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 THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

William A. Check, Ph.D.
Senior Vice President, Science & Technology
and Chief Technology Officer

Matt Tooley
Vice President,
Broadband Technology

Rick Chessen
Steven F. Morris
Loretta P. Polk
Danielle J. Piñeres
National Cable & Telecommunications Association
25 Massachusetts Avenue, NW – Suite 100
Washington, DC 20001-1431
(202) 222-2445

August 26, 2016

Table of Contents

I. INTRODUCTION AND SUMMARY 1

II. THE COMMISSION SHOULD ADOPT HARD DOWN BIAS OUTAGE REPORTING REQUIREMENTS THAT PROVIDE MEANINGFUL INFORMATION ABOUT CONSUMER IMPACT 3

A. The Commission Should Focus On Hard Down Outages, Not Performance Degradation 4

B. The Commission Should Adopt a User Minutes Metric, Not Throughput, Packet Loss, or Latency 9

C. A Two-Step Reporting Process Beginning 24 Hours After an Outage Will Provide the Commission with the Most Accurate Outage Information While Minimizing the Burden on Providers 15

D. BIAS Providers Should Have No Obligation to Report On the Performance of Networks or Companies Over Which They Have No Control 16

E. Business Data Services Should Not Be Subject to Outage Reporting Requirements 18

III. THE COMMISSION SHOULD PRESERVE THE EXISTING REPORTING REQUIREMENTS FOR VOIP PROVIDERS 20

IV. THE COMMISSION SHOULD CONTINUE ITS POLICY OF STRICTLY PRESERVING THE CONFIDENTIALITY OF OUTAGE REPORTING DATA 22

V. THE COMMISSION SHOULD NOT ADDRESS CYBERSECURITY ISSUES IN THIS PROCEEDING 25

VI. CONCLUSION 28

I. INTRODUCTION AND SUMMARY

Cable operators' high speed Internet access networks are designed to limit customer-affecting outages. Today's robust networks use the latest technologies to build in significant redundancies that allow cable operators to deliver top-quality service to customers, even in the face of rapidly increasing demand and occasional infrastructure damage.

The Commission states that its goal in imposing, for the first time, outage reporting requirements on BIAS and other broadband providers is to "ensure reliability of broadband networks used to deploy critical communications services," particularly 9-1-1 and NG911 emergency communications.[1] Both the reporting metrics and approach proposed by the Commission, however, will not benefit consumers, are not tailored to identify widespread outages that prevent consumers from using services in an emergency, and would impose substantial and unnecessary costs on broadband providers and by extension their customers.

Rather than adopt its proposed approach, the Commission should only require BIAS providers to report hard down outages that actually result in a loss of all service to subscribers, not performance degradation as measured by throughput, latency, or packet loss. These metrics are primarily designed to assist broadband providers with network management or to define quality of service levels in commercial agreements, not to describe consumer-impacting outages. Each provider may use different means of monitoring service levels, which could create

---

[1] *Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications*; *New Part 4 of the Commission's Rules Concerning Disruptions to Communications; 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, Further Notice of Proposed Rulemaking, and Order on Reconsideration, 31 FCC Rcd 5817, 5856 ¶ 93 (2016) (*Order & FNPRM*).

inconsistent assessments and reporting of service degradation. Hard down outage information—measured in user minutes and reported in two steps—will, however, provide the Commission with the most accurate and consistent picture of consumers affected and will prove less burdensome for providers across different types of network configurations to measure and report.

The Commission also should not require broadband providers to report outages associated with their provision of business data services (BDS) or with the performance of networks or companies over which they have no control. Broadband providers have contracts with BDS customers that specify performance standards and reporting obligations and the Commission need not impose additional requirements. Also, because broadband providers lack access to the information necessary to submit meaningful reports on outages attributable to other companies' networks or services, the Commission should not require the submission of such reports.

The Commission should also reject its proposed changes to the outage reporting requirements for Voice over Internet Protocol (VoIP) providers. Decreasing the time to report, increasing the number and type of reports, and requiring reports on performance degradation, would impose a significant burden on industry, would result in the filing and withdrawal of unnecessary reports, and would not provide any benefit to consumers. The Commission rejected such stringent reporting requirements for VoIP providers in 2012 and has not adequately justified a departure from these relatively recent rules.

The National Cable & Telecommunications Association (NCTA) urges the Commission to continue to preserve the confidentiality of outage reporting data. The Commission has long treated this data as confidential, recognizing that it is both competitively sensitive and could reveal network vulnerabilities to those who would exploit them. The Commission should not

now depart from longstanding policy in order to share data with a broader audience, which would increase the risk that outage data is improperly accessed.

Finally, the Commission should not address cybersecurity issues in this proceeding. The cybersecurity of broadband networks is already under discussion in industry-led forums, including in the Commission's Communications Security, Reliability and Interoperability Council (CSRIC), the National Institute of Science and Technology's (NIST) Cybersecurity Framework, and the Communications Sector Coordinating Council (CSCC) as part of the public-private partnership with the Department of Homeland Security (DHS). Addressing cybersecurity in this proceeding would at best be duplicative and at worst would conflict with or detract from existing efforts.

