

**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
)	

REPLY COMMENTS OF COMCAST CORPORATION

WILLKIE FARR & GALLAGHER LLP
1875 K Street, NW
Washington, DC 20006

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

LAWLER, METZGER, KEENEY
& LOGAN, LLC
1717 K Street, NW, Suite 1075
Washington, DC 20006

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

Counsel for Comcast Corporation

September 12, 2016

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY.....	1
II.	THE RECORD ESTABLISHES THAT BROADBAND NETWORKS ARE MORE RESILIENT THAN LEGACY NETWORKS, UNDERMINING THE PRIMARY RATIONALE FOR INTRUSIVE OUTAGE REPORTING REQUIREMENTS.	2
III.	IF THE FCC MOVES FORWARD, THERE IS BROAD AGREEMENT THAT ANY NEW RULES MUST BE NARROWLY TAILORED TO PROVIDE MEANINGFUL INFORMATION TO THE COMMISSION.....	5
	A. Commenters Agree That the Commission Should Remain Focused on Its Public Safety Objectives.	5
	B. There Is Broad Industry Support for the Principle That Outage Reports Should Be Required Only for Hard-Down Outages That Impact Customers.	6
	C. The Record Demonstrates That Performance Degradation Standards Are Unnecessary and Undesirable.	8
IV.	COMMENTERS OVERWHELMINGLY AGREE THAT THE PROPOSED RULES ARE OVERLY BROAD.	10
	A. There Is Consensus That Any New Rules Should Exclude Dedicated Services. ...	10
	B. Commenters Agree That Any Reporting Obligations for BIAS Providers Must Be Limited to Networks They Own or Control.....	12
	C. The Record Demonstrates That Cybersecurity Issues Are More Appropriately Addressed In Ongoing Working Groups.	13
V.	THE COMMISSION SHOULD IMPLEMENT A SINGLE OUTAGE REPORTING PROCESS CONSISTING OF NO MORE THAN TWO STEPS.	15
VI.	THE COMMISSION SHOULD REJECT CALLS TO LOOSEN CONFIDENTIALITY PROTECTIONS OR GRANT STATES ACCESS TO OUTAGE REPORTING INFORMATION ABSENT SIGNIFICANT RESTRICTIONS AND CONTROLS.	17
VII.	CONCLUSION	21

**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
)	

REPLY COMMENTS OF COMCAST CORPORATION

Comcast Corporation (“Comcast”) hereby addresses comments filed in response to the Further Notice of Proposed Rulemaking adopted by the Federal Communications Commission (“FCC” or “Commission”) in the above-referenced proceedings.¹

I. INTRODUCTION AND SUMMARY

The initial comments reflect very broad consistency among different industry segments and across a range of issues on which the Commission sought comment. Specifically, the record establishes that:

- Due to their redundant, flexible infrastructure, broadband networks are less vulnerable to outages and more resilient than legacy networks, and service providers have strong incentives to ensure their continued reliability;

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

- To the extent the FCC decides to extend outage reporting obligations to broadband Internet access services (“BIAS”), those requirements must be narrowly focused on providing information that is both useful to the Commission and relevant to its public safety responsibilities;
- Consistent with the FCC’s focus on access to emergency services, reporting obligations should be limited to hard-down outages that affect at least 900,000 user minutes, and last at least 30 minutes (*i.e.*, instances of performance degradation should not trigger reporting obligations);
- Reporting obligations should not apply to dedicated services or cybersecurity issues and should extend only to outages affecting networks that a BIAS provider owns or controls;
- A single outage reporting process with no more than two steps should apply to interconnected voice over Internet protocol (“VoIP”) providers and, if needed, BIAS providers; and
- Confidential outage reports should not be shared with state agencies, especially if the Commission expands its outage reporting requirements to collect sensitive broadband network information. If the FCC nonetheless allows such sharing, stringent safeguards would be needed to protect this information and limit its disclosure.

In light of the clear record on these matters, the Commission must refine its proposals in order to ensure that the agency does not collect information that will be of little or no value to advancing public safety objectives. If the current proposals are adopted, the Commission will be inundated with unhelpful information, minimizing the data’s utility to the FCC while simultaneously maximizing the burdens on providers.

II. THE RECORD ESTABLISHES THAT BROADBAND NETWORKS ARE MORE RESILIENT THAN LEGACY NETWORKS, UNDERMINING THE PRIMARY RATIONALE FOR INTRUSIVE OUTAGE REPORTING REQUIREMENTS.

The Commission’s various proposals for onerous, overbroad reporting requirements appear to be predicated on the mistaken assumption that broadband networks are inherently more susceptible to large-scale, customer-impacting outages than PSTN networks.² The record amply shows that this is not the case. In fact, as Comcast observed in its initial comments, broadband

² See *id.* ¶ 103.

networks are designed to prevent and withstand these types of outages.³ Given the paucity of evidence of widespread broadband outages or reliability problems, commenters were rightfully perplexed by the Commission’s conclusion that outage reports are nonetheless needed to ensure broadband reliability.⁴ Rather, as the comments make clear, it is providers’ accountability to consumers in the marketplace – not regulation – that has driven and will continue to drive network reliability.

Numerous commenters detail how, due to a high level of redundancy in network architecture and the ability to route traffic around any problems, broadband networks are more reliable than legacy networks.⁵ As AT&T explains, “[b]roadband networks are *not* more susceptible to outages than the TDM-based network. The robust and dynamic engineering of broadband networks enables redundancy and resiliency beyond the bounds of the static PSTN.”⁶ USTA similarly observes that “the decentralized nature of [broadband] network[s], combined with wide adoption of industry best practices, has contributed over time to creating one of the most reliable communications infrastructures in the world.”⁷ The National Cable & Telecommunications Association (“NCTA”) aptly sums up the consensus of the industry

³ Comcast Comments at 3-6, 7-10. (Unless otherwise noted, all comments cited herein were filed in PS Docket No. 15-80 on August 26, 2016.)

⁴ See, e.g., Alliance for Telecommunications Industry Solutions (“ATIS”) Comments at 3-4.

⁵ See American Cable Association (“ACA”) Comments at 7-8 & n.17; AT&T Comments at 5; ATIS Comments at 3-4; CenturyLink Comments at 5; Comtech Comments at 2; NCTA Comments at 5-6; United States Telecom Association (“USTA”) Comments at 11-13; Verizon Comments at n.7.

⁶ AT&T Comments at 5 (emphasis added). Putting a finer point on it, AT&T continues, “[W]ell-engineered broadband networks allow for higher order redundancy (N + 1 architectures, rather than just a single redundant node) in a more economic fashion, allowing greater investments in resiliency and network security.” *Id.*; see also Verizon Comments at 4 n.7 (“Contrary to the suggestion in the *Further Notice* [], fiber and IP-enabled networks are physically more sustainable and redundant, and less prone to outages than the copper PSTN.”).

⁷ USTA Comments at 12.

commenters: “[B]roadband networks are inherently redundant and employ a variety of mechanisms to ensure the automatic routing and rerouting of information to minimize disruptions, congestion, and failures in connectivity.”⁸

Quite simply, broadband networks continue to be designed to withstand the types of outages that concern the Commission. The vast majority of network “disruptions” are neither felt nor seen by customers, and hard-down outages that impact large numbers of customers are few and far between. Not surprisingly, the record makes clear that new regulatory reporting requirements are a solution in search of a problem with respect to ensuring network reliability. A small minority of commenters’ unsubstantiated assertions aside,⁹ commenters overwhelmingly agree that market incentives drive BIAS providers to ensure well-functioning, redundant, and resilient networks.¹⁰ Accordingly, the Commission’s proposed regulations are unnecessary.

⁸ NCTA Comments at 5-6; *see* NCTA Comments, PS Docket No. 11-82, at 5 (Aug. 8, 2011) (“Architecturally, broadband packet-switched networks are designed differently from traditional circuit-switched networks.”).

⁹ *See* Boulder Regional Emergency Telephone Service Authority (“BRETSA”) Comments at 10; California Public Utilities Commission (“CPUC”) Comments at n.18; Public Knowledge Comments at 1.

¹⁰ *See, e.g.*, AT&T Comments at 6 (“In a competitive free market, as is the case here, competitive pressures guarantee efficient and well-run networks that serve the needs of their customers.”); ACA Comments at 8 (explaining that its members’ market-based incentives “ensure that their networks operate in a safe and reliable manner” and that broadband network operators compete for their customers’ business on the basis of service quality, including reliability); ATIS Comments at 4 (“The networks’ continued reliability and resiliency is driven not by regulation but by competition and by the providers’ recognition of the importance of meeting or exceeding their customers’ expectations.”); CenturyLink Comments at 5 (“Given how robustly these networks are designed and the considerable competitive pressures providers face to deliver high quality, reliable service to their customers, outage reporting is simply not needed to drive enhanced reliability.”).

III. IF THE FCC MOVES FORWARD, THERE IS BROAD AGREEMENT THAT ANY NEW RULES MUST BE NARROWLY TAILORED TO PROVIDE MEANINGFUL INFORMATION TO THE COMMISSION.

Numerous commenters argue against extending mandatory reporting obligations to broadband providers, raising legitimate questions as to whether new rules are warranted at all.¹¹ As a result, it is far from clear that public safety or other compelling considerations require the adoption of any new outage reporting requirements. If the Commission nevertheless decides to expand its outage reporting obligations, the record establishes that it must do so in a way that both minimizes costs and burdens for service providers and avoids requirements that are unrelated to the Commission's public safety responsibilities. In particular, the overwhelming majority of the commenting parties agree that only hard-down outages that have a significant impact on consumers should be reportable – *i.e.*, incidents that last for at least 30 minutes and potentially affect 900,000 user minutes.¹² In contrast, the record shows that reporting metrics based on performance degradation criteria are inappropriate and would prove to be needlessly complicated.¹³

A. Commenters Agree That the Commission Should Remain Focused on Its Public Safety Objectives.

Should the Commission move forward and extend outage reporting obligations to broadband networks, the record makes clear that any new requirements must be carefully tailored to yield useful and meaningful information about actual outages that could impact public

¹¹ See ACA Comments at 3; AT&T Comments at 5-6; ATIS Comments at 3; Comtech Comments at 3; ITTA Comments at 2; USTA Comments at 1, 2-3; WISPA Comments at 6.

¹² See, *e.g.*, ACA Comments at 11-12, 19; AT&T Comments at 17-18; ATIS Comments at 10-12; Comcast Comments at 18-20.

¹³ See, *e.g.*, ATIS Comments at 10-11; CenturyLink Comments at 14-15; ITTA Comments at 9-14; NCTA Comments at 4-7, 9-14; NTCA—The Rural Broadband Association (“NTCA”) Comments at 4-5.

safety.¹⁴ As Verizon notes, from the outset, the Commission’s outage reporting rules have focused on critical communications during major network disruptions.¹⁵ The FNPRM provides no good policy reason to deviate from that approach, and the record shows that no such reason exists.

Indeed, neither the Commission nor any commenter has explained how *any* public safety benefits will stem from the overly broad, onerous new reporting obligations proposed in the FNPRM.¹⁶ If the Commission moves forward, it should ensure that any rules are clearly tied to its public safety mission. As Verizon aptly states, “[t]o further the Commission’s important public safety duties, network reliability rules and policies should remain focused on major network failures with widespread geographic and consumer impact that affect services most significant to emergency and other critical situations.”¹⁷ Comcast wholly agrees.

B. There Is Broad Industry Support for the Principle That Outage Reports Should Be Required Only for Hard-Down Outages That Impact Customers.

Building on the principle that the Commission should be focused on outages that potentially affect public safety, almost all commenters strongly urge the FCC to require reporting only when there is a hard-down disruption that impacts consumers. As these parties point out, a hard-down standard focused on consumer impact provides an administratively practical, bright-line test and offers an accurate “snapshot of the scope and scale of an event.”¹⁸

¹⁴ See, e.g., ACA Comments at 4; CenturyLink Comments at 6; NCTA Comments at 4; NTCA Comments at 3; Verizon Comments at 3.

¹⁵ See Verizon Comments at 2.

¹⁶ See, e.g., USTA Comments at 2, 3-6, 19 (“[T]he Commission has failed to identify any public safety benefits that would justify the significant burdens associated with its proposals.”).

¹⁷ Verizon Comments at 1-2.

¹⁸ CenturyLink Comments at 14; see also AT&T Comments at 17-18; ATIS Comments at 11-12; NCTA Comments at 10-11.

In determining the appropriate threshold for hard-down outages, there is substantial support in the comments for applying the same reporting threshold to BIAS that currently applies to VoIP providers (*i.e.*, 30 minutes' duration potentially affecting 900,000 user minutes).¹⁹ As ATIS notes, “[t]his approach is reasonable and has proven to be a good metric for voice outage reporting [that] has withstood the test of time.”²⁰ Further, the use of a bright-line standard with which providers already have significant experience should simplify compliance and require fewer resources to put into effect.²¹

In contrast, there is broad opposition to the Commission’s proposal to adopt a throughput-based metric for identifying reportable events. First, use of a simple throughput metric would require providers to file reports even when their customers continue to receive service. Consequently, this misguided approach would shift the focus of the Commission’s reporting regime away from what should be its central concern: service outages that have a significant impact on consumers. Second, a throughput metric would subject service providers to a perpetually changing goalpost as they increase bandwidth to accommodate consumer demand. As CenturyLink notes, “a throughput-based metric risks quickly becoming obsolete or outdated” as consumer demand for broadband continues to accelerate.²² Furthermore, ATIS correctly observes that, “[a]s customer bandwidth usage and expectations increase, the proposed bandwidth-based metric would require reporting under NORS for outages impacting fewer and

¹⁹ See AT&T Comments at 17; ATIS Comments at 11-12; Comcast Comments at 18-20; NCTA Comments at 10-11; *see also* CenturyLink Comments at 14 (generally supporting the 30 minute/900,000 user minutes standard, but also suggesting that the Commission limit the reporting obligation to outages that disrupt at least 5,000 customers).

²⁰ ATIS Comments at 12.

²¹ See AT&T Comments at 18; NCTA Comments at 11.

²² See CenturyLink Comments at 14.

fewer customers.”²³ Similarly, NCTA notes that reliance on a throughput-based standard could lead to anomalous results, wherein “an outage to a small number of high-capacity customers might trigger a reporting requirement, while an outage to a much larger number of low-capacity customers would not.”²⁴ In short, these logistical difficulties and anomalous results counsel against implementing any throughput-based metric as part of the Commission’s outage reporting regime.²⁵

C. The Record Demonstrates That Performance Degradation Standards Are Unnecessary and Undesirable.

In the FNPRM, the Commission suggests that BIAS and VoIP service providers could be required to report on events that involve the loss of “general useful availability and connectivity.”²⁶ This proposal, which “extend[s] far beyond the specific goal of updating the NORS requirements for an IP world,”²⁷ generated widespread opposition based on a variety of valid concerns.

Perhaps most notably, Comcast and other commenting parties emphasize that the suggested metrics for throughput, packet loss, and latency “would [not] provide the Commission with accurate information on whether customers can access the Internet to contact emergency personnel.”²⁸ As ATIS notes, “there are no established industry standards that would indicate to

²³ ATIS Comments at 11.

²⁴ NCTA Comments at 10.

²⁵ Notably, the limited number of parties that support performance degradation reporting do so in a vague manner that does not evince an understanding or appreciation of these technical difficulties. *See, e.g.*, CPUC Comments at 11; New York Public Service Commission (“NYPS”) Comments at 10; Virginia State Corp. Commission Comments at 6.

²⁶ FNPRM ¶¶ 133, 166.

²⁷ NCTA Comment at 4-5.

²⁸ NCTA Comments at 12; *see also* AT&T Comments at 18-19; ATIS Comments at 12-14 (noting that reports filed pursuant to the proposed service quality metrics would provide the Commission with

BIAS providers that certain markers of network performance could or should be read to indicate an outage.”²⁹

In fact, depending on the circumstances, “degradation” can be affirmatively helpful since IP networks are “engineered to ensure that throughput variations, packet loss, and latency rarely affect customers while maintaining high levels of flexibility, efficiency, and [quality of service].”³⁰ Engineering for flexibility and efficiency “ensure[s] that time-sensitive voice packets go through while less sensitive traffic, such as email, may be delayed.”³¹

In addition, the new obligations “would create new, more burdensome, and confusing requirements.”³² For example, NTCA notes that “[s]mall, rural providers are not currently collecting data in regard to network degradation, nor is there a plug-and-play, cost-effective solution that small providers could employ to capture the requested information.”³³ These burdens simply would not be outweighed by any limited benefits of requiring reporting in these circumstances.³⁴ As a result, the Commission should reach the same conclusion that it did in 2012 and decline to adopt such reporting metrics.³⁵

information “that is not reliable and not relevant to responding to outages that prevent consumers from contacting emergency services”); Comcast Comments at 14-18.

²⁹ ATIS Comments at 14.

³⁰ AT&T Comments at 18.

³¹ *Id.* at 18-19; *see also* Comcast Comments at 14 (“[S]ome packet loss can actually *improve* the customer experience, as demonstrated by studies of bufferbloat and Active Queue Management.”).

³² NTCA Comments at 5; *see also* WISPA Comments at 13.

³³ NTCA Comments at 5.

³⁴ ITTA Comments at 13 (“As with the Commission’s other proposals in the *FNPRM*, [the performance degradation proposals] would be an endeavor laden with exorbitant costs with little to no benefit to the Commission’s public safety mission.”).

³⁵ *See 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*, Report and Order, 27 FCC Rcd. 2650 ¶ 90 (2012) (“*2012 Order*”).

IV. COMMENTERS OVERWHELMINGLY AGREE THAT THE PROPOSED RULES ARE OVERLY BROAD.

In addition to proposing sweeping measures that would fundamentally alter what constitutes a reportable event, the Commission also advances a number of other proposals that would inappropriately broaden the scope of outage reporting obligations.³⁶ The Commission should limit the scope of its outage reporting rules to exclude dedicated services from such requirements, limit any reporting obligations to networks that a provider owns or controls, and continue addressing cybersecurity issues through preexisting channels.

A. There Is Consensus That Any New Rules Should Exclude Dedicated Services.

In keeping with the goal of providing the Commission with targeted, meaningful information about wide-scale outages that could impact access to emergency communications, the record makes clear that any new rules adopted in this proceeding should not apply to providers of dedicated services. Such rules simply are not needed and would prove costly, adding burdens to dedicated services providers without increasing accountability or producing a discernible public safety benefit.³⁷

³⁶ See, e.g., CenturyLink Comments at 2 (“[M]any of the proposed rules are overly broad and not sufficiently targeted to meet the objectives the Commission intends or is authorized to pursue.”); NTCA Comments at 2-3 (arguing that the FCC “appears to be using the need to update rules for broadband as a pretext for regulatory overreach – proposing wide-sweeping reforms that extend far beyond the straightforward task at hand”).

³⁷ Some commenters argue that, on top of being superfluous, additional FCC outage reporting obligations for dedicated services could be quite costly for service providers. For example, NCTA explains that, contrary to the Commission’s assumptions, not all dedicated services providers collect and retain real-time quality-of-service metrics, and “[a]djusting existing operations to collect and report near-real-time outage data would impose significant costs on [dedicated services] providers, which ultimately could increase the cost to the customer for these services.” NCTA Comments at 19; see also ACA Comments at 24 (explaining why “the Commission’s assumption that all dedicated services providers today already collect internal data to support their contractual obligations so that providing it to the Commission in the event of an outage could be done at minimal cost is incorrect”).

Many commenters agree that dedicated services should be excluded from any new FCC outage reporting obligations, particularly because such services are already subject to stringent contractual guarantees.³⁸ Comcast, ITTA, NCTA, and other commenters stress that the very characteristics that are the hallmarks of dedicated services – *i.e.*, “their *dedicated* use by enterprise purchasers for *point-to-point* data transmissions, typically subject to service-level agreements with provisions governing service outages”³⁹ – make it wholly unnecessary for the Commission to have ongoing and detailed “visibility” into potential outages.⁴⁰

As NCTA explains, contractual guarantees for dedicated services “provide strong market incentives for providers . . . to minimize outage events and performance degradation, as such events typically result in a service credit or other penalty on the service provider.”⁴¹ These agreements also often require providers to quickly remedy service degradations when they occur.⁴² Neither the Commission nor the very few commenters supporting the inclusion of dedicated services provide a persuasive explanation as to “how [dedicated services] data is related to public safety, [or] what the Commission would do once the data is processed, given that affected parties are already fully compensated and carriers have significant incentives to live up to contractual commitments.”⁴³

³⁸ See ACA Comments at 5, 20; AT&T Comments at 11; ATIS Comments at 6; Comcast Comments at 21-22; ITTA Comments at 5; NCTA Comments at 18; USTA Comments at 14-15.

³⁹ ITTA Comments at 5 (emphasis in original).

⁴⁰ See *id.*; Comcast Comments at 21; NCTA Comments at 18; USTA Comments at 14 (stating that any Commission action in this area is “wholly redundant and unnecessary” because dedicated services generally only directly affect one customer, who already has guaranteed recourse).

⁴¹ NCTA Comments at 18; see also, *e.g.*, ACA Comments at 25; USTA Comments at 15.

⁴² See, *e.g.*, Comcast Comments at 22.

⁴³ USTA Comments at iv, 13-14. The NYPSC and CPUC ask the Commission to extend outage reporting to dedicated services providers but do not take into account dedicated services providers’ contractual relationships with their customers or that those customers already are subject to outage

B. Commenters Agree That Any Reporting Obligations for BIAS Providers Must Be Limited to Networks They Own or Control.

If outage reporting obligations are extended to BIAS providers, the Commission must also make clear that BIAS providers are not obligated to report outages that occur on networks that they neither own nor control. As NCTA, ITTA, and other commenters explain, BIAS providers do not have ready access to the outage-related information of other network operators or applications providers, and the Commission should not make BIAS providers “clearinghouses” for the sake of convenience to the Commission.⁴⁴ In other words, commenters agree that the Commission must not “saddle individual BIAS providers with responsibility for the reporting of some events that are outside of their control or knowledge.”⁴⁵

NCTA correctly explains that the same redundancies and interconnections that make the Internet less vulnerable to outages also mean that Internet traffic often transits multiple providers’ networks before reaching the Internet backbone and then its ultimate destination.⁴⁶ As the Commission is well aware, the Internet’s infrastructure includes not only the last-mile, middle-mile transport, and backbone facilities, but also content delivery networks, server farms,

reporting obligations. The NYPSC concludes that outage reporting for dedicated services would facilitate “quick, efficient communications between and among affected companies, emergency service providers and state and federal regulators,” without explaining why this would occur as a result of new reporting requirements. NYPSC Comments at 9. The CPUC likewise makes conclusory statements about the importance of cell backhaul to wireless networks, but offers no explanation of how new reporting requirements would (1) provide the FCC with useful information (especially given that any outages affecting the wireless network will already be reported by the wireless provider), (2) better incentivize cell backhaul providers that already must live up to contractual commitments, or (3) outweigh the costs of subjecting providers to new regulatory obligations. *See* CPUC Comments at 8.

⁴⁴ *See* NCTA Comments at 16; ITTA Comments at 17; WISPA Comments at 22.

⁴⁵ ITTA Comments at 17; *see also* CTIA Comments at 8-9; NCTA Comments at 16; NTCA Comments at 5-6; USTA Comments at 10-14; Vonage Comments at 3, 7-10; WISPA Comments at 22-23.

⁴⁶ *See* NCTA Comments at 16-17.

and services operated by application providers.⁴⁷ BIAS providers would have little to no ability to identify – let alone report on – disruptions to underlying interconnecting providers’ networks or disruptions at the application layer, nor should they be required to undertake new obligations or form new economic arrangements with interconnecting networks for the sake of filing regulatory reports.⁴⁸ In short, a requirement for BIAS providers to be the “central reporting point” for these types of disruptions not only would be impractical in the extreme, but also would lead to misinformation and jumbled reporting.⁴⁹ As CTIA puts it, “[t]he Commission offers no justification for such an unfair and infeasible requirement.”⁵⁰

C. The Record Demonstrates That Cybersecurity Issues Are More Appropriately Addressed In Ongoing Working Groups.

The FNPRM seeks comment on whether service providers should be required to furnish additional information regarding cybersecurity issues that are not related to hard-down outages.⁵¹

⁴⁷ See *id.* at 17.

⁴⁸ See *id.*; ACA Comments at 19-20 (noting that BIAS providers “will not necessarily have any visibility into why that connection is down or the steps being taken for restoration of service” with respect to other networks); CenturyLink Comments at 11 (“Because the Internet is a network of networks, it is not possible for any single BIAS to assure delivery of an end user’s communication to any destination of the end user’s choosing on the Internet.”); NTCA Comments at 5 (“[S]mall, rural BIAS providers often rely upon middle-mile, transit, and/or the backbone of several unrelated, third-party service providers – all of whom have extensive, even national, networks and none of whom a smaller provider is likely to be able to control or even bargain with from a position of negotiating strength such that visibility into network disruptions will be shared freely.”); WISPA Comments at 22 (“In many cases, providers have no way of determining if any particular service outside of their control is functioning properly or how to fix it.”).

⁴⁹ FNPRM ¶ 112; see also, e.g., USTA Comments at 13 (“[G]iven the interconnected nature of the internet, the Commission’s proposal would be confusing for all stakeholders to implement.”).

⁵⁰ CTIA Comments at 9.

⁵¹ See FNPRM ¶ 125.

There is only extremely limited support for such reporting.⁵² The majority of the comments explain why the current system should *not* be expanded to include cybersecurity issues.⁵³

In particular, the comments point out that the current Part 4 rules already require providers to furnish information regarding issues such as unintended changes to software or firmware in connection with a reportable service disruption.⁵⁴ More fundamentally, the comments emphasize that “[s]everal forums already exist for ongoing government and industry collaboration on the cybersecurity of communications infrastructure.”⁵⁵ As a result, a Commission-imposed reporting requirement could detract from or conflict with existing flexible, industry-driven approaches to cybersecurity.⁵⁶

Other parties aptly note that Commission action unilaterally seeking additional cybersecurity information both appears to be inconsistent with the Chairman’s announced commitment to public-private partnerships for addressing cybersecurity issues and ignores the mechanisms already in place for obtaining such information.⁵⁷ Put simply, the record is clear that the Commission should continue to rely on the collaborative work of groups such as the Communications Security, Reliability and Interoperability Council (“CSRIC”), which include representatives from government, industry, and the academic world. These organizations embody the Chairman’s “new paradigm” and have already demonstrated the ability to produce

⁵² See CPUC Comments at 9-10 (apparently supporting adoption of a cybersecurity reporting requirement).

⁵³ See, e.g., ACA Comments at 30-31; ATIS Comments at 7-9; CenturyLink Comments at 11-13; Comcast Comments at 32-35; T-Mobile Comments at 16-17; USTA Comments at 17-19.

⁵⁴ See, e.g., CenturyLink Comments at 11-12; USTA Comments at 17.

⁵⁵ NCTA Comments at 25.

⁵⁶ *Id.*

⁵⁷ See Comcast Comments at 33-34; USTA Comments at 17-18.

timely, comprehensive proposals for cybersecurity risk management and industry best practices.⁵⁸

V. THE COMMISSION SHOULD IMPLEMENT A SINGLE OUTAGE REPORTING PROCESS CONSISTING OF NO MORE THAN TWO STEPS.

Numerous parties emphasize in their comments that, if the Commission were to impose outage reporting obligations on BIAS providers, it should apply the two-step administrative process that currently governs reports by VoIP providers.⁵⁹ Similarly, commenters note that the reporting process for VoIP providers should remain unchanged.⁶⁰ Under this approach, both BIAS and VoIP providers would file an initial notification within 24 hours after discovery of the reportable event and a final report within 30 days after discovery.

Despite the fact that no public safety concern would be advanced by adoption of more burdensome requirements, a limited number of commenters nevertheless insist that a greater number of reports are needed. For example, the Washington Utilities and Transportation Commission (“WUTC”) proposes requiring BIAS providers to comply with the three-step reporting process that currently applies to TDM-based wireline services: initial notifications within two hours after discovery of an outage and subsequent reports within three days and 30 days.⁶¹ Even more concerning, the NYPSC contends that BIAS providers should be required to

⁵⁸ See, e.g., 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”).

⁵⁹ See ACA Comments at 27-30; CenturyLink Comments at 20-21; Comcast Comments at 23-27; T-Mobile Comments at 15-16; USTA Comments at 8-10.

⁶⁰ See CenturyLink Comments at 20-21; NCTA Comments at 20-22.

⁶¹ WUTC Comments at 2.

file an initial notification within 60 minutes after discovery of a reportable event, an initial report within 72 hours, and a final report within 30 days after discovery.⁶²

These commenters substantially overvalue early, initial reports. As ATIS explains, “it is often difficult to identify the root cause or even validate that a reportable event has occurred” within the two-hour window that currently applies to legacy wireline networks.⁶³ CenturyLink similarly notes that “[t]he broadband networks at issue are extremely complex and time is needed to diagnose problems accurately and restore service.”⁶⁴ As a result, initial notifications filed within an unduly short filing window will include little useful information,⁶⁵ and many such notifications ultimately will be withdrawn after further investigation.⁶⁶

Moreover, mandating the submission of reports within the first few hours of an outage ignores the fact that personnel responsible for preparing these documents include technical experts whose energies should be focused on restoring service.⁶⁷ Indeed, the Commission adopted the current two-step process for interconnected VoIP outages in 2012 in part to permit service providers “to *work* the outage problem as opposed to *reporting* on the outage.”⁶⁸ This objective remains equally as valid with respect to BIAS services as it is to VoIP, and it remains as valid in 2016 as it was in 2012. Accordingly, the Commission should continue to rely on a two-step reporting process for VoIP outages and do the same for any BIAS outages it subjects to

⁶² NYPSC Comments at 9.

⁶³ ATIS Comments at 18.

⁶⁴ CenturyLink Comments at 21.

⁶⁵ See T-Mobile Comments at 15-16; USTA Comments at 9.

⁶⁶ Comcast Comments at 25 (noting that Comcast “estimates that up to *fifty percent* of its notifications are withdrawn under the current system”); see also ACA Comments at 28-29; NCTA Comments at 15-16.

⁶⁷ See AT&T Comments at 15; T-Mobile Comments at 16; USTA Comments at 8-9.

⁶⁸ 2012 Order ¶ 95 (emphasis added).

reporting obligations, thereby ensuring that the FCC receives adequate notice of a reportable outage without unduly interfering with a provider's ability to restore service as quickly as possible.

VI. THE COMMISSION SHOULD REJECT CALLS TO LOOSEN CONFIDENTIALITY PROTECTIONS OR GRANT STATES ACCESS TO OUTAGE REPORTING INFORMATION ABSENT SIGNIFICANT RESTRICTIONS AND CONTROLS.

The initial comments make clear that there is no reasoned basis or record support for the Commission to alter its longstanding rules and procedures treating NORS reports as presumptively confidential and exempt from public disclosure under the Freedom of Information Act ("FOIA").⁶⁹ Nothing has changed over the past twelve years to alter the Commission's sound policy or the national security and commercial sensitivity concerns on which its policy is based. In fact, such protections are all the more critical today, especially if the Commission extends reporting obligations to BIAS providers. Numerous commenters rightly urge the Commission to continue to treat NORS reports as presumptively confidential for these very reasons.⁷⁰ And the Commission has not pointed to any evidence that these risks have diminished such that they are now outweighed by any perceived benefit of public disclosure, let alone by "undefined 'transparency' objectives."⁷¹

⁶⁹ See 47 C.F.R. § 4.2 ("Reports filed under this part will be presumed to be confidential.").

⁷⁰ See AT&T Comments at 21-22; ATIS Comments at 19-21; CenturyLink Comments at 19 ("The reasons these reports were granted confidential treatment in the first place is because of the sensitive information they contain and the need to safeguard proprietary network data from both security and competitive perspectives. In the intervening years since that time, the security and competitive environments have only grown *more intense*, making the need to protect confidential information more critical now than ever." (emphasis added)); Comcast Comments at 27-31; CTIA Comments at 19-20; NCTA Comments at 23-24 ("Information can be shared so rapidly using modern communications technologies that outage data exposed in one accidental disclosure or intentional breach can travel quickly to all corners of the world."); USTA Comments at 15-16; WISPA Comments at 23.

⁷¹ CTIA Comments at 3; *see also id.* at 19 ("There are no grounds to reconsider the confidential treatment of outage reports based on the 'evolution' of networks or consumer expectations."); AT&T

Comments of state agencies readily acknowledge that NORS reports warrant confidential protection, yet they nonetheless advocate for policy changes that would inevitably whittle away the Commission’s presumption of confidentiality.⁷² These comments only reinforce many parties’ – including Comcast’s – concerns that confidential NORS reports should not be shared with state commissions or other state or local entities, especially if the Commission expands its NORS program to collect sensitive broadband network information. States’ access to such data would substantially increase the risk of harm from unauthorized disclosure. This risk is a function not only of the significant expansion of who has access to this sensitive data, but also of variations in states’ open records laws, agency structures, and information technology capabilities.⁷³

Comments at 22 (“To the extent the Commission ‘evolves’ on this issue, it should evolve in the direction of more security, not less.”); CenturyLink Comments at 19; NCTA Comments at 24.

⁷² The WUTC says it “understands and agrees that information regarding outages, including root cause analysis, locations, network performance, and time to restoral, is not only competitively sensitive but specifically critical regarding national security.” WUTC Comments at 2. The NYPSC likewise says it “understands the need for confidentiality restrictions.” NYPSC Comments at 3. Only BRETSA supports public disclosure, arguing that service providers *think* that NORS information is confidential when, in fact, it is simply “market information” to which consumers should have access. BRETSA Comments at 10-11. BRETSA goes so far as to argue that service providers “cloak their service failures behind claims that the information is proprietary or warrants protection for homeland security purposes, and enlist the Commission as a tacit ally” *Id.* at 11. Given the broad consensus that outage information indeed warrants strong confidentiality protection, however, BRETSA’s claim is a far cry from the truth.

⁷³ See NCTA Comments at 24 (“The more widely that the Commission shares sensitive outage reporting information with other federal and state agencies, the greater the risk that it could fall into the wrong hands.”); AT&T Comments at 21 n.68 (noting that state-level confidentiality protections may be “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”); CTIA Comments at 21 (“Prior to authorizing access to a state agency, the Commission should analyze that state’s Sunshine or public access laws that may put confidential reports collected through NORS at risk of disclosure.”); USTA Comments at 16 (“[T]o the extent the state FOIA or Public Records Acts do not provide equivalent protection as the federal FOIA, the terms of the federal FOIA should apply to any broadband outage information.”); Comtech Comments at 5 (noting that “NORS is not designed for state use . . . and is not currently organized so that state specific data could be easily available”).

NARUC dismisses these concerns, arguing that “[a]ll the FCC has to do . . . is to condition access to the data on a State providing *some level of confidential treatment*.”⁷⁴ State agencies in California, Virginia, and Washington appear to take similar positions based on state-level confidentiality rules and procedures.⁷⁵ But such an unpredictable patchwork of disclosure requirements is exactly what worries Comcast and other NORS participants.⁷⁶ For example, the CPUC argues that state commissions should have direct access to NORS based only on a certification that they have “appropriate protections in place” to prevent public disclosure of NORS data.⁷⁷ But while the CPUC says it “remains committed to the FCC’s determination that information about outages in the telecommunications network should be kept confidential,” it hastens to add that California does not afford confidential treatment to information about outages in the electric grid and that it agrees with the FNPRM’s suggestion that the presumption of confidentiality for NORS reports “may need to evolve as networks, and consumer expectations about transparency, also evolve.”⁷⁸

⁷⁴ NARUC Comments at 5 (emphasis added).

⁷⁵ See *Petition of the California Public Utilities Commission*, ET Docket No. 04-35, at 17 (Nov. 12, 2009) (“CPUC Petition”) (requesting direct access to NORS based on a state’s certification “that it has appropriate protections in place . . . that would preclude disclosure of confidential NORS data to the public”); Virginia State Corporation Commission Comments at 7 (stating they “believe that the VSCC has the ability to provide any information designated as confidential the protection to which it ought to be afforded”); WUTC Comments at 2 (acknowledging confidentiality concerns but asserting that, “as important as confidentiality is, it should not be used as reason to prohibit access to the NORS by state and local jurisdictions”).

⁷⁶ See, e.g., AT&T Comments at 22-24 (urging the Commission to require states “to certify annually that providers’ outage reports are not subject to any state open-record laws”); CTIA Comments at 21 (recommending that the Commission “require each agency requesting access to outage data to evaluate and report on the specific state laws and regulations that will be used to protect NORS data”); USTA Comments at 16 (asserting that “any access by a state or federal agency . . . should be extremely limited” and that “[s]tate and federal agencies that are granted access to such information should be required to guarantee no less than the same level of confidentiality and protection provided by the Commission”).

⁷⁷ CPUC Petition at 17; see also CPUC Comments at 14-15.

⁷⁸ CPUC Comments at 14 (quoting FNPRM ¶ 145).

In light of inevitable variations in states' treatment of confidential information, Comcast is concerned that providing states with direct access to NORS would mark a significant and troubling "evolution" in the presumption of confidentiality – one that could seriously undermine longstanding expectations of nondisclosure based on uniform federal rules and policies. Again, these concerns would only be magnified with the inclusion of broadband outage data or cybersecurity-related data.

If the Commission nevertheless chooses to proceed with NORS information sharing, it must, at a minimum – as numerous commenters have cautioned – impose stringent nondisclosure requirements that leave no doubt that states remain bound by federal standards of confidentiality, and make sure other appropriate safeguards are in place *before* a state agency may receive NORS access.⁷⁹ As NCTA suggests, the Commission should: (1) limit access to the data to the few direct employees at each eligible state agency who process outage information; (2) prohibit individuals with access from using the information for any other purpose; and (3) prohibit individuals with access from sharing the information with other members of the eligible agency, any outside parties, or other federal, state, or local government agencies.⁸⁰ These and other controls proposed by industry commenters should be made an express and binding condition of states' access to NORS.⁸¹

⁷⁹ See, e.g., AT&T Comments at 22-24; ATIS Comments at 20-21; CenturyLink Comments at 18-19; CTIA Comments at 20-21; NCTA Comments at 24; USTA Comments at 15-16.

⁸⁰ See NCTA Comments at 25.

⁸¹ See AT&T Comments at 22-24 (recommending that the FCC limit access to certain state employees who complete security training and sign nondisclosure agreements and condition a state's access to NORS on that state agreeing not to impose state-specific outage reporting requirements on reporting entities); ATIS Comments at 20-21 (suggesting that access to NORS "should be provided only to those states . . . with reporting obligations that are consistent with Part 4 requirements and that have laws in place to prevent the disclosure of outage data and agree to abide by the confidentiality and other restrictions established by the Commission"); CenturyLink Comments at 18-19 (recommending that third parties be prohibited from accessing NORS data, that any use of the data must be within the agency's role

Moreover, the Commission should not hesitate to affirm that its Part 4 outage reporting processes and thresholds – including any obligations adopted for BIAS outage reporting in this proceeding – are part of a carefully tailored regulatory scheme involving jurisdictionally interstate services that leaves no room for conflicting obligations under state law.⁸² The Commission should give little credence to claims that states have an independent need to collect their own outage data, much less that states should be permitted to impose inconsistent reporting or disclosure requirements based on their own policy judgments.⁸³ In all events, there can be no doubt that stringent limitations on states’ access to and use of NORS data are necessary to promote federal regulatory goals.

VII. CONCLUSION

Commenters agree that broadband networks are resilient and designed to withstand the very types of outages that concern the Commission, calling into question the FCC’s premise for onerous new reporting requirements. If the Commission nonetheless adopts new outage reporting requirements, the record clearly illustrates that the rules should be narrowly crafted

of protecting health and public safety, and that the agency must immediately disclose to providers any breach or unauthorized release of NORS data); CTIA Comments at 20-21 (proposing periodic audits of state access to NORS, data breach notification requirements, and access controls to eliminate inactive account information); USTA Comments at 16 (recommending that access to outage data “should be limited to specifically identified state and federal agencies personnel with a need to know”).

⁸² Cf. *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601 ¶ 433 (2015) (establishing “a comprehensive regulatory framework governing broadband Internet access services nationwide” and announcing the Commission’s “firm intention to exercise our preemption authority to preclude states from imposing obligations on broadband service that are inconsistent with the carefully tailored regulatory scheme we adopt in this Order”).

⁸³ See CPUC Comments at 15-16 (arguing that “the CPUC in no way intended to waive its ability to seek this data independently and directly from providers pursuant to state law” and that states should have “the ability to obtain outage data directly from providers, as states see fit”); NARUC Comments at 5; Public Knowledge Comments at 1 (reiterating arguments that “mandatory reporting data should be made public rather than kept confidential” and encouraging the FCC to provide “news reporters, policy advocates and others engaged in public debate over the reliability of our critical communications infrastructure access to a reliable source of [outage] information”).

both to provide meaningful information to the Commission and limit the burdens and costs imposed on service providers. In this vein, commenters overwhelmingly agree that the Commission should require reporting only for hard-down, customer-impacting BIAS network outages, using a metric and reporting regime that mirrors the current VoIP approach. The Commission should not include a performance degradation threshold for reporting, extend any new rules to dedicated services, require BIAS providers to report on networks they do not own or control, or require separate cybersecurity reports. The record also shows that, if the Commission allows states to access NORS, numerous safeguards would be needed to ensure that the states protect and maintain the confidentiality the FCC affords to outage reports.

Respectfully submitted,

/s/ Kathryn A. Zachem

WILLKIE FARR & GALLAGHER LLP
1875 K Street, NW
Washington, DC 20006

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

LAWLER, METZGER, KEENEY
& LOGAN, LLC
1717 K Street, NW, Suite 1075
Washington, DC 20006

Counsel for Comcast Corporation

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

September 12, 2016