

DOCKET FILE COPY ORIGINAL

Before the  
Federal Communications Commission  
Washington, D.C. 20554

MAILED  
APR 12 2011  
FCC Mail Room

In the Matter of	)	
	)	
Reliability and Continuity of Communications Networks, Including Broadband Technologies	)	PS Docket No. 11-60
	)	
Effects on Broadband Communications Networks of Damage or Failure of Network Equipment or Severe Overload	)	PS Docket No. 10-92
	)	
Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks	)	EB Docket No. <u>06-119</u>

NOTICE OF INQUIRY

Adopted: April 7, 2011

Released: April 7, 2011

Comment Date: July 7, 2011

Reply Comment Date: September 1, 2011

By the Commission: Chairman Genachowski and Commissioners Copps, McDowell, Clyburn, and Baker issuing separate statements.

TABLE OF CONTENTS

Heading	Paragraph #
I. INTRODUCTION .....	1
II. BACKGROUND .....	7
III. NOTICE OF INQUIRY .....	14
A. Continuity of Service .....	15
B. Reliability and Resiliency .....	27
C. Action by the Commission .....	43
D. Legal Authority .....	49
IV. PROPOSED TERMINATION OF RELATED PROCEEDINGS .....	51
V. CONCLUSION .....	52
VI. PROCEDURAL MATTERS .....	53
A. Ex Parte Presentations .....	53
B. Comment Filing Procedures .....	54
C. Accessible Formats .....	55
VII. ORDERING CLAUSE .....	56

## I. INTRODUCTION

1. By this Notice of Inquiry (“Notice”), we seek comment on a broad range of issues regarding the reliability and resiliency of our Nation’s communications networks. Specifically, we consolidate several lines of inquiry broadly derived from initiatives set forth in the National Broadband Plan (“*NBP*”)<sup>1</sup> regarding the reliability and continuity of our Nation’s communications infrastructure, including broadband networks. Among other matters, the *NBP* identified the inadequacy of backup power and insufficient communications backhaul redundancy as key factors that contribute to the congestion or failure of commercial wireless data networks, particularly during emergencies such as large-scale natural and man-made disasters.<sup>2</sup> The *NBP* also recommended that the Commission engage in an exploration of the reliability and resiliency standards being applied to broadband networks in order to ascertain what action, if any, the Commission should take to bolster the reliability of broadband infrastructures.<sup>3</sup>

2. In this Notice, we initiate a comprehensive examination of issues regarding the reliability, resiliency and continuity of communications networks, including broadband technologies. First, we explore the ability of communications networks to provide continuity of service during major emergencies, such as large-scale natural and man-made disasters. Next, we consider issues related to broadband network reliability and resiliency in the context of whether standards might be needed to ensure adequate levels of service to meet public safety and other critical infrastructure needs. Third, we discuss what actions, if any, the Commission should take to foster improved performance with respect to the reliability and continuity of operations. Fourth, we seek comment on the sources of legal authority that could provide the basis for Commission action. Finally, we seek comment on whether, for the reasons discussed below, we should consolidate two of the above-captioned proceedings -- PS Docket 10-92 (*Effects on Broadband Communications Networks of Damage or Failure of Network Equipment or Severe Overload*), and EB Docket 06-119 (*Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*) -- into this proceeding. Were we to consolidate these proceedings into this Notice, we seek comment on whether we should then terminate those two proceedings. If we decide to terminate those proceedings, we would consider the record in those proceedings, to the extent relevant, in this proceeding.

3. We address the matters raised herein against the backdrop of today’s increasingly interconnected world, one in which communications services, including broadband technologies, play a critical role in all segments of our Nation’s society and economy. As the communications infrastructure migrates from older technologies to broadband technology, critical communications services will be carried over a communications network infrastructure that may or may not be built to the high carrier grade<sup>4</sup> standards of legacy wireline systems. This potential for differences in service reliability could be a major source of concern for critical sectors, such as energy and public safety, and for consumers in general.

---

<sup>1</sup> Omnibus Broadband Initiative, Federal Communications Commission, *Connecting America: The National Broadband Plan* (“*NBP*”) (Mar. 2010).

<sup>2</sup> *NBP*, Chapter 12 (“Energy and the Environment”), Section 12.1 (“Broadband and the Smart Grid”).

<sup>3</sup> *NBP*, Chapter 16 (“Public Safety”), Section 16.2 (“Promoting Cybersecurity and Protecting Critical Infrastructure”).

<sup>4</sup> Although not a precise term of art in the telecommunications field, “carrier grade” generally refers to systems, hardware, or software that are extremely reliable, well tested, and proven in their capabilities.

4. Businesses rely on communications to conduct financial and other transactions, and hospitals and healthcare providers rely on communications services to provide medical care. Government agencies, at all levels, rely on communications services to ensure the safety of the public and to provide other services, while power companies and other utilities use communications services for their operations and to deploy energy-efficient technologies. Many of these sectors are becoming increasingly reliant on broadband-based technologies. For example, power companies are looking to broadband technologies as they begin to deploy Smart Grid.<sup>5</sup> Hospitals and healthcare providers can leverage broadband technologies for video consultation, remote patient monitoring, and better access to electronic healthcare records.<sup>6</sup> Financial institutions use broadband technology to clear large volumes of transactions to keep the economy running efficiently. Moreover, consumers increasingly are relying on broadband platforms in addition to, or in place of, legacy platforms for voice communications.<sup>7</sup>

5. Thus, it is vital that our Nation maintains a communications network that offers reliable and resilient service in the face of significant equipment or system failure, and which is sufficiently survivable to provide some continuity of service during major emergencies, regardless of whether the network is legacy or broadband-based. This is critically important in emergencies that occur during major natural or man-made disasters, including terrorist attacks, when access to communications services increasingly becomes a matter of life or death. People dialing 9-1-1, whether using legacy or broadband-based networks, must be able to reach emergency personnel for assistance; and when networks dedicated to public safety become unavailable, first responders must have access to commercial communications, including broadband technologies, to coordinate their rescue and recovery efforts. Hospitals require reliable communications to provide emergency medical care. Other critical infrastructure providers, such as power companies, must have reliable communications services to aid in their own repair and restoration efforts. Finally, organizations and individuals alike must have access to communications services to reach emergency responders during and following a major disaster. Individuals must also have some way to contact affected family members and loved ones.

6. By commencing this inquiry today, we seek to establish a dialog with all interested stakeholders, including network operators and other communications service providers; public safety and other Federal, state, tribal, territorial and local governmental agencies; hospitals and healthcare providers; consumers; and other critical infrastructure providers, such as utility companies. We believe that these efforts will serve the public interest by establishing a foundation for future initiatives designed to maximize reliable and resilient communications for the benefit of all Americans, particularly with respect to public safety and national security concerns.

## II. BACKGROUND

7. In recent years, the Commission has engaged in several efforts involving the overall reliability and resiliency of the Nation's telecommunications and broadband network infrastructure.

8. Two ongoing efforts of note include the Network Outage Reporting System (NORS) and

---

<sup>5</sup> See, e.g., *Communications Requirements of Smart Grid Technologies*, United States Department of Energy, October 5, 2010 ("DOE Smart Grid Report"), available at: [http://www.gc.energy.gov/documents/Smart\\_Grid\\_Communications\\_Requirements\\_Report\\_10-05-2010.pdf](http://www.gc.energy.gov/documents/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf)

<sup>6</sup> See *NBP*, Chapter 10, "Health Care."