II. THE COMMISSION SHOULD ADOPT HARD DOWN BIAS OUTAGE REPORTING REQUIREMENTS THAT PROVIDE MEANINGFUL INFORMATION ABOUT CONSUMER IMPACT

The Commission's primary goal in extending its outage reporting rules to broadband providers is to "ensure reliability of broadband networks used to deploy critical communications services," particularly 9-1-1 and NG911 emergency communications.[2] As explained in this section, the Commission's proposed approach will not serve this goal. Performance degradation is not a good proxy for outages that actually prevent subscribers from accessing broadband services and reports based on metrics such as throughput, latency, and packet loss would be too complex, inconsistent, and too costly to report.

---

[2] *Id.*

The Commission also need not and should not require BDS providers to submit outage reports to the Commission, or require any broadband provider to submit information regarding other companies' networks or services.

A. The Commission Should Focus On Hard Down Outages, Not Performance Degradation

The Commission should focus on identifying broadband outages that preclude customers from using services for emergency communications. Part 4 of the Commission's rules defines an outage as a "significant degradation in the ability of an end user to establish and maintain a channel of communications."[3] A focus on hard down outages is consistent with Part 4 and would provide the Commission with targeted information on outages that actually affect consumers' ability to contact emergency personnel through 9-1-1 and NG911 services.[4] It would also reduce the burden of new reporting requirements on providers, as it would be difficult, time consuming, and costly to collect the performance degradation information the Commission seeks.

In the BIAS context, a hard down outage is an event that causes customers to lose all broadband functionality. This type of event is the BIAS equivalent of the loss of a dial tone in the legacy voice context.

---

[3] 47 C.F.R. § 4.5(a).

[4] *See, e.g.*, *Order & FNPRM*, 31 FCC Rcd at 5862 ¶ 104 ("Given the potential for broad-scale, highly-disruptive outages in the broadband environment – and particularly those impacting 911 service – the adoption of updated broadband reporting requirements would likely provide the Commission with more consistent and reliable data on critical communications outages . . . . As NG911 functionality becomes centralized within broadband networks, network vulnerabilities specific to emergency services will emerge, and the Commission should be well-informed of such vulnerabilities.").

In contrast to hard down outages, degradation in the performance of a broadband network—as measured using packet loss, latency, or throughput—does not necessarily prevent communications by consumers and therefore does not accurately describe true outage events. A temporary increase in packet loss or latency or decrease in throughput—such as those due to normal operating mechanisms of the TCP protocol—likely would not affect end users at all, or might prevent only the use of certain services (video streaming, for instance) while leaving intact a consumer's ability to communicate with emergency personnel. Reports on degradation would in many cases provide the Commission with information that is not relevant to understanding and responding to outages that prevent consumers from contacting emergency services,[5] and therefore would not provide any benefit to consumers. Broadband performance degradation therefore should not trigger a reporting obligation.[6]

Performance degradation is also too complex an event to require reporting by broadband providers. Contrary to the suggestion in the *Order & FNPRM*,[7] broadband networks are inherently redundant and employ a variety of mechanisms to ensure the automatic routing and

---

[5] Indeed, many cable providers offer managed VoIP services separately from BIAS traffic over shared facilities, so BIAS packet loss and latency metrics are irrelevant to these customers' abilities to utilize VoIP services to access emergency services. Conversely, hard down outages would impact both managed VoIP and BIAS traffic.

[6] As discussed in further detail in Part V, below, NCTA also opposes the imposition of outage reporting obligations for cybersecurity-related events such as "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." *Order & FNPRM*, 31 FCC Rcd at 5869 ¶ 125. These network cybersecurity issues are best addressed in the context of existing voluntary, industry-led collaborations with government.

[7] *Id.* at 5861-62 ¶ 103 ("[B]roadband networks' interrelated architectural makeup renders them more susceptible to large-scale service outages.").

rerouting of information to minimize disruptions, congestion, and failures in connectivity. In addition to redundant fiber rings, routers, and optical node receivers, many networks use techniques like asymmetrical routing,[8] multipath TCP,[9] and Link Aggregation Groups[10] to manage traffic flow and maximize performance. However, traffic managed using these techniques may take different paths from subscriber to destination and back, or multiple, concurrent paths from subscriber to destination. It can therefore be very difficult to pinpoint the origin or root cause of performance degradation experienced by a particular consumer.

Because broadband networks are designed differently and different networks may operate in very different ways, imposing service degradation reporting obligations on providers would result in asymmetrical reporting obligations and the provision of inconsistent outage information. Inconsistent reports across providers would not provide the Commission with an accurate or

---

[8] "In Asymmetric routing, a packet traverses from a source to a destination in one path and takes a different path when it returns to the source." Arvind Durai, *Asymmetric Routing and Firewalls*, Cisco (2008), http://www.cisco.com/web/services/news/ts_newsletter/tech/chalk talk/archives/200903.html.

[9] Multipath TCP allows routers to distribute packets associated with one stream of information over multiple paths, "automatically—and quickly—adjust[ing] to congestion in the network, moving traffic away from congested paths and toward uncongested paths." Iljitsch van Beijnum, *Multipath TCP*, IETF J. (Sept. 2009), http://www.internetsociety.org/articles /multipath-tcp.

[10] Link aggregation allows network operators to logically aggregate multiple physical links together to form a single layer interface to load balance traffic across the interface. Link aggregation groups improve link availability because each group contains multiple redundant links. *See* JUNIPER NETWORKS, *Understanding Aggregated Ethernet Interfaces and LACP* (2015), http://www.juniper.net/documentation/en_US/junos15.1/topics/concept/interfaces-lag-overview.html.

complete picture of systematic problems and therefore would not achieve the Commission's goals in this proceeding.

