁷

⁶⁵ *Id.*

⁶⁶ *New Part 4 of the Commission’s Rules Concerning Disruptions to Communications, Report & Order & FNPRM*, 19 FCC Rcd. 16830 ¶ 45 (2004) (“2004 R&O”).

⁶⁷ *Id.* (citations omitted; emphasis added).

Prior to this determination, DHS had explained in comments that outage reporting data generally – and particularly the data requested by the Commission in its NORS template – was information that “pertains to or affects our ability to protect the Homeland” and “requires special safeguarding.”⁶⁸ DHS urged that, “[w]hile this information is critical to identify and mitigate vulnerabilities in the system, it can equally be employed by hostile actors to identify vulnerabilities for the purpose of exploiting them.”⁶⁹

Other parties have echoed these concerns. For example, AT&T told the Commission in 2011 that, “[g]iven that the nature of the data collected involves both confidential commercial information and information concerning facilities that are a part of the ‘Nation’s critical information infrastructure,’ it is imperative that any information collected by the Commission . . . be treated as confidential.”⁷⁰ AT&T rightly stressed that “[a]ny public dissemination of information concerning the root causes of network outages could facilitate attacks on those networks and undermine the efforts of the Commission to reinforce the reliability of those networks.”⁷¹ Accordingly, “[c]aution should be the byword in any use and dissemination of information collected under this regime.”⁷² Just last year, CTIA likewise emphasized that “[t]he

⁶⁸ See Comments of the Dep’t of Homeland Sec., ET Docket No. 04-35, at 14 (June 2, 2004). This information includes the direct and root causes of a disruption; the duration of a disruption; the range and types of services affected; the scope and gravity of the impact across all platforms and geographic areas; specific equipment failures; specific network elements affected; remedial measures/best practices applied; and an appraisal of the effectiveness of those measures/best practices. *Id.*

⁶⁹ *Id.*

⁷⁰ Comments of AT&T Inc., PS Docket No. 11-82, at 22 (Aug. 8, 2011).

⁷¹ *Id.*

⁷² *Id.*

Commission’s decision making process on this issue should be guided by the same principles that led to the decision to make NORS data confidential in the *2004 Outage Reporting Order*.⁷³

Comcast wholeheartedly agrees with these views. Nothing has changed in the past twelve years to tip the balance of the scale toward public disclosure. To the contrary, the concerns DHS espoused more than a decade ago are all the more salient today, especially given the proposed inclusion of granular data that could highlight broadband network vulnerability at a time when broadband networks are even more ingrained in the everyday lives of our nation’s citizens, public and private institutions, and businesses, and when both the capabilities and the determination of America’s enemies are growing. If the Commission moves forward with its outage reporting proposal, it must establish firm safeguards around broadband data. The Commission also should continue to ensure that its Part 4 rules provide that outage reports are presumptively protected from public disclosure under FOIA and share access to the NORS database with only DHS under stringent safeguards.⁷⁴

B. The Commission Should Not Share Outage Reports With States.

In the Further Notice, the Commission proposes to direct the Bureau to “develop proposals for how information could be shared appropriately with state entities.”⁷⁵ Given the

⁷³ Comments of CTIA – The Wireless Ass’n, PS Docket No. 15-80, ET Docket No. 04-35, at 13-14 (July 16, 2015) (“CTIA 2015 Comments”).

⁷⁴ See 2004 R&O ¶ 47 (“We will, therefore, make available to DHS, in encrypted form and immediately upon receipt, all electronically submitted outage reports.”). Presumptive protection from public disclosure under FOIA is all the more important given that the Commission recently lowered the standard for when confidential documents may be accessible under FOIA, without proper notice and comment, in an order issued in the Charter-Time Warner Cable-Bright House transaction. See Comcast Corp. & NBCUniversal Media, LLC, Petition for Reconsideration, MB Docket No. 15-149, at 5 (Oct. 13, 2015) (seeking reconsideration of an order that, among other substantive rule changes, no longer requires a showing that public disclosure of confidential information is “necessary” in response to a FOIA request).

⁷⁵ See FNPRM ¶ 147.

highly confidential and sensitive nature of VoIP and broadband outage data, however, the Commission should not allow such information to be shared with state entities. Allowing states access would increase the risk of inappropriate disclosure due to, among other things, less secure systems and open records laws. More generally, increasing the number of people who have access to the data inherently increases the risk of breach or accidental disclosure.