<sup>7</sup> See, e.g., *NBP*, Chapter 3 ("Current State of the Broadband Ecosystem"); see also *Preserving the Open Internet, Broadband Industry Practices*, GN Docket No. 09-191, WC Docket No. 07-52, Report and Order, 25 FCC Rcd 17905, 17916 ¶ 22 (2010).

the Disaster Information Reporting System (DIRS). In operation since 2004, NORS is a mandatory information reporting system that collects service outage information filed primarily by voice and paging communications providers subject to Part 4 of our Rules.<sup>8</sup> Through analysis of these reports, the Commission looks for trends that could identify systemic weaknesses in our Nation's communications infrastructure and attempts to identify patterns and explore potential solutions concerning the underlying causes of significant network outages. DIRS is a voluntary, web-based system activated on a case-by-case basis that communications providers can use to report communications infrastructure status and situational awareness during times of crisis.<sup>9</sup>

9. More recently, in March 2010, the *NBP* was released with a goal of ensuring that every American has access to broadband capability particularly in underserved areas.<sup>10</sup> Among other matters, the *NBP* addressed issues broadly related to critical infrastructure preparedness and survivability, and recommended that the Commission investigate the resiliency and reliability standards of communications networks, particularly broadband networks.<sup>11</sup> In this regard, it identified the twin issues of inadequate backup power and insufficient communications backhaul redundancy as significant factors that have been shown to impair the reliability of commercial networks for mission-critical control applications.<sup>12</sup> The *NBP* also recommended that the Commission explore the reliability and resiliency standards being applied to broadband networks to ascertain what action, if any, the Commission should take to bolster the reliability of broadband infrastructures.<sup>13</sup> Furthermore, the *NBP* recommended that the Commission explore the survivability of commercial broadband communications networks to determine whether commercial communications service providers, including broadband providers, have adequate measures in place to maintain operations during major emergencies.<sup>14</sup>

10. In April 2010, in response to recommendations in the *NBP*,<sup>15</sup> the Commission adopted a Notice of Inquiry ("*Survivability Notice*") concerning the survivability of broadband communications networks.<sup>16</sup> In the *Survivability Notice*, the Commission sought comment on the impact of direct physical

---

<sup>8</sup> Providers subject to the Part 4 outage reporting rules include those providing voice or paging services using wireline, wireless, cable, or satellite facilities. See 47 C.F.R. Part 4, "Disruptions to Communications."

<sup>9</sup> Examples include information on the status of broadcast facilities (AM, FM, and TV), cable television, wireless cell sites by county, wireline and wireless facilities, and others.

<sup>10</sup> The *NBP* includes a detailed strategy for achieving affordability and maximizing use of broadband to advance consumer welfare, civic participation, public safety and homeland security, community development, health care delivery, energy independence and efficiency, education, employee training, private sector investment, entrepreneurial activity, job creation and economic growth, and other national purposes. See *NBP* at XI.

<sup>11</sup> See *NBP*, Chapter 16, Recommendation 16.12.

<sup>12</sup> See *NBP* at 251. More specifically, it addressed the potential reliance on commercial network data communications for Smart Grid and other power technologies and stated that the lack of mission-critical wide-area broadband networks capable of meeting the requirements of the Smart Grid threatens to delay the implementation of such technologies.

<sup>13</sup> *NBP*, Chapter 16 ("*Public Safety*"), Section 16.2 ("*Promoting Cybersecurity and Protecting Critical Infrastructure*").

<sup>14</sup> *Id.* at Recommendation 12.1 (cross-referencing Chapter 16 "*Public Safety*").

<sup>15</sup> See *NBP*, Recommendation 16.10.

<sup>16</sup> *In the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload*, Notice of Inquiry, PS Docket No. 10-92 ("*Survivability Notice*"), 25 FCC Rcd 4333 (2010).

damage and severe overload to broadband communications networks. Several commenters raised concerns about the reliability of commercial communications systems during major emergencies and expressed support for the Commission's examination of the backup power issue.<sup>17</sup> Other commenters stated that communications network providers adequately engineer and manage their networks to ensure survivability and redundancy on their own initiative, and that, apart from fostering voluntary industry efforts toward improvement, there is no need for regulatory intervention by the Commission.<sup>18</sup>

11. In February 2011, in a somewhat different context, the Commission adopted a Notice of Proposed Rulemaking ("*Form 477 NPRM*") that seeks comment on modernizing its Form 477 data program.<sup>19</sup> Established in 2000, Form 477 is the Commission's primary tool for collecting data about broadband and local telephone networks and services.<sup>20</sup> The form presently requires providers of broadband service, local telephone service, interconnected Voice over Internet Protocol (VoIP) service, and mobile telephone service to report the number of subscribers they have in their respective service areas.<sup>21</sup> Among other matters, the *Form 477 NPRM* seeks comment on whether additional data collections relating to service quality and customer satisfaction are necessary to fulfill the Commission's goals.<sup>22</sup> More specifically, this part of the *Form 477 NPRM* focuses on retrospective data at a macro level regarding matters such as network downtime; the number of trouble reports or customer complaints regarding network performance or degradation; complaints regarding service provider customer care and billing; installation and repair intervals; and general customer satisfaction.<sup>23</sup> The Notice we adopt today, by comparison, takes a distinct, but complementary, approach to addressing reliability and resiliency concerns by focusing in a more granular fashion on prophylactic technical and procedural measures that might prospectively improve performance in these areas.

12. In January 2006, the Commission established the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks ("*Katrina Panel*" or "*Panel*").<sup>24</sup> The *Katrina Panel* was charged with reviewing the impact of Hurricane Katrina on all sectors of the telecommunications and media industries, including public safety communications. The *Katrina Panel*

---

<sup>17</sup> See, e.g., various comments and reply comments filed in response to the *Survivability Notice*, including Initial Comments of Edison Electric Institute (filed June 25, 2010); Reply Comments of Utilities Telecom Council (filed Sept. 7, 2010); Reply Comments of Southern Company Services, Inc. (filed Sept. 7, 2010); Reply Comments of National Association of State Utility Consumer Advocates (filed Sept. 7, 2010); and Reply Comments of Financial Services Sector Coordinating Council (filed Sept. 8, 2010).

<sup>18</sup> See, e.g., Initial Comments of AT&T and of Alliance for Telecommunications Industry Solutions (ATIS), filed on June 26, 2010.

<sup>19</sup> *In the Matter of Modernizing the FCC Form 477 Data Program*, FCC 11-14, WC Docket No. 11-10; 07-38, adopted Feb. 8, 2011 ("*Form 477 NPRM*").

<sup>20</sup> *Local Competition and Broadband Reporting*, CC Docket No. 99-301, *Report and Order*, 15 FCC Rcd 7717, 7718, ¶ 1 (2000).

<sup>21</sup> *Local Telephone Competition and Broadband Reporting*, *Report and Order*, WC Docket No. 04-141, 19 FCC Rcd 22340, 22342-43, para. 3 (2004).

<sup>22</sup> See *Form 477 NPRM*, FCC 11-14, at ¶¶ 89-99.

<sup>23</sup> See *id.* at ¶ 98.