Service degradation experienced by consumers may also be attributable to parties other than, and unknown to, a broadband provider, such as web sites, cloud providers, or transit networks. "There are multiple . . . elements (both on the home and server side) that are not directly controllable by the broadband access provider that can and do have a significant impact on the quality of the user experience."[11] Accordingly, "ISP-only measurements may present a picture that is at best, incomplete, and at worst, misleading, at least in terms of understanding overall [quality of experience] impact."[12] However, because other providers often do not inform broadband providers of problems in their networks or applications, broadband providers cannot accurately monitor, report, or control such events. As discussed in further detail in Part II.D, below, broadband providers should not be required to report outages or degradation attributable to other providers.

To the extent that the Commission wishes to obtain real-time, consumer-focused information about network performance degradation to complement BIAS providers' reports on hard down outages, such information is already readily accessible from a variety of sources. One such source of information is publicly available from RIPE (Réseaux IP Européens), the

---

[11] Bill Lehr, et al., *Measuring Internet Performance When Broadband Is the New PSTN*, at 13-14 (2012), https://www.measurementlab.net/publications/measuring-internet-performance .pdf (*Measuring Internet Performance*).

[12] Jason Livingood, *The Need for a New Global Internet Measurement Platform*, QoE Workshop Paper, at 2 (2015), http://aqualab.cs.northwestern.edu/component/attachm ents/download/613.

European Regional Internet Registry. RIPE's "Atlas" project[13] employs a global network of more than 9,000 probes installed on various providers' networks to measure and provide public information regarding Internet connectivity and reachability, including round trip time.[14] RIPE's Routing Information Services can also be used to show "end-to-end connectivity issues that users actually experience" by providing information on network interconnection points.[15] All the test measurement results generated by the RIPE Atlas probes are publicly available in real-time using industry standard application programming interfaces. Case studies demonstrate that RIPE data was successfully used to detect Internet outages, including an outage referenced in the *Order & FNPRM* and the impact of Superstorm Sandy on Internet access in the United States.[16] In addition, the Commission manages the Measuring Broadband America (MBA) initiative, which provides annually the results of rigorous broadband performance testing for thirteen of the

---

[13] RIPE ATLAS, https://atlas.ripe.net.

[14] RIPE ATLAS, *Frequently Asked Questions (FAQ): What data to the probes collect?*, RIPE Network Coordination Centre, https://atlas.ripe.net/about/faq/#what-data-do-the-probes-collect.

[15] RIPE NNC, *FAQ: Routing Information Services: How Can RIS Data be Used?*, https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/faq-ris.

[16] *See* Emile Aben, *Time Warner Cable Outage*, RIPE NCC (Aug. 28, 2014), https://labs.ripe.net/Members/emileaben/time-warner-cable-outage; Emile Aben, *RIPE Atlas: Hurricane Sandy and How the Internet Routes Around Damage*, RIPE NCC (Nov. 12, 2012), https://labs.ripe.net/Members/emileaben/ripe-atlas-hurricane-sandy-global-effects; *see also* Romain Fontugne, *Pinpointing Delay and Forwarding Anomalies Using RIPE Atlas Built-in Measurements – Or How I Learned to Stop Worrying and Love the Built-Ins*, RIPE NCC (May 18, 2016), https://labs.ripe.net/Members/romain_fontugne/pinpointing-delay-and-forwarding-anomalies-in-ripe-atlas-built-in-measurements (describing a method to use large numbers of traceroute measurements available from RIPE to detect network disruptions).

largest wireline broadband providers.[17] The MBA Report tracks the average packet loss and latency for each participating BIAS provider, grouped by technology,[18] and is the source of the most comprehensive directly measured national consumer broadband performance data available. Finally, the Interconnection Measurement Project, managed by Princeton University, gathers and analyzes data from seven participating BIAS providers that have installed a common tool to measure traffic at their interconnects.[19] Crowdsourced data like these, when properly designed and implemented, can be a supplement to the data that the Commission collects through outage reporting and their importance could grow as the scope and detail of such data increase.

B. The Commission Should Adopt a User Minutes Metric, Not Throughput, Packet Loss, or Latency

The metrics proposed by the Commission for defining a reportable outage would require the collection of data not easily accessible to providers and would not provide clear insight into network outages that actually preclude use by customers. Rather than adopting new metrics for which there is no clear standard and no clear measurement regime, the Commission would be better served by using the familiar "user minutes" approach.

---

[17] FCC, *Measuring Broadband America*, https://www.fcc.gov/general/measuring-broadband-america.

[18] FCC, *2015 Measuring Broadband America Fixed Broadband Report*, at 17-18 (2015), http://data.fcc.gov/download/measuring-broadband-america/2015/2015-Fixed-Measuring-Broadband-America-Report.pdf.

[19] Princeton University, Center for Information Technology Project, *Interconnection Measurement Project*, http://interconnection.citp.princeton.edu.