Indeed, once state commissions or other agencies beyond the FCC and DHS are given access to highly confidential data, it can become hard to limit (short of litigation) who else may receive access to that data – whether on purpose or by accident – and hard to ensure that those entities consistently adhere to the Commission’s confidentiality requirements.

Notably, states continue to seek direct access to current NORS reports and doubtless would seek similar access to broadband outage data.⁷⁶ Numerous parties have on multiple occasions explained to the Commission why states should not have such access, with the primary concern being the:

. . . states’ inability to guarantee the safeguarding of carriers’ commercially and national security-sensitive confidential information as the Commission does For example, states cannot guarantee that carriers’ reports would not be subject to public information requests. The inability to make that guarantee stems from the fact that any current state rule or law is subject to the vagaries of the state legislature, which could easily undo any current exemption outage reports may have under the state’s open record laws.⁷⁷

Again, these concerns are only magnified with the inclusion of broadband outage data, and – as discussed below – would be even further magnified with the inclusion of cybersecurity data.

⁷⁶ See, e.g., Letter from Nat’l Ass’n of Regulatory Util. Comm’rs, to FCC Commissioners, ET Docket No. 04-35 (Mar. 18, 2015) (providing a resolution supporting state access to NORS database).

⁷⁷ Comments of AT&T Servs, Inc., PS Docket No. 15-80, ET Docket No. 04-35, at 25 (July 16, 2015); see also CTIA 2015 Comments at 13-14 (urging the Commission “to carefully consider the risks of unauthorized disclosure of NORS data accessed by state commissions or federal agencies to other parties”).

VII. CYBERSECURITY ISSUES ARE BEST ADDRESSED THROUGH ONGOING PUBLIC-PRIVATE PARTNERSHIPS AND WORKING GROUPS.

In the Further Notice, the Commission asks a series of questions related to whether, in addition to network outages, providers should be required to report information regarding cybersecurity issues. Among these questions, the Commission seeks comment on requiring such reporting for “failures that are software-related or firmware-induced, or unintended modifications to a database that otherwise do not trigger hard-down outages or performance degradations.”⁷⁸ Comcast agrees with the Commission that managing cybersecurity risks will require the ongoing, coordinated attention of industry participants, DHS, and other key governmental agencies. This rulemaking, however, is not the forum for addressing these extremely complicated and sensitive issues.⁷⁹

As the Commission is aware, Comcast and other broadband service providers already go to enormous lengths to detect and address cybersecurity problems – including distributed denial of service (“DDoS”) attacks, route hijackings, and other unintended modifications – as they arise. For example, Comcast abides by a set of internally-developed corporate and service-oriented best practices, policies, and standards aimed at protecting both its network infrastructure and subscribers from cyber threats. As a result, Comcast’s IP-based network is equipped to identify and neutralize the effects of a DDoS attack immediately (within seconds), and of other attacks immediately after detection and confirmation (usually within minutes) – in either case, well before any end user has experienced a service outage.

Moreover, the communications industry already works closely with the federal government on security issues. Comcast engages in ongoing collaboration with the DHS Office

⁷⁸ FNPRM ¶ 125.

⁷⁹ *Id.* ¶ 126.

of Cybersecurity and Communications, which serves as the Sector Specific Agency for the communications industry. Comcast also works closely with the U.S. Communication Sector Coordinating Council (“CSCC”), a group of more than thirty U.S. companies and associations from the wireline, wireless, cable, satellite, and broadcast industries that meets regularly and consults with DHS and other agencies to address critical infrastructure protection priorities and cross-sector issues. Similarly, the National Institute of Standards and Technology (“NIST”) currently is in the process of considering feedback it received from businesses in order to update its “voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks.”⁸⁰

The Commission itself has convened the Communications Security, Reliability and Interoperability Council (“CSRIC”), a federal advisory committee that brings together representatives of government, industry, and academia to work collaboratively and voluntarily to make recommendations on a variety of reliability-related topics, including cybersecurity. Of particular relevance, CSRIC Working Group 4 issued a 415-page report just last year that addressed industry cybersecurity risk management and best practices.⁸¹ Comcast and the rest of the industry have spent significant time and resources participating actively in CSRIC working groups and in many other governmental and non-governmental standards bodies.