<sup>24</sup> *Notice of Establishment of the Commission's Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, 71 Fed. Reg. 933 (2006) ("*Katrina Panel*").

released its report (“*Katrina Panel Report*” or “*Katrina Report*”) on June 12, 2006.<sup>25</sup> The *Katrina Report* identified a lack of power or fuel to maintain operation of portions of the telecommunications system as a significant concern. The report also cited flooding and backhaul failure as two other primary contributors to the majority of telecommunications network disruptions.<sup>26</sup>

13. In 2007, acting on the findings of the *Katrina Panel*, the Commission issued an Order (“*Katrina Panel Order*”) directing the Public Safety and Homeland Security Bureau (“PSHSB”) to implement several recommendations of the Panel.<sup>27</sup> Among other actions, the Commission adopted rules requiring communications providers to ensure a minimum level of backup power capability to maintain network operations for a period of time after the failure of commercial power sources.<sup>28</sup> These rules, which were the subject of judicial challenge by several wireless providers, never took effect and were ultimately vacated by the U.S. Court of Appeals for the District of Columbia Circuit (D.C. Circuit) after the Commission communicated its intent to the court to revise them in further rulemaking proceedings.<sup>29</sup>

### III. NOTICE OF INQUIRY

14. In the following paragraphs, we discuss continuity of service during emergencies, as well as the reliability and resiliency of communications networks, including broadband technologies. We also explore options for possible action by the Commission and the sources of legal authority for any such action if the Commission were to decide to act. We also seek an analysis of the costs and benefits of the various matters raised in this inquiry. Thus, we ask commenters to address particularly the following concerns with respect to the numerous issues raised: What are the cost and benefits associated with any potential courses of action? How could any requirements the Commission might consider be tailored to impose the least amount of burden on those affected? What potential regulatory approaches (including market-based approaches such as permits and fees) would maximize the potential net benefits to society (benefits net of costs)? To the extent feasible, what explicit performance objectives should the

<sup>25</sup> *Independent Panel Reviewing Impact Of Hurricane Katrina On Communications Networks, Report And Recommendations To The Federal Communications Commission* (2006) (“*Katrina Panel Report*”), available at <http://www.fcc.gov/pshs/docs/advisory/hkip/karrp.pdf>.

<sup>26</sup> *Id.*

<sup>27</sup> *In the Matter of Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, Order, 22 FCC Rcd. 10541, 10565 (2007) (“*Katrina Panel Order*”), on recon., 22 FCC Rcd 18013 (2007), vacated, *CTIA v. FCC*, Nos. 07-1475 *et al.* (Order dated July 31, 2009).

<sup>28</sup> See 47 C.F.R. §§ 12.2, *et seq.* (2007) (“Redundancy of Communications Systems”).

<sup>29</sup> The Commission had provided that the rules would not take effect until the agency had published notice of approval from the U.S. Office of Management and Budget (“OMB”) under the Paperwork Reduction Act (44 U.S.C. 3501 *et seq.*) of the rules’ information collections. After the wireless petitioners filed their petitions for review challenging the backup power requirements, the D.C. Circuit issued an Order stating that the consolidated cases were not ripe for review and holding them in abeyance pending OMB’s action. *CTIA – The Wireless Association v. FCC*, 530 F.3d 984, 986, 989 (D.C. Cir. 2008). OMB disapproved the information collection, see Office of Mgmt. & Budget, Executive Office of the President, Notice of Office of Mgmt. & Budget Action (2008), available at [http://www.reginfo.gov/public/do/PRAViewICR?ref\\_nbr=200802-3060-019](http://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=200802-3060-019), and the Commission decided not to exercise its authority under the Paperwork Reduction Act to override the disapproval, see 44 U.S.C. § 3507(f)(1). Instead, the Commission filed a letter with the court stating its intent to revise the subject rules and requesting that the court dismiss the consolidated cases as moot. Letter from Nandan M. Joshi, Counsel for FCC, to Mark Langer, Clerk of the U.S. Court of Appeals for the District of Columbia Circuit (Dec. 3, 2008). In an unpublished opinion, the court ordered the petitions for review be dismissed as moot and vacated the challenged rules. *CTIA – The Wireless Association v. FCC*, No. 07-1475 (D.C. Cir. filed July 31, 2009).

Commission specify to facilitate monitoring the success of any potential course of action?

**A. Continuity of Service**

15. *Overview.* It is critical that our Nation have access to reliable and resilient communications networks, especially during times of major emergencies, such as large-scale natural and man-made disasters. As noted above, various reports and comments we have received in other proceedings have raised concerns that commercial communications networks may not be sufficiently reliable in such circumstances.<sup>30</sup>

16. In light of these concerns, we seek detailed information regarding any factors that significantly contribute to disruptions in communications service during major emergencies. We also seek comment on existing industry standards or practices that address these matters. We seek information on what preparatory or preventive measures are presently, or should be, taken by communications service providers to ensure that communications are maintained during major emergencies. We invite comment on the benefits and disadvantages of potential solutions to ensure continuity of service. We also seek comment on how the benefits of any regulatory requirements might be quantified, as well as on the cost of implementing such solutions, who would bear the cost, and how. Our objective is to evaluate existing industry standards and practices and to determine what actions, if any, the Commission should take to ensure that the public continues to have access to communications during major emergencies.

17. *Discussion.* We recognize that the ability of communications providers to continue operation during major emergencies is affected by many complex considerations. Lack of backup power and inadequate backhaul redundancy have already been identified as two leading factors. We address these two concerns in greater detail below. However, to consider the entire ecosystem of relevant factors, we begin with a more general inquiry. Specifically, we ask commenters to provide detailed information about any other factors the Commission should consider in this proceeding in addition to the concerns just mentioned. What is the precise nature of these other factors? Under what circumstances do they arise? What approaches does industry follow to avoid or mitigate them?

18. For example, the *Katrina Panel Report* found that lack of access to carrier sites located within disaster areas was a major issue impacting the ability of carriers to restore communications following Hurricane Katrina.<sup>31</sup> Since then, the Federal government and various states, particularly in the Gulf region, have taken steps to address this issue.<sup>32</sup> We seek comment on whether communications service providers have seen improvement in their ability to restore communications during recent hurricanes and other events. If not, what approaches could be taken to alleviate such problems in the future?

---

<sup>30</sup> See *id.* See also *DOE Smart Grid Report*, *supra* n. 2; *Katrina Panel Report* at 5, *et seq.*

<sup>31</sup> This was particularly problematic during the recovery efforts after Hurricane Katrina and severely limited access to affected sites. See *Katrina Panel Report*, *supra* note 8, at 15–17.

<sup>32</sup> For example, the Commission's Public Safety and Homeland Security Bureau has worked with the Department of Homeland Security and the Gulf States on this issue as instructed by the Commission in the *Katrina Panel* proceeding, and it is our understanding that some states now have written plans in place to allow access to carrier sites during and after emergencies. We further note that the Security and Accountability for Every Port Act of 2006 ("Safe Port Act") includes a section amending the Robert T. Stafford Disaster Relief and Emergency Assistance Act ("Stafford Act") (42 U.S.C. § 5170) by adding to the end of the Stafford Act provisions designed to promote greater access to disaster sites by an "essential service provider," which is defined as an entity that provides telecommunications service (or other utilities such as electric, water, sewer, and natural gas). See *Safe Port Act*, Pub. L. 109-347, Title VI, § 607, 120 Stat 1884, 1941-1942.

19. The *Katrina Panel Report* also found that flooding was another significant factor that impeded the ability of carriers to restore communications. We seek comment on the lessons learned in this regard since the *Katrina Panel Report*. For example, what, if any, preventive approaches to mitigate flooding have been identified? Which ones have been adopted or implemented by industry? What is the specific technical nature of these approaches? What are their advantages and disadvantages? What are the costs associated with these approaches? What additional measures could be taken to avoid or mitigate flood damage that could disrupt communications services? How would they be implemented? By whom?