For hard down outages, the Commission proposes a complicated throughput-based reporting criterion focusing on "the number of Gbps minutes affected by the outage"[20] that the industry does not currently use to gauge the impact of outages on customers.[21] The proposal would seem to produce odd results, where 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. Although the Commission adopted a capacity-based metric—first, the "DS3 minute," now the "OC3 minute"—to define a threshold for reporting outages of major transport facilities, that metric was never designed to capture customer impact.[22]

Instead of the approach proposed in the *Order & FNPRM* and in keeping with a consumer-focused approach, the Commission should adopt the standard user minutes metric used to report outages in legacy services. Specifically, a hard down BIAS outage—meaning the lack of a broadband "dial tone"—should be reportable when it impacts a BIAS account for a specific period of time and affects a set number of user minutes. But in no event should such reporting

---

[20] *Order & FNPRM*, 31 FCC Rcd at 5871 ¶ 130.

[21] The Commission notes that Comcast proposed a "bandwidth-based standard" in the context of major transport facility outage reporting. *Id.* at 5870 ¶ 129. Given the considerable differences between major transport services and BIAS, the Commission should not assume that a proposal in one context would be appropriate in the other.

[22] *New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16,830, 16,899 ¶ 135 (2004) (*2004 Part 4 Order*) ("The DS3 minute reporting requirement does not require the reporting carriers to make any effort to determine the actual or potential impact of the outage on end users or 'customers.'"); *see also Order & FNPRM*, 31 FCC Rcd at 5825 ¶ 17.

thresholds for BIAS be lower than the thresholds that apply to voice outages (*i.e.*, an outage that lasts at least 30 minutes and potentially affects at least 900,000 user minutes[23]).

Providers that offer other services subject to outage reporting obligations are already familiar with this approach, which would therefore require less training and fewer resources for personnel to implement. A focus on user minutes also seeks to quantify the actual impact on customers, in keeping with Part 4 and the Commission's goals in this proceeding. Finally, a threshold of at least 900,000 user minutes will help to minimize the impact of broadband reporting obligations on small providers that often have fewer personnel and equipment resources to dedicate to monitoring and reporting than larger providers.

For the reasons already described in Part II.A, in contrast to user minutes, performance degradation does not serve as a good proxy for determining when an outage prevents consumers from communicating with emergency personnel. Throughput, latency, and packet loss—all proposed by the Commission as metrics to evaluate performance degradation[24]—can serve as useful tools for some aspects of a provider's internal network monitoring but cannot be used to describe a functional loss of service to individual consumers.

Packet loss is a measure of how many data packets traveling between two end points fail to reach their destination. BIAS providers monitor packet loss data in order to determine how well a circuit between two elements is operating, but they do not and cannot track packet loss on an end-to-end basis between the customer and each possible destination of the customer's

---

[23] 47 C.F.R. § 4.9(f)

[24] *Order & FNPRM*, 31 FCC Rcd at 5873-75 ¶¶ 137-42.

traffic.[25] Latency is a measure of the time it takes a data packet to travel from one point to another. BIAS providers monitor latency of a sampling of end-to-end transactions as a proxy for network performance. Throughput is a measure of the amount of data moved between two points in a specific period of time. BIAS providers monitor throughput as part of capacity planning and traffic analysis, but typically not to determine whether a particular customer can reliably access the Internet.

None of these metrics, individually or in combination, would provide the Commission with accurate information on whether customers can access the Internet to contact emergency personnel. First, packet loss, latency, and throughput must be measured between two particular endpoints. BIAS providers focus primarily on aggregate or average data derived from several such end-to-end measurements. Although some BIAS providers can examine these metrics from a particular end user's perspective when a problem arises, it would be cost prohibitive for BIAS providers to monitor and collect throughput, latency, and packet loss information from every customer's perspective all of the time. In short, BIAS providers utilize these metrics to help assess certain aspects of overall network health, but these big-picture averages, or even the individual measurements for particular routes, would tell the Commission virtually nothing about a particular end user's connection, and provide no benefit to the consumer in relation to 9-1-1 and NG911 services.

---

[25] Moreover, IP networks by design drop packets in order to signal congestion and allow the Transmission Control Protocol (TCP) to adjust to optimize delivery rate for the available capacity. Once the protocol adjusts, transient packet loss disappears. In other words, some packet loss in a network is normal and desirable and while packet loss might measure short-term issues, it is not designed to capture longer duration problems like outages.

Second, there are a variety of factors apart from issues arising in a BIAS provider's network that impact the packet loss, latency, and throughput experienced by a particular customer. For example, these metrics can vary depending upon the sites and content that a customer accesses. They can also vary due to problems in other providers' networks that a customer's traffic must traverse before reaching its destination. Finally, throughput, packet loss, and latency measurements do not reflect compensation mechanisms that networks and applications build in to minimize the impact of network issues on the customer experience. For instance, because BIAS is a "best efforts" service, applications that ride over top of the Internet build in tools to minimize the impact of latency on the customer. Therefore, even when a network measurement signals less than optimal latency over a particular path in the network, the latency may not be perceived by the end user.

In short, a snapshot of packet loss, latency, or throughput data for a sample of connections within a BIAS provider's network will not provide the Commission with reliable information about a single customer's ability to use her broadband service. Furthermore, even if this data was suitable for identifying outages, it would be difficult and expensive to gather and report.