⁸⁰ NIST, *Framework for Improving Cybersecurity*, Version 1.0, at 1 (Feb. 12, 2014), <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>; see also NIST, *Cybersecurity Framework Feedback: What We Heard and Next Steps*, at 8-9 (June 9, 2016), <http://www.nist.gov/cyberframework/upload/Workshop-Summary-2016.pdf>.

⁸¹ *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report*, CSRIC (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (“CSRIC WG4 Report”); see also, e.g., CSRIC, *Remediation of Server-Based DDoS Attacks: Final Report*, Working Group 5 (Sept. 2014), [https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_\(pdf\)_V11.pdf](https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf); CSRIC, *EAS Security Subcommittee: Final Report*, Working Group 3 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG3-EAS_SECURITY_FINAL_011316.pdf.

In short, voluntary public-private collaboration has produced effective and timely responses and solutions to significant cyber threats. The Commission should maintain its focus in this proceeding on network outage issues and allow cybersecurity voluntary initiatives to continue unimpeded.⁸² To the extent the Commission nevertheless believes that it requires additional cybersecurity information, it should use the existing mechanisms for obtaining such information. DHS has designated the National Coordinating Center for Communications as the Information Sharing and Analysis Center for “facilitat[ing] the exchange of vulnerability, threat, intrusion, and anomaly information amongst government and industry telecommunications participants.”⁸³ In addition, industry stakeholders have committed to aiding the Commission in “develop[ing] a voluntary program for annual meetings between the FCC, DHS and individual companies.”⁸⁴

Of course, information regarding cybersecurity incidents provided to any governmental agency must be protected by DHS’s Protected Critical Infrastructure Information (“PCII”) Program,⁸⁵ which establishes “uniform procedures on the receipt, validation, handling, storage,

⁸² Indeed, Chairman Wheeler has stressed the importance of a new “regulatory paradigm” in addressing cybersecurity concerns. Under this paradigm, industry and the FCC collaborate “to develop standards and processes.” Remarks of Chairman Tom Wheeler, Aspen Inst., at 5 (Aug. 14, 2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0815/DOC-340777A1.pdf. The FCC “does not impose specific regulations” but instead “work[s] with industry to inspect the implementation of the agreed-to policies while maintaining the ability to step in with regulation if necessary.” *Id.*; see also Remarks of Chairman Tom Wheeler, Am. Enter. Inst., at 1 (June 12, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf (“[T]he Commission relies on industry and the market first while preserving other options if that approach is unsuccessful.”).

⁸³ Dep’t of Homeland Sec., Nat’l Coordinating Ctr. for Commc’ns, <https://www.dhs.gov/national-coordinating-center-communications> (last visited Aug. 26, 2016).

⁸⁴ CSRIC WG4 Report at 368.

⁸⁵ 6 C.F.R. pt. 29.

marking, and use of critical infrastructure information.”⁸⁶ The Commission has yet to assure DHS that it will comply with these PCII safeguards. Indeed, it is far from clear that the Commission even has the legal authority to adequately protect against public disclosure of any highly sensitive cybersecurity information it may collect or access. The Commission cannot use the guise of outage reporting to obtain information with fewer safeguards than it otherwise would be required to implement.

VIII. THE COMMISSION MUST ENSURE THAT ANY NEW REQUIREMENTS COMPORT WITH THE PAPERWORK REDUCTION ACT.

The Commission’s proposed expansion of its outage reporting rules would impose new paperwork burdens on reporting entities like Comcast.⁸⁷ Requiring BIAS providers to provide outage reports would constitute a “collection of information” under the Paperwork Reduction Act of 1995 (“PRA”).⁸⁸ As the Commission considers this proposal, it must take into account the burdens that would be imposed on reporting entities in order to adhere to the PRA’s many requirements.

Notably, the PRA requires the Commission to demonstrate and then certify that each information collection “is necessary for the proper performance of the functions of the agency, including that the information has practical utility.”⁸⁹ The PRA also requires information collections to: (a) “reduce[] to the extent practicable and appropriate the burden on persons who

⁸⁶ Dep’t of Homeland Sec., PCII Program, <https://www.dhs.gov/pcii-program> (last visited Aug. 26, 2016). Congress’s passage of the Cybersecurity Information Sharing Act of 2015 (“CISA”) affirmed the importance of encouraging entities to share cyber threat information by protecting the information shared and the entities that share it. *See* Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title I (2015).