20. We are also interested in gathering information about any other factors that have an impact on the ability to maintain or restore communications operations, including those which might be unique to specific circumstances. For example, which of these factors might be more significant with respect to smaller carriers, carriers serving rural areas, or those serving tribal lands? Similarly, what factors might be unique to broadband networks or to satellite systems and networks? Are there sufficient numbers of properly trained technical personnel to deploy over widespread disaster areas, and if not, is this a factor in not being able to maintain or restore operation of communications networks during emergencies? To what extent do these issues apply to communications infrastructure in geographically remote locations? Do communications service providers have contingency plans in place if key personnel are unavailable to respond to a situation, and if so, how are such contingency plans implemented? We invite commenters to address these and any other relevant factors.

21. Furthermore, we seek comment on any standards and best practices that presently exist in the industry regarding the provision of service during major emergencies. Who has developed these standards and best practices? What do they cover? Are they enforceable, and if so, how? What are the advantages, disadvantages, and costs of any such provisions? Are there other matters that are not covered by these standards and best practices that should be addressed, why, and how? We also seek information on any standards and best practices that network operators have developed to use in-house. Does the commercial communications sector make trade-offs during major disasters between network coverage and capacity? If so, what are the trade-offs? What would be the effect on capacity if a carrier gives priority to maintaining most of its radio frequency (RF) coverage footprint? How, and by whom, should access to communications infrastructure be managed in times of disaster? Who should be able to access what resources and in what quantities? What standards and best practices have other countries, Federal agencies, and state, tribal, territorial, or local governments developed that might prove useful here? We ask commenters to address any other significant considerations with respect to industry standards and practices, including any evolving trends and industry initiatives addressing the avoidance or mitigation of service disruptions in major emergencies.

22. With respect to preparatory and preventive measures, we invite commenters to provide details about measures industry presently uses to maintain or restore communications during emergencies, including their advantages and disadvantages and costs and benefits. How could such measures be employed most effectively? We particularly seek comment on what approaches would be best suited to activate emergency service continuity remotely for a period of time when direct human access to a site might not be possible during an emergency. How could standards and definitions for critical commercial communications infrastructure be aligned with similar performance objectives for dedicated public safety systems within a region? What mechanisms would provide the best opportunity to achieve such alignment? What would be the relative advantages and disadvantages and costs and benefits of such an approach?

23. *Backup Power.* We seek comment on how various backup power techniques or performance standards could or should be employed to ensure adequate levels of service continuity during major emergencies. Is there a need for specific backup power requirements? If the Commission were to

find there is a need for specific backup power requirements, what standards should it, or should it not, specify and why? Should the Commission specify minimum requirements for the duration of backup power capacity? Should the Commission consider adopting refueling requirements or standards for generators that may lack adequate standalone fuel capacity for the duration of a disaster? If the Commission were to find there is a need for specific backup power requirements, should they be uniform for all communications service providers or should there be different levels of backup for different services based upon other factors? If so, what factors should the Commission consider? For example, under what circumstances should backup power solutions be designed to maintain communications service throughout an entire service area or up to a certain percentage of a service area? What service levels should communications service providers maintain during such times and how would those levels be achieved? What criteria should the Commission use to determine which sites require backup power? Should backup power solutions be designed to maintain all types of communications; voice-only communications; text and video communications; telecommunications relay services, to ensure access by people with hearing or speech disabilities; and/or critical communications services such as 9-1-1 services and communications that support emergency response? Should the duration and level of quality of service requirements vary depending on whether the communications assets are located in areas more prone to disaster (e.g., Gulf Coast, West Coast)?

24. We note that, in the years since Hurricane Katrina, there have been many developments in back-up power technology. For example, cell sites have been designed to operate with lower power consumption, placing less of a strain on available sources of back-up power. Furthermore, solar cell technology has advanced and may be a viable option for back-up powering applications. To what extent are technologies like this in use today and how do they affect the ability of communications service providers to maintain service during power outages? Will such advances in back-up power technologies overtake traditional solutions like batteries and generators? If so, what steps, if any, would facilitate their adoption, and when should we expect such advances in back-up power technologies to overtake traditional solutions? How should the Commission consider these emerging technologies for the purposes of this inquiry?

25. We also seek comment on potential challenges to deploying backup power solutions. For example, during the *Katrina Panel* proceeding, carriers cited zoning and environmental laws and processes as major impediments to implementing certain backup power solutions.<sup>33</sup> Others noted restrictions in private leasing agreements.<sup>34</sup> In what manner do these potential impediments, or other related issues, present challenges to the deployment of backup power solutions? What other factors either encourage or discourage network operators from implementing backup power solutions? For example, to what extent is the cost of adopting adequate backup power solutions a factor, and how would this cost be borne? What challenges to deploying backup power solutions might be unique to small carriers or those serving rural parts of the country or tribal lands?

26. *Backhaul Redundancy.* As noted above, the *Katrina Panel Report* found that inadequate backhaul redundancy also plays a significant role in contributing to service disruptions during major emergencies. We ask commenters to address in detail whether and how this factor can impair operation of communications networks during major emergencies. What necessary services or key equipment (i.e., master control stations, master clocks and network time servers) would severely degrade or cause wireless

---

<sup>33</sup> See *In the Matter of Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, Order on Reconsideration, 22 FCC Rcd 18013, 18021 (2007) (“*Katrina Panel Order On Reconsideration*”).

<sup>34</sup> See *id.*

and wireline networks to be unavailable in the absence of backhaul redundancy? What are the relative advantages and disadvantages of different backhaul technologies in terms of technical feasibility and cost effectiveness? For example, what are the relative merits of microwave backhaul versus fiber with respect to capacity, cost, and vulnerability, and how would the merits of each vary with respect to aerial or buried plans in different types of terrain? What relative resiliency and reliability characteristics would these or other technologies have in different emergency situations, such as loss of primary grid power or major physical damage to network equipment or other infrastructure? How can the Commission ensure backhaul redundancy across multiple providers and companies when many communications service providers lease backhaul facilities from other companies?

## **B. Reliability and Resiliency**

27. *Overview.* Wireline communications networks have traditionally been designed and deployed to achieve carrier grade reliability in normal operation using a combination of highly failure resistant equipment and dedicated end-to-end connections. As such, major components in the network core, such as switches, are typically designed to meet downtime objectives not exceeding two minutes per year.<sup>35</sup> Wireline communications service providers also achieve very fast fault recovery times overall through heavy reliance on redundancy and automatic switchover throughout the network. By comparison, the Internet is based on Internet protocol (IP) technology which does not rely on such dedicated end-to-end connections. While this “connectionless” approach of IP theoretically offers a degree of built-in fault tolerance and resiliency to network failures, these benefits will not be fully realized if the underlying network infrastructure itself is not reliable on a network-wide scale. Moreover, as discussed more fully below, modified IP technology, such as Multiprotocol Label Switching (MPLS), is now widely deployed in broadband communications networks. It is unclear at this time what effect such modifications might have, either positive or negative, on the overall reliability and resiliency of broadband communications over IP-based networks.

28. At the same time, three major industry sectors are converging on ever more extensive use of broadband technologies: public safety, commercial communications, and utilities. As a result of this convergence, consumers of communications services at all levels may be generally unaware of the technological platform used to deliver their communications services; however, they typically expect the same level of service and service reliability regardless of the platform. Furthermore, as our communications infrastructure migrates from older technologies to IP-based broadband technology, there are concerns that critical communications services are more likely to be carried over a communications network that in fact might not possess the same high reliability standards as legacy wireline networks. This potential for a decline in service reliability and resiliency is a source of concern for critical sectors such as public safety, energy, and finance, as well as for the general public.<sup>36</sup> Our objective in this discussion is to determine what action, if any, the Commission should take to bolster the reliability of our Nation’s broadband communications platform. We therefore invite comment on whether or how the Commission should establish performance goals for resilient broadband networks under different scenarios.<sup>37</sup> We seek comment on the benefits and disadvantages of various approaches to ensuring reliable and resilient service. We also invite comment on the cost of implementing such performance goals and how such expenses would be borne. Moreover, we seek comment on what lessons, if any, the

<sup>35</sup> This exceeds what is colloquially known as “five nines” availability in the industry. This refers to 99.999% availability, or unavailability of 0.001%.