The Commission suggests that broadband providers have performance degradation data at their fingertips, ready to report,[26] but this simply is not the case. The costs associated with reporting outages based on packet loss, latency, or throughput would be significant. Although broadband providers do to some extent utilize these network performance indicators, no industry

---

[26] *Order & FNPRM*, 31 FCC Rcd at 5878-79 ¶¶ 150-53 ("Because providers already routinely collect much of this data, we believe that the cost of compliance of additional rules would be only the cost of filing additional reports.").

standard metric exists for judging when performance degradation crosses the line into an outage. Broadband providers use this information internally to make technical decisions about network management, but do not collect it in a reportable format or in a manner that would meaningfully describe any impact to consumers. As Bill Lehr, Steve Bauer, and David Clark of the Massachusetts Institute of Technology note, "[Internet service providers] . . . engage in significant performance measurements to facilitate real-time network management (e.g., load balancing, fault monitoring, and SLA verification tasks), network provisioning, and longer-term strategic planning and investment," but gathering and reporting outage information "is a non-trivial task . . . [because] neither the deployed systems nor the operational procedures have been designed with these reporting tasks in mind."[27] In addition, they explained that "[c]ollecting and transporting the raw data in real-time to the network operations center where it can be processed, analyzed, and managed presents a difficult challenge that incurs significant operational costs."[28] Deploying the additional equipment and manpower to turn monitoring into reporting would be significantly more costly than the Commission has estimated and would vastly exceed the benefits to be gleaned from this performance degradation information that may not reflect actual consumer impact.

---

[27] *Measuring Internet Performance* at 17, 23.

[28] *Id.* at 19.

C. A Two-Step Reporting Process Beginning 24 Hours After an Outage Will Provide the Commission with the Most Accurate Outage Information While Minimizing the Burden on Providers

The Commission should not, as it proposes, adopt a three-tier outage reporting system for BIAS providers or require that providers file an initial notification within 120 minutes.[29] A two-tier reporting structure with a notification report filed within 24 hours—as the Commission currently requires for VoIP providers[30]—strikes the right balance between timeliness of filing, accuracy of information, and burden on providers.

BIAS providers need at least 24 hours to identify reportable outages and gather sufficiently detailed information while still dedicating sufficient resources to service restoration. Due to the vast and interconnected nature of broadband networks, providers may not know within two hours whether an event constitutes a reportable outage, much less be able to provide the detailed information that the Commission seeks (such as the root cause of the outage). In fact, as providers noted in response to the Commission's Notice of Proposed Rulemaking on VoIP outage reporting (*VoIP NPRM*), short fuse notification requirements often result in over-reporting and cause providers to withdraw many reports when they later determine an event was not a reportable outage.[31] Requiring an initial notification report within two hours would also

---

[29] *Order & FNPRM*, 31 FCC Rcd at 5868 ¶ 121.

[30] 47 C.F.R. § 4.9(g).

[31] Comments of Verizon and Verizon Wireless at 15-16, PS Docket No. 11-82 (filed Aug. 8, 2011) (Verizon Comments); *see also* Reply Comments of MetroPCS Communications, Inc. at 3-4, PS Docket No. 11-82 (filed Oct. 7, 2011) (MetroPCS Reply Comments).

consume valuable personnel resources at a time when providers should be focused on service restoration.

As the Commission concluded in 2012 with respect to VoIP outages, a two-tier reporting system "reduce[s] the providers' workloads" while still providing the Commission with both early situational awareness and the opportunity to obtain full outage details within the same timeframe that it receives final reports from other service providers.[32] Requiring an interim report places a significant burden on providers with only minimal corresponding benefits. The Commission therefore should adopt a two-tier reporting system for hard down BIAS outages.

D. BIAS Providers Should Have No Obligation to Report On the Performance of Networks or Companies Over Which They Have No Control

The Commission seeks "comment on whether BIAS providers could be used as a central reporting point for all broadband network outages, i.e., whether our Part 4 assurance goals for broadband outage reporting can be effectuated through, or should be limited to, an approach in which only BIAS providers (as opposed to other entities providing networks or services) would be required to report."[33] BIAS providers do not have ready access to outage information for other network operators or application providers and the Commission should not impose a burdensome clearinghouse function on BIAS providers for its convenience.

The same robust redundancies and interconnections that make the Internet less vulnerable to outages than traditional networks also mean that consumer traffic most often transits multiple

---

[32] *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, 2688 ¶ 96 (2012) (*2012 Part 4 Order*).

[33] *Order & FNPRM*, 31 FCC Rcd at 5865 ¶ 112.

providers' networks before reaching the Internet backbone and its ultimate destination. In most cases, broadband providers have no knowledge of or control over outages on other providers' networks or failures in the Internet backbone. Consequently, broadband providers may not be able even to locate the source of the outage or to determine whether or not particular customers can access their services.

Moreover, Internet infrastructure includes not only so-called 'last mile' facilities, middle-mile transport and backbone facilities operated by broadband providers, but content delivery networks, server farms, and services operated by 'application' providers. Threats to Internet communications are global in scope and their source is at least as likely to originate or be associated with applications and content services as with the broadband facilities on which they are carried.[34] As with outages on the networks of underlying or peer providers, broadband providers have little to no ability to identify or report on disruptions in the application layer.

While the notion that BIAS providers could aggregate and supply information to the Commission on all events and failures that affect Internet service may have some surface appeal, such an approach is neither realistic nor fair. Broadband providers cannot be held responsible for identifying outages or other failures that originate on other providers' networks or are associated with the applications and content services of other providers.