⁸⁷ *See* FNPRM ¶ 219.

⁸⁸ 44 U.S.C. § 3502(3).

⁸⁹ *Id.* § 3506(c)(3)(A).

shall provide information to or for the agency”;⁹⁰ and (b) “be implemented in ways consistent and compatible, to the maximum extent practicable, with the existing reporting and recordkeeping practices of those who are to respond.”⁹¹

Office of Management and Budget (“OMB”) regulations implementing the PRA likewise require the Commission to “demonstrate that it has taken *every reasonable step* to ensure” that its proposed information collections are “the least burdensome necessary for the proper performance of the agency’s functions to comply with legal requirements and achieve program objectives.”⁹² Notably, OMB’s rules also impose further obligations on the Commission. For example, OMB mandates that information collections have practical utility.⁹³ In addition, information collections requiring written response in fewer than 30 days – such as the proposed notification and initial report – are subject to a rebuttable presumption of invalidity.⁹⁴

These requirements are clear: information collections must be rooted in *necessity*,⁹⁵ and must minimize burdens. The Commission must not lose sight of this fact as it considers its proposed outage reporting rules.⁹⁶

⁹⁰ *Id.* § 3506(c)(3)(C).

⁹¹ *Id.* § 3506(c)(3)(E).

⁹² 5 C.F.R. § 1320.5(d)(1)(i) (emphasis added).

⁹³ *Id.* § 1320.5(d)(1)(ii)-(iii).

⁹⁴ *See id.* § 1320.5(d)(2) (requiring OMB not to approve the information collection unless the FCC can demonstrate that expedited timing “is necessary to satisfy statutory requirements or other substantial need”).

⁹⁵ Unnecessary information collections, in whole or in part, will not be approved by OMB. *See* 44 U.S.C. § 3508; 5 C.F.R. § 1320.5(f) (“[T]o the extent that OMB determines that all or any portion of a collection of information is unnecessary, for any reason, the agency shall not engage in such collection or portion thereof.”).

⁹⁶ Inattention to PRA requirements has caused certain Commission regulations to be blocked altogether, while others have been delayed and then limited to achieve PRA compliance. *See, e.g.*, Notice of Action, Office of Mgmt. & Budget, ICR Ref. No. 200804-3060-012 (July 9, 2008), http://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=200804-3060-012 (disapproving the leased

IX. CONCLUSION

For the forgoing reasons, the Commission should ensure that any outage reporting requirements adopted in this proceeding are narrowly crafted to provide meaningful information – focused on public safety – to Commission staff, and limit the burdens and costs imposed on service providers. Only customer-impacting, “hard down” outages should be reported by BIAS providers, using a metric and reporting regime that mirrors the VoIP approach. And the Commission must include appropriate safeguards to protect the confidentiality of reports if new reporting requirements are adopted. The Commission also should refrain from expanding this proceeding to address cybersecurity or related concerns that are being addressed in other fora.

Respectfully submitted,

WILLKIE FARR & GALLAGHER LLP
1875 K Street, N.W.
Washington, D.C. 20006

/s/ Kathryn A. Zachem
Kathryn A. Zachem
Mary P. McManus
COMCAST CORPORATION
300 New Jersey Avenue, N.W., Suite 700
Washington, DC 20001

LAWLER, METZGER, KEENEY
& LOGAN, LLC
1717 K Street, N.W., Suite 1075
Washington, D.C. 20006

Brian A. Rankin
Beth A. Choroser
Pamela S. Miranda
COMCAST CORPORATION
One Comcast Center
55th Floor
Philadelphia, PA 19103

Counsel for Comcast Corporation

August 26, 2016

access information collection); Notice of Action, Office of Mgmt. & Budget, ICR Ref. No. 200802-3060-019 (Nov. 28, 2008), http://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=200802-3060-019 (disapproving the backup power information collection); Notice of Action, Office of Mgmt. & Budget, ICR Ref. No. 201311-3060-001 (Aug. 15, 2014), http://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201311-3060-001# (modifying the FCC’s special access data collection requirements).