<sup>36</sup> See *NBP* at 322, Recommendation 16.12.

<sup>37</sup> In legacy networks, for example, every node has a performance objective contributing to overall end-to-end reliability. Resilient networks, therefore, tolerate failure while maintaining an overall performance goal.

Commission can learn from efforts at the state and local levels, as well as in other countries, to ensure reliable and resilient service.

29. *Discussion.* As an initial matter, we seek comment on whether one can safely assume that key elements of the Internet, such as its transport layer protocols and electronic equipment, when functioning as a whole, can offer the same carrier grade standards as legacy wireline systems under mission-critical conditions. For example, while carriers can use data retransmission and rerouting strategies to address certain network hardware reliability and resiliency problems, some transport protocols used to support quality of service in broadband networks do not take full advantage of these techniques.<sup>38</sup> In the rest of this section, we seek comment on both equipment and protocol-related issues that can compromise the reliability and resiliency of broadband networks for critical communications purposes.

30. *Equipment Reliability.* We seek comment on the nature of existing reliability standards used in the industry for critical components like top-level DNS servers, edge routers, gateway routers, core routers, and the like. Who promulgates and enforces such standards or practices? Are they voluntary or mandatory? Are these standards and practices adequate to address the reliability and resiliency concerns discussed here? Do manufacturers presently provide adequate estimates of relevant reliability data for major pieces of equipment that they develop? If not, should they be required to do so? Going forward, what kinds of equipment that are not presently covered by adequate reliability performance standards or best practices should be subject to such requirements?

31. We also seek comment on the parameters that existing standards or practices generally address. For example, do existing standards and practices apply downtime objectives or other reliability standards to major pieces of equipment in broadband networks? One source indicates that carrier class routers may be expected to have downtimes of less than 5.3 minutes per year.<sup>39</sup> To what extent does this downtime objective represent typical core routers in broadband networks? To what extent, if any, should the Commission apply downtime objectives to DNS servers, gateway routers, or other similarly critical equipment? If the Commission were to adopt downtime objectives or other reliability standards, what should they be? Alternatively, should the Commission set overall service goals, so that, for example, redundancy in the network would prevent a DNS service disruption if any ISP-operated DNS server went down?

32. *Protocol Issues.* We seek comment on how the particular characteristics of any given protocol could impair or enhance reliability for critical communications. We particularly seek comment on whether, and the extent to which, some protocols might be designed to emphasize one performance aspect, while inadvertently losing the ability to take full advantage of other intrinsic IP rerouting and retransmission features that could enhance overall reliability. Are there such trade-offs, and if so, how can they be identified? What metrics could be used to quantify the impact of such protocols on overall network reliability?

33. Many broadband providers have moved to Multiprotocol Label Switching (MPLS) to facilitate creating “virtual links” between distant nodes as a way to ensure Quality of Service (QoS) for

---

<sup>38</sup> Transmission Control Protocol, for example, makes use of data retransmission, which improves reliability; while other protocols, such as User Datagram Protocol, might not. Various services may use either of these, or other, protocols, each having different characteristics.

<sup>39</sup> See *Understanding High Availability of IP and MPLS Networks*, available at: <http://www.ciscopress.com/articles/article.asp?p=361409&seqNum=4>.

broadband services.<sup>40</sup> Could such virtual links between distant nodes compromise some of the built-in resiliency features of IP, and if so, how? To what extent, if any, might broadband services be less resilient to network equipment failures when MPLS or other similar protocols are used? What effects, if any, could MPLS or similar protocols have on end-to-end availability and other reliability/resiliency metrics?

34. Session Initiation Protocol (SIP) is a signaling protocol increasingly used for controlling multimedia communications including voice and video over IP.<sup>41</sup> Telephony networks employing SIP can implement many of the more advanced call processing features present in Signaling System 7 (SS7), though the two protocols themselves are very different.<sup>42</sup> We seek comment on how to evaluate whether SIP and similar protocols are sufficiently reliable to provide essential or mission-critical communications. To what extent, if any, should the Commission establish reliability objectives for networks employing SIP and what should those objectives cover?

35. MPLS and SIP are just two examples of protocol-related matters with potential implications for the reliability of broadband networks. We encourage commenters to address the reliability and resiliency implications of any other applications and protocols. For example, as 4G technologies mature, voice communications may migrate to VoIP on a 4G platform. We seek comment on whether VoIP operating on 4G networks would be as reliable as voice communications carried on other platforms. Can 4G networks support mission-critical VoIP communications, or will they be able to in the future? If so, when?

36. We further seek comment on the role of policy-based routing in the overall integrity of the Internet routing infrastructure. Policy-based routing is a routing protocol that makes routing decisions contingent on business parameters such as cost. Routing decisions that are constrained in this way may or may not be optimally resilient or reliable. To what extent do communications service providers use policy-based routing in broadband networks? What are the costs and benefits of policy-based routing, from the standpoint of both good business practice and network resiliency? Does the use of policy-based routing have any effect on the resiliency of communications networks? If so, what effects, and do communications service providers understand those effects? Does the use of policy-based routing expose the communications infrastructure to any risks? If so, what are they and can they be mitigated?

37. *Capacity Issues.* Communications networks are typically designed to handle a certain amount of traffic during routine operation, plus some overhead capacity to accommodate higher than normal demand. In the event of a failure of a major node, back-up nodes would ideally be designed to handle all of the additional traffic. In reality, however, redundant equipment may not be able to handle all of the additional traffic generated when the primary node fails.<sup>43</sup> When the primary node fails, there can

---

<sup>40</sup> John Evans & Clarence Filsfils, *Deploying IP and MPLS QOS for Multiservice Networks, Theory and Practice* (Morgan, Kaufmann 2007).

<sup>41</sup> "SIP is an application-layer control protocol that can establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls. SIP can also invite participants to already existing sessions, such as multicast conferences. Media can be added to (and removed from) an existing session. SIP transparently supports name mapping and redirection services, which supports personal mobility - users can maintain a single externally visible identifier regardless of their network location." See SIP: Session Initiation Protocol (Internet Engineering Task Force (IETF), RFC 3261, June 2002), available at: <http://www.ietf.org/rfc/rfc3261.txt>.

<sup>42</sup> *Id.*

<sup>43</sup> See Jim Kennedy, *The Importance of the Network in IT Disaster Recovery Planning*, available at: <http://www.continuitycentral.com/feature0554.htm>. After the failure of a node in a redundant pair, the other node in the pair might be required to handle more than one hundred percent of the usual peak busy hour load, due to development of a backlog during the period during which a processor or system has failed but not yet been taken out (continued....)

be bottlenecks that can seriously degrade or interrupt service. We seek comment on how system capacity issues, or any other similar considerations, differ between public switched telephone network (“PSTN”) infrastructure and IP technology with respect to redundancy, recovery, and other relevant factors. What best practices presently exist, and what additional best practices might be needed to address these concerns? We note, for example, that several industry sponsored best practices already exist that address capacity, with several specifically related to DNS servers.<sup>44</sup> However, none of the best practices appears to provide objective capacity requirements. Would it be beneficial to have requirements relating to the capacity of primary and back-up paths in broadband networks? If so, what equipment in broadband networks should have capacity requirements, and who should set these requirements? What are the advantages and disadvantages and costs and benefits to requiring equipment suppliers to test and provide estimates of the capacity of major equipment?

38. *Cascading Overloads & Graceful System Recovery.* In some circumstances, failure of one component in a network – and ironically, even the process of restarting a failed piece of equipment – can result in cascading overloads that overwhelm the entire system. For example, when a core router fails, a large number of subscribers to a service that depends on that router may find that the service has become extremely slow or completely unavailable. Subsequently, when the failed server is brought back online, cascading overloads can propagate throughout the network.<sup>45</sup> We seek comment on what measures could be taken to ensure graceful system recovery and to avoid or mitigate vulnerability to cascading failures. Should there be equipment safeguards to ensure restoration of service in a controlled manner? Should there be requirements regarding the additional capacity of back-up paths to cover users or equipment trying to reestablish service? We also ask commenters to address the advantages and disadvantages and costs and benefits of requiring suppliers to demonstrate that their products have sufficient overload capacity to handle such scenarios.

39. *Maintenance Procedures.* One would not necessarily expect routine maintenance procedures to be a significant source of system failures and network outages. However, it has been reported that 20 percent of all failures on broadband networks are due to planned maintenance.<sup>46</sup> Maintenance activities can fail for a variety of reasons, ranging from human error to the shipment of faulty cards, to faulty fiber, to configuration errors. We seek comment on the safeguards or standards that are already in place or should be considered, if any, to minimize service disruptions caused by procedural errors during routine maintenance. For example, what maintenance procedures, if any, should be followed when servicing or replacing equipment, troubleshooting software or performing Border Gateway

(Continued from previous page)

of service. Because the processor is still in service, user traffic is sent to it for processing, and because the processor is not working, the traffic is not delivered properly to its requested destination, thus creating a backlog.

<sup>44</sup> See, e.g., NRIC Best Practices, available at: <https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm>. A search for all NRIC Best Practices that include the word “capacity” yielded seventeen such best practices.

<sup>45</sup> “When a router restarts, it will lose routing adjacencies or sessions with its neighbors for a particular protocol or all protocols. Once its neighbors detect the lost adjacency they will recompute new routes and send new route information to their neighbors. This will propagate throughout the network resulting in network-wide routing updates (route flapping) as well as lost packets. Router performance can also degrade due to the scale of route updates or if more than one router simultaneously restarts. During this period the restarting router cannot receive traffic because its neighbors have cleared its previously advertised routes.” See Alcatel, Router High Availability for IP Networks “Graceful Restarts,” at 5, available at: [http://www.telecomreview.ca/eic/site/tprrp-gcrrt.nsf/vwapj/Router\\_HA\\_for\\_IP.pdf/\\$FILE/Router\\_HA\\_for\\_IP.pdf](http://www.telecomreview.ca/eic/site/tprrp-gcrrt.nsf/vwapj/Router_HA_for_IP.pdf/$FILE/Router_HA_for_IP.pdf).

<sup>46</sup> Athina Markopoulou, Gianluca Iannaccone, Supratik Bhattacharyya, Chen-Nee Chuah & Christophe Diot, “Characterization of Failures in an IP Backbone,” INFOCOM 2004 paper, at 1, available at [http://www.ieee-infocom.org/2004/Papers/48\\_1.PDF](http://www.ieee-infocom.org/2004/Papers/48_1.PDF) (“Our results indicate that 20% of all failures can be attributed to scheduled network maintenance activities.”).

Protocol (BGP) updates or card restarts that reset the internal routing tables? What other procedural safeguards, if any, would it be beneficial to follow? To what extent are such safeguards already in place, and what best practices, if any, have been developed in this area?

40. *Single Points of Failure.* The access portions of most networks generally contain single points of failure.<sup>47</sup> For example, in legacy telecommunications networks, only one connection exists between the customer and the central office. As a result, the central office becomes a single point of failure for access to the PSTN. With respect to broadband access networks, we seek comment on whether edge routers (also known as access routers) that sit at the periphery of the network and which handle large volumes of traffic could become single points of failure. To what extent have such vulnerabilities already been addressed through industry standards and/or best practices? For example, what kind of standards or best practices are being, or should be, applied to the number of diverse paths from edge router to gateway routers? What parameters do or should these standards or best practices depend on? For example, do or should they depend on the amount of traffic handled by the edge router or the downtime of the routes from the edge router to the gateway router? To what extent should these standards or best practices depend on the availability of the edge router or the gateway router?

41. *Silent Failures.* Silent failures happen when a malfunction occurs in a manner that makes it difficult to detect. Such failures could occur in instances where the monitoring system itself fails or the monitoring processes fail to identify a failure (e.g., a DSLAM with a failed alarm). Alternatively, a network system could not be monitored at all. We seek comment on how broadband networks could become more resilient to silent failures. To what extent, if any, have standards or best practices been developed to address this vulnerability? To what extent, if any, should standards be required for broadband network operators to monitor equipment and links to detect failures as quickly as possible and to avoid silent failures? Is there equipment in broadband networks that should be monitored on a continual basis? For example, one network provider has found that operating a back-up system with reserve capacity is more effective than keeping the back-up system in standby mode, as a system that is regularly in use tends to be prepared to handle disasters more readily than a system that has been sitting idle and unused for an extended period of time.<sup>48</sup> Is there equipment for which the Commission should encourage such practices? If so, how would encouraging such practices be beneficial and what would be the costs?

42. *Other Matters.* The particular issues discussed in this section are merely illustrative. Thus, we also ask commenters to address any other technical issues not mentioned herein that could have an adverse impact on network reliability and resiliency.

### C. Action by the Commission

43. In connection with all of the matters discussed above, we seek comment on actions the Commission might take to promote improvements in the overall reliability and resiliency of our Nation's communications network infrastructure, including broadband technologies.<sup>49</sup> For example, what role, if any, should the Commission take to encourage the development of standards to address the issues raised herein? If the Commission were to take a more active role to foster adoption of best practices or other

---

<sup>47</sup> For example, on the customer access line, there is generally a single modem; a single copper, coax, or fiber drop; and a single card terminating the customer's signal at the provider's office.

<sup>48</sup> See Comments of Comcast Corporation at 5-6 (filed June 28, 2010) in the *Survivability Notice* proceeding.

<sup>49</sup> While our focus here is on actions that may be taken by the Commission, we also welcome comment on what role other Federal agencies might play and how such efforts might be coordinated with any action taken by the Commission.

standards, what approach, or approaches, should it take? What lessons can be learned from existing initiatives? We also seek comment on potential barriers to implementation such as relative cost-benefit considerations and any other concerns.

44. We seek comment on ways the Commission could motivate and encourage communications service providers to take appropriate measures, on a voluntary basis, to enhance overall reliability and resiliency in the course of day-to-day operations, as well as continuity of operations during major emergencies. In this context, what affirmative roles, if any, could the Commission play in working with states, tribal, and/or local governments on existing initiatives or requirements that they might impose? Are there new initiatives that the Commission should implement? If so, what are they and how would they work? Are there grants or other funding mechanisms that might encourage communications carriers to implement measures to maintain service during major emergencies? If so, what are they? Have such mechanisms proven beneficial and effective in other contexts? If so, which ones, and what is the nature of such programs? If not, should the Commission recommend to Congress or other Federal agencies that such programs be established? If so, how should such programs be structured? What would be the advantages and disadvantages and costs and benefits of such programs?

45. Given today's increasingly interconnected world, one in which communications services, including broadband technologies, play a critical role in all segments of our society and economy, would a regulatory approach to fostering enhanced reliability, resiliency, and continuity of operation be more or less effective than voluntary, self-directed efforts by industry? What are the advantages and disadvantages and costs and benefits of these two approaches? If the Commission were to promulgate regulations, what particular technical or procedural requirements should it adopt? How should such rules be structured? What facilities should be covered? What minimum technical standards should apply? Should such rules be limited to communications assets located in areas prone to disaster or should they extend to communications facilities used to provide communications services to public safety, hospitals, power grids, and other critical infrastructure services? Should any regulations extend to text and video communications, as well as telecommunications relay services, to ensure access by people with hearing or speech disabilities? If the Commission were to adopt specific requirements, are there certain communications service providers (e.g., small carriers) to which exemptions or different requirements should apply? Are there certain factors that, if present, should excuse compliance from such requirements?

46. If the Commission were to adopt technical requirements relating to maintaining continuity of operations during major emergencies, how could it ensure compliance? In the *Katrina Panel* proceeding, the Commission adopted a requirement that service providers submit lists of their communications assets that were in compliance with its backup power rule, those falling under each of three exemptions, and those not in compliance and not subject to an exemption.<sup>50</sup> Virtually all industry stakeholders participating in that proceeding as well as the Paperwork Reduction Act process argued that the reporting scheme was overly burdensome and costly.<sup>51</sup> If the Commission were to adopt backup power or other technical requirements relating to continuity of operation during emergencies, what alternatives to the *Katrina Panel* proceeding's approach, if any, should it adopt? What would be the advantages and disadvantages and costs and benefits of such requirements? Would a self-certification requirement or periodic audits be sufficient? If the Commission did not adopt a reporting requirement, how could it ensure compliance with continuity of operation requirements?

---

<sup>50</sup> See 47 C.F.R. §§ 12.2, *et seq.* (2007) ("Redundancy of Communications Systems").

<sup>51</sup> See *Katrina Panel Order On Reconsideration*, 22 FCC Rcd at 18026.

47. Should the Commission require communications service providers to develop emergency response plans? If so, what information should be contained in such plans? Should the Commission require that service providers file emergency response plans with the Commission? If so, when, and how often? Should these plans be subject to Commission review prior to implementation? If not, should these plans be subject to review by the Commission at some point after implementation? What would be the advantages and disadvantages and costs and benefits of such a requirement?

48. As a general matter, we also seek comment on what consideration, if any, the Commission should give to any continuity of operation requirements that may presently, or in the future, be imposed by states, tribal, territorial, or local governments, and how any actions taken by the Commission should bear upon such requirements. We also seek comment on any initiatives related to continuity of operation in other countries, including successful and unsuccessful examples, and how those experiences might inform our consideration of these matters.

#### **D. Legal Authority**

49. We seek comment on the Commission's legal authority to take action to address these important issues. What provisions of the Communications Act would support Commission action to ensure the reliability and continuity of networks during major emergencies? For example, would the Commission's licensing authority under section 307(a) permit it to address matters related to network reliability, resiliency, or the maintenance of operation during major emergencies by license holders (including licensees providing interconnected VoIP service and broadband service) if the Commission finds that the "public convenience, interest, or necessity will be served thereby"?<sup>52</sup> Similarly, could the Commission adopt regulations through its authority under section 316(a)(1) to modify licenses "if in the judgment of the Commission such action will promote the public interest, convenience, and necessity"?<sup>53</sup> Would Section 303(b), which requires the Commission to "[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class," give the Commission the authority to establish service reliability levels and the means for achieving those levels?<sup>54</sup> With respect to common carriers, would section 201(b), which requires that all "practices" of common carriers be just and reasonable, permit the Commission to adopt regulations specifying minimum reliability, resiliency or continuity of service requirements for a carrier's practices to be considered "just and reasonable"?<sup>55</sup>

50. Similarly, would section 214(d) permit the Commission to require a carrier to incorporate backup power or other emergency preparedness equipment in its networks or to adhere to reliability and resiliency measures as an obligation to "provide itself with adequate facilities for the expeditious and efficient performance of its service as a common carrier"?<sup>56</sup> Would the Commission have authority to impose such requirements on interconnected VoIP providers or broadband Internet access service

---

<sup>52</sup> 47 U.S.C. § 307(a) ("The Commission, if public convenience, interest, or necessity will be served thereby, subject to the limitations of this Act, shall grant to any applicant therefor a station license provided for by this Act.").

<sup>53</sup> 47 U.S.C. § 316(a); *Celtronix Telemetry v. FCC*, 272 F.3d 585 (D.C. Cir. 2001).

<sup>54</sup> 47 U.S.C. § 303(b).

<sup>55</sup> 47 U.S.C. § 201(b) ("All . . . practices . . . for and in connection with [interstate or foreign communication by wire or radio] shall be just and reasonable, and any such . . . practice . . . that is unjust or unreasonable is hereby declared to be unlawful.").

<sup>56</sup> *Id.* § 214 (d).

providers pursuant to its ancillary authority?<sup>57</sup> For example, does maintaining reliable and resilient interconnected VoIP service, particularly during emergencies, further the goal of section 251(a) that all telecommunications carriers interconnect with other carriers, since if a telecommunications carrier's customer is unable to place a call to an interconnected VoIP provider's customer because of an interconnected VoIP provider's failure to provide reliable and resilient service, the carrier's customer effectively would be denied the intended benefits of section 251(a)? Could lack of reliable and resilient broadband service during an emergency prevent a user of common carrier services from communicating with interconnected VoIP subscribers, who also rely on broadband connections?<sup>58</sup> What other statutory provisions could support Commission action in this area, either directly or through the use of ancillary authority?

#### IV. PROPOSED TERMINATION OF RELATED PROCEEDINGS

51. We propose to terminate the above-captioned proceedings PS Docket 10-92 (*Effects on Broadband Communications Networks of Damage or Failure of Network Equipment or Severe Overload*) and EB Docket 06-119 (*Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*). The issues raised in this proceeding are interrelated to and overlap with issues raised in both the *Survivability NOI* and the *Katrina Panel* proceeding. Further, with respect to the *Katrina Panel* proceeding, we note that the Commission's last substantive action took place in 2007. In addition, many of the issues raised by commenters in that proceeding are either pending in another proceeding or have been addressed in the *Katrina Panel Order* or in other proceedings. Consequently, we anticipate no further substantive action in that docketed proceeding and believe that closing that proceeding would serve the public interest. To ensure a comprehensive examination of all issues related to reliability, resiliency, survivability, and continuity of communications networks, we believe that consolidation of all of these issues into this proceeding and termination of the *Survivability Notice* proceeding would serve the public interest. We seek comment on this proposal.<sup>59</sup> Under this proposal, the Commission would consider the record of the two terminated proceedings, to the extent relevant, in this proceeding.

#### V. CONCLUSION

52. We intend for the record generated by this proceeding to provide the opportunity for a thorough discussion of the reliability and continuity of the operational capabilities of our Nation's communications infrastructure.

#### VI. PROCEDURAL MATTERS

##### A. Ex Parte Presentations

53. This matter will be treated as a "permit-but-disclose" proceeding in accordance with the

---

<sup>57</sup> Under *Comcast v. FCC*, rules adopted by the Commission must be within the Commission's subject matter jurisdiction over interstate and foreign wire and radio communications and tied to a statutorily mandated responsibility. *Comcast Corp. v. FCC*, 600 F.3d 642, 661 (D.C. Cir. 2010).

<sup>58</sup> See 47 C.F.R. § 9.3 (defining interconnected VoIP as a service that, among other things, "[r]equires a broadband connection from the user's location").

<sup>59</sup> Our approach here is consistent with the procedures for termination of dormant proceedings recently adopted by the Commission. See *Amendment of Certain of the Commission's Part 1 Rules of Practice and Procedure and Part 0 Rules of Commission Organization*, Report and Order, CG Docket No. 10-44, FCC 11-16, \_\_ FCC Rcd \_\_ (2011).

Commission's *ex parte* rules.<sup>60</sup> Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentations must contain summaries of the substance of the presentations and not merely a listing of the subjects discussed. More than a one- or two-sentence description of the views and arguments presented is generally required.<sup>61</sup> Other rules pertaining to oral and written *ex parte* presentations in permit-but-disclose proceedings are set forth in section 1.1206(b) of the Commission's rules.<sup>62</sup> Parties wishing to file materials with a claim of confidentiality should follow the procedures set forth in section 0.459 of the Commission's rules. Confidential submissions may not be filed via ECFS but rather should be filed with the Secretary's Office following the procedures set forth in 47 C.F.R. § 0.459. Redacted versions of confidential submissions may be filed via ECFS.

## B. Comment Filing Procedures

54. Pursuant to sections 1.415, 1.419, and 1.430 of the Commission's rules,<sup>63</sup> interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using: (1) the Commission's Electronic Comment Filing System (ECFS), (2) the Federal Government's eRulemaking Portal, or (3) by filing paper copies.<sup>64</sup>

- **Electronic Filers:** Comments may be filed electronically using the Internet by accessing the ECFS: <http://fjallfoss.fcc.gov/ecfs2/> or the Federal eRulemaking Portal: <http://www.regulations.gov>.
- **Paper Filers:** Parties who choose to file by paper must file an original and four copies of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.

Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- Effective December 28, 2009, all hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12<sup>th</sup> St., SW, Room TW-A325, Washington, DC 20554. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes must be disposed of before entering the building.
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

<sup>60</sup> See 47 C.F.R. §§ 1.1200 & 1.1206. Although a Notice of Inquiry proceeding is generally exempt from the *ex parte* rules, we find that the public interest is best served by treating this matter of critical importance to the reliability of our Nation's communications networks as a "permit-but-disclose" proceeding. See 47 C.F.R. §§ 1.1200(a), 1.1204(b)(1).

<sup>61</sup> See 47 C.F.R. § 1.1206(b).

<sup>62</sup> See 47 C.F.R. § 1.1206(b).

<sup>63</sup> 47 CFR §§ 1.415, 1.419, 1.430.

<sup>64</sup> See *Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12<sup>th</sup> Street, SW, Washington DC 20554.

**C. Accessible Formats**

55. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to [fcc504@fcc.gov](mailto:fcc504@fcc.gov) or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

**VII. ORDERING CLAUSE**

56. Accordingly, IT IS ORDERED that, pursuant to sections 1, 4(i), 4(j), 4(o), 7(b), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i)-(j) & (o), 157(b) and 403, this Notice of Inquiry IS ADOPTED.

57. IT IS FURTHER ORDERED that comments with respect to the proposed termination of PS Docket 10-92 and EB Docket 06-119 shall be filed within 30 days after publication of this item in the *Federal Register*.

FEDERAL COMMUNICATIONS COMMISSION



Marlene H. Dortch  
Secretary

**STATEMENT OF  
CHAIRMAN JULIUS GENACHOWSKI**

Re: *Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket No. 11-60

The recent devastating earthquake and tsunami in Japan are a stark reminder of how heavily we depend on reliable and resilient communications networks, especially during major emergencies. It is an unfortunate irony that such disasters often provide the best opportunity to learn about the strengths and weaknesses of communications infrastructure.

The terrible events in Japan are an example of a tragedy of scale in a broadband society. The Japanese used broadband to mitigate the impact of these natural disasters, and their efforts offer examples for us.

For example, the Japan Meteorological Agency's earthquake early warning system relied on broadband to automatically issue alerts via cell phones and TV after the first, less harmful earthquake shock wave, providing a short window for people to prepare for the more powerful shock wave that followed.

The broadband-based warning system also caused many energy plants, industrial facilities, and transportation services to shut down automatically, averting problems at these locations. High-speed trains automatically came to a safe stop in response to earthquake alerts transmitted along the rail system.

The United States does not currently have a comparable earthquake warning system. It is something we should consider, especially for our regions that are most prone to earthquakes.

The events in Japan also demonstrate the importance of reliable and resilient Internet-based communications, especially mobile services. Residents of Japan with mobile phones, for example, were able to rely on their battery-powered devices to access web-based disaster message boards, Twitter, and social networking sites to report on their status and check for updates regarding family and friends. People reporting into disaster message boards could choose a pre-set status message or write their own short message, and millions of such messages were recorded in the days after the earthquake and tsunami.

The continued ability to use wireless devices to access the Internet was in large part due to the redundancy of Japan's wireless mesh network, which can automatically reroute signals over alternate paths if one route is destroyed. The reliability of mesh networking is another lesson we can draw from Japan.

I understand that the Government of Japan and Japanese communications providers have put considerable thought and planning into disaster contingency plans, including backup power requirements. We strive to learn more about the specific best practices in Japan, which enabled an impressive communications recovery in light of widespread devastation. In the United States,

we have no federal rules on backup power, and we have to ask whether that situation is acceptable. The inquiry we initiate today is intended to explore this and similar important questions.

The Japanese tragedy showed the role that broadcasting plays in emergencies. Radio in particular played a significant role in Japan, as residents who lost power could turn on the radio in their cars and receive essential information.

The Japanese tragedy also showed the importance of having redundant transmission facilities. Three of seven trans-Pacific undersea cables had sections of their systems badly damaged in the earthquake. These undersea cable systems are expected to be restored in the next two months, but because of both the redundancy and the resiliency of the undersea cable networks, international communications to Japan continued even on the days immediately following the earthquake.

Such redundancy is generally in place for undersea cable systems that directly serve the United States. The Commission keeps a close eye on the resiliency of these important communications networks, and Japan shows us why it is important that we be vigilant.

Events such as those in Japan shine a light on the importance of ensuring reliable and resilient critical communications infrastructure at all levels, at all times, and especially during major disasters.

In the United States, virtually every segment of our society relies heavily on communications networks – both wireless and wireline, both legacy systems and, increasingly, broadband networks. This includes our Nation's first responders and public safety providers; the energy, health care, and financial sectors; and homes and businesses across America.

The rapid migration of our Nation's communications infrastructure from older legacy technologies to Internet Protocol-based broadband technology underscores the need for an assessment of the reliability of our communications networks.

That is why the National Broadband Plan recommended that the Commission commence an inquiry to better understand the reliability and resiliency standards being applied to broadband networks. Users of communications services today – whether large enterprises, small businesses, or individual consumers – expect the same reliable service no matter what platform they use (and may not even be aware of what platform they use).

Today the Commission takes another step to implement the National Broadband Plan by launching a disciplined approach to gathering information about the reliability and resiliency of our Nation's communications infrastructure. Our goal is to determine what actions we should take to ensure that our communications networks remain functioning when there is a natural or manmade disaster.

Communications service providers have a legitimate interest in protecting sensitive commercial and proprietary information. And we understand the real-world economic

constraints that commercial providers face. We will be mindful of that while seeking to understand the robustness of our communications networks and identify actions to improve the operations of our communications systems in an emergency. These