---

[34] *See* Comments of the National Cable & Telecommunications Association at 9-10, PS Docket No. 11-82 (filed Aug. 8, 2011) (NCTA Comments).

E. Business Data Services Should Not Be Subject to Outage Reporting Requirements

The Commission proposes to impose outage reporting obligations not only on BIAS providers, but also on providers of "dedicated services" or BDS.[35] BDS contracts already contain negotiated performance standards and reporting obligations and the Commission need not impose additional requirements.

As the Commission recognizes, BDS is provided subject to "performance guarantees, such as guarantees for traffic prioritization, guarantees against certain levels of frame latency, loss, and jitter to support real-time IP telephony and video applications, or guarantees on service availability and resolving outages."[36] These contractual guarantees already provide strong market incentives for providers offering BDS to minimize outage events and performance degradation, as such events typically result in a service credit or other penalty on the service provider.

The Commission has not shown that the benefits of imposing outage reporting obligations on BDS providers would exceed the costs. The Commission claims that such reports will help it to "facilitate and promote systemic improvements to reliability,"[37] but fails to demonstrate that BDS customers are not receiving reliable service or how it could improve upon

---

[35] *Order & FNPRM*, 31 FCC Rcd at 5866-68 ¶¶ 114-20.

[36] *Business Data Services in an Internet Protocol Environment; Investigation of Certain Price Cap Local Exchange Carrier Business Data Services Tariff Pricing Plans; Special Access for Price Cap Local Exchange Carriers; AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, Tariff Investigation Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd 4723, 4728 ¶ 13 (2016).

[37] *Order & FNPRM*, 31 FCC Rcd at 5862 ¶ 104.

existing, market-driven mechanisms for enhancing network performance. For instance, providers' existing contracts drive them to provide consistently high standards of service today, and fierce competition among providers drives tomorrow's innovations in network operation. In such an environment, it is difficult to envision significant public benefits such as improved network performance or a reduction in outages deriving from the imposition of BDS outage reporting requirements.

As with BIAS providers, the Commission assumes that BDS providers already collect a host of data on quality of service metrics such as packet loss, latency, and jitter.[38] Although providers do generally on a periodic or as-needed basis discuss and/or notify some BDS customers in the event of disruptions, the specific information shared will vary depending upon the nature of the outage event, will be governed by specific agreements, and will be considered confidential and proprietary. Any such mutually agreed upon periodic sharing is substantially different from collecting and reporting outage data to the Commission. Adjusting existing operations to collect and report near real-time outage data would impose significant costs on BDS providers, which ultimately could increase the cost to the customer for these services. Absent a significant benefit from such reporting, the Commission should not impose these costs.

In short, there is no reason for the Commission to add to the requirements contained BDS providers' service level agreements, as outage reporting requirements would impose costly data gathering requirements on BDS providers without significant anticipated public benefits.

---

[38] *Id.* at 5879 ¶¶ 152-53.

III. THE COMMISSION SHOULD PRESERVE THE EXISTING REPORTING REQUIREMENTS FOR VOIP PROVIDERS

The Commission proposes to move from a two- to a three-tier reporting system for VoIP providers, to require submission of an initial notification within two hours instead of 24 hours, and to require VoIP providers to report significant performance degradation.[39] As explained below, the proposed changes are not warranted.

When the Commission first adopted hard down outage reporting requirements for VoIP providers in 2012, it concluded that the two-tier reporting system beginning 24 hours after an outage (with a tighter four-hour notification deadline only for 9-1-1 affecting outages) would "provide the Commission with the information it needs while reducing the reporting burden on providers."[40] The Commission explicitly adopted a longer (24 hour) outage notification interval for VoIP providers than for legacy service providers because "'data networks operate differently than voice networks, and the cause of some degradations of service may not be as clearly identifiable, which can lead to inaccurate reporting, or over-reporting, under strict time constraints.'"[41] It also adopted a two-report rather than a three-report system to reduce the burden on providers, concluding that an initial notification and final report provided the Commission with timely and sufficient information.[42]

The same reasoning applies today. Requiring providers to file a report too soon after an event leads to the provision of inaccurate or unnecessary reports. Even with the existing 24-hour

---

[39] *See Order & FNPRM*, 31 FCC Rcd at 5881-83 ¶¶ 160-65.

[40] *See 2012 Part 4 Order*, 27 FCC Rcd at 2677 ¶ 101.

[41] *Id.* at 2688 ¶ 95 (quoting MetroPCS Reply Comments at 3).

[42] *See id.* at 2688 ¶ 96.

notification requirement, NCTA's members often must withdraw initial notifications after concluding that an event did not constitute a reportable outage. As commenters noted in response to the initial *VoIP NPRM*, requiring providers to file a notification within two hours of an event also can result in the provision of incomplete or inaccurate information, and can detract from service restoration and recovery efforts.[43]

The VoIP outage described by the Commission in the *Order & FNPRM* does not, as the Commission claims, justify the imposition of more onerous reporting requirements but rather demonstrates that the existing VoIP outage reporting process is working exactly as the Commission envisioned. The Commission complains that it did not receive notice of one VoIP outage until 23 hours after its discovery. However, that notification was timely filed under the Commission's existing rules,[44] adopted a mere four years ago. The Commission does not explain what it would have done differently if it had been told of the outage sooner and it has given no persuasive reason why it now requires access to such notifications on an expedited basis. The existing rules provide for a shorter four-hour notification period when the outage might impact a special 9-1-1 facility, which "provides the Commission with timely situational awareness" "so that the agency can direct emergency response efforts appropriately."[45] The

---

[43] *Id.* at 2687-88 ¶ 94; *see also* MetroPCS Reply Comments at 5; Comments of Comcast Corporation at 3-4, PS Docket No. 11-82 (filed Aug. 8, 2011); NCTA Comments at 8; Comments of T-Mobile USA Inc. at 10, PS Docket No. 11-82 (filed Aug. 8, 2011); Verizon Comments at 14-16; Comments of the Voice on the Net Coalition at 8, PS Docket No. 11-82 (filed Aug. 8, 2011).

[44] 47 C.F.R. § 4.9(g)(ii) (requiring VoIP providers to submit an outage notification "[w]ithin 24 hours of discovering that they have experienced on any facilities that they own, operate, lease, or otherwise utilize, an outage of at least 30 minutes duration").

[45] *Order & FNPRM*, 31 FCC Rcd at 5881-82 ¶ 161.

current reporting structure and timing requirements strike the right balance between burden on providers and public benefit, and the right balance between timeliness and accuracy. Circumstances have not changed since 2012 in a manner that would justify the imposition of a three-tier reporting structure with tighter timeframes and the Commission should not do so.

The Commission also should not require VoIP providers to submit reports on performance degradation. In 2012, the Commission opted not to impose performance degradation reporting for VoIP providers, concluding that a focus on hard down outages "captures most of the expected benefits while avoiding the much larger costs."[46] As the Commission concluded in 2012, and for the same reasons described in detail in Part II.A-B above, performance degradation reporting obligations impose significant costs on providers that would not exceed the public benefits to be anticipated from such reports.

IV. THE COMMISSION SHOULD CONTINUE ITS POLICY OF STRICTLY PRESERVING THE CONFIDENTIALITY OF OUTAGE REPORTING DATA

In the *Order & FNPRM*, the Commission correctly recognizes the importance of protecting the confidentiality of outage data submitted to the Commission, noting that improper disclosure of such data would result in a "likelihood of substantial competitive harm" and would undermine the Commission's "national defense and public safety goals."[47] The Commission also recognizes that sharing data with other actors, including other state and federal agencies "raises a number of complex issues."[48] Nevertheless, the Commission seeks further comment on

---

[46] *See 2012 Part 4 Order*, 27 FCC Rcd at 2672-73 ¶¶ 55-56.

[47] *Order & FNPRM*, 31 FCC Rcd at 5848-49 ¶ 81 (internal quotations omitted).

[48] *Id.* at 5853-54 ¶ 89.

whether confidential outage information submitted by broadband providers should be accessible to other state and federal entities.[49] The Commission has a long and successful track record of preserving the presumptive confidentiality of outage reports and should not now put reports submitted by broadband providers at risk of disclosure by sharing them broadly with other state and federal agencies.

Since 2004, the Commission has treated outage reports as confidential.[50] At the time it adopted this rule, the Commission concluded that, "[g]iven 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, . . . there is a presumptive likelihood of substantial competitive harm from disclosure of information in outage reports."[51] It also noted that the potential benefits of disclosing the reports "are . . . substantially outweighed by the potential harm to the public and national defense that might result from disclosure."[52]

If the Commission adopts new reporting obligations for BIAS providers, there is no basis for departing from the Commission's longstanding policy of treating outage information as presumptively confidential. Indeed, preserving the confidentiality of these reports is more important than ever. Information can be shared so rapidly using modern communications technologies that outage data exposed in one accidental disclosure or intentional breach can

---

[49] *See id.* at 5876-77 ¶¶ 145-48.

[50] *2004 Part 4 Order*, 19 FCC Rcd at 16,855 ¶ 45.

[51] *Id.*

[52] *Id.*

travel quickly to all corners of the world. Moreover, the Commission has pointed to no evidence that the risk that these reports could "fall into the hands of terrorists who seek to cripple the nation's communications infrastructure" has diminished.[53] 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. Consequently, the Commission should not depart from its longstanding policy and should instead continue to treat outage reports as presumptively confidential and limit sharing to existing processes.

If the Commission determines that there are limited circumstances where it may be in the public interest to authorize a state agency to access confidential Network Outage Reporting System (NORS) data, it should clearly define those circumstances and require state agencies to submit a request for Commission approval explaining why they are eligible to receive the data, what they plan to do with it, and how they will protect the confidentiality of any data they receive. In the context of access to VoIP-only outage reports, NCTA previously suggested that the Commission would need to ensure that each such state agency had effective procedures in place to protect the confidentiality of outage data.[54] Stringent safeguards would be even more

---

[53] *Id.*; *see also Order & FNPRM*, 31 FCC Rcd at 5848-49 ¶ 81.

[54] Specifically, NCTA suggested that such safeguards should include requiring each state agency: (1) to certify that "'it will keep the data confidential and that it has in place confidentiality protections at least equivalent to those set forth in the federal Freedom of Information Act (FOIA)'"; (2) to provide a list of each agency employee that will have access to NORS information, and (3) to describe the training mechanisms in place to ensure that such employees understand the confidential nature of the data and the procedures put in place to protect it. Comments of the National Cable & Telecommunications Association at 2-3, PS Docket No. 15-80 (filed July 16, 2015) (quoting *Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Notice of Proposed Rulemaking, Second Report and Order and Order on Reconsideration, 30 FCC Rcd 3206, 3224 ¶¶ 51-53 (2015)).

critical with the potential addition of broadband outage data or cybersecurity information. For instance, recognizing that the risk of accidental disclosure or data breach inevitably increases as the number of individuals with access to data increases, the Commission should limit the individuals at an eligible state agency who would have access to the data to the few people who process outage information. It would also be appropriate to prohibit individuals with access from using the information for any other purpose and from sharing the information with other members of the agency, any outside parties, or other federal, state, or local government agencies.

V. THE COMMISSION SHOULD NOT ADDRESS CYBERSECURITY ISSUES IN THIS PROCEEDING

The Commission seeks comment on whether it should expand its "definition of Part 4 outages to include 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," and proposes to modify NORS to support the submission of outage and disruption information associated with such cybersecurity failures.[55] NCTA respectfully submits that the outage reporting system is not the right venue for addressing cybersecurity issues. Several forums already exist for ongoing government and industry collaboration on the cybersecurity of communications infrastructure and a Commission-imposed reporting requirement could detract from or conflict with existing flexible, industry-driven approaches to cybersecurity.[56]

---

[55] *Order & FNPRM*, 31 FCC Rcd at 5869 ¶¶ 124-25.

[56] Notably, the U.S. Department of Homeland Security serves as the Sector Specific Agency for communications industry critical infrastructure. *U.S. Dep't of Homeland Security, About DHS, Organization, Operational and Support Components, National Protection and Programs Directorate, Office of Infrastructure Protection, Critical Infrastructure Sectors,*

The Commission's own CSRIC V has three working groups dedicated to cybersecurity in communications systems—WG5 (cybersecurity information sharing), WG6 (Secure Hardware and Software – Security by Design), and WG7 (Cybersecurity Workforce).[57] These working groups will build on the efforts of CSRIC IV's WG4, which last year issued a comprehensive report on cybersecurity risk management and best practices for communications networks.[58]

On a broader scale, NIST, as directed by Executive Order,[59] has collaborated with industry to develop a nationwide, voluntary cybersecurity framework.[60] The framework "enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure," and recognizes that "[o]rganizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances

---

Communications Sector, Sector Specific Plan (2016), https://www.dhs.gov/communications-sector.

[57] FCC, *Communications Security, Reliability and Interoperability Council V*, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability.

[58] The Communications Security, Reliability and Interoperability Council IV, *Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report* (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (*CSRIC Cybersecurity Report*).

[59] Exec. Order No. 13,636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

[60] NIST, *Cybersecurity Framework, Background: Framework for Improving Critical Infrastructure Cybersecurity*, http://www.nist.gov/cyberframework/.

– and how they implement the practices in the Framework will vary."[61] The CSCC also deals with cybersecurity risks to critical communications infrastructure, providing a venue for companies to "help develop and share best practices for protecting critical assets and functions, have access to early warning about threats, collaborate on incident mitigation and gain enhanced capabilities in restoration and continuity."[62]

The NIST, CSRIC, and CSCC processes focus primarily on industry-developed, voluntary best practices for managing cybersecurity risk, recognizing that there is no one-size-fits-all approach for cybersecurity. A Commission-imposed requirement on all broadband providers to monitor specific cybersecurity threats such as software and firmware issues or unintended modifications to a database—particularly when providers can manage such risks in a way that does not impact consumers—would conflict with the collaborative and flexible approach that government and industry have taken to date. Moreover, outage reporting requirements in such circumstances would prove duplicative when the CSRIC and NIST recommendations already contain voluntary information sharing procedures.[63] The Commission therefore should not address cybersecurity issues in this proceeding.

---

[61] NIST, *Framework for Improving Cybersecurity*, Version 1.0, at 1-2 (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (NIST Framework).

[62] U.S. COMMUNICATIONS SECTOR COORDINATING COMMITTEE, *FAQ: Why Should My Business Join the CSCC?*, http://www.commscc.org/faq/.

[63] *See, e.g.*, *CSRIC Cybersecurity Report* at 10, 29, 30 ("CSRIC recommends that the FCC promote the sustained voluntary collaboration and facilitate the sharing of cybersecurity threat information."); NIST Framework at 33 ("Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.").

VI. CONCLUSION

In order to ensure that the Commission receives the most meaningful and accurate information about consumer-impacting broadband and VoIP outages while limiting the reporting burden on service providers, the Commission should: (1) limit broadband reporting to hard down outages measured in user minutes, not performance degradation measured in throughput, packet loss, or latency; (2) require only two, not three reports, the first of which should be filed within 24 hours; (3) not require BDS providers to file outage reports; (4) preserve the existing reporting structure for VoIP providers; (5) continue to protect the confidentiality of outage data; and (6) not address cybersecurity issues in this proceeding.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Steven F. Morris
Loretta P. Polk
Danielle J. Piñeres
National Cable & Telecommunications Association
25 Massachusetts Avenue, NW – Suite 100
Washington, DC 20001-1431
(202) 222-2445

William A. Check, Ph.D.
Senior Vice President, Science & Technology and Chief Technology Officer

Matt Tooley
Vice President,
Broadband Technology

August 26, 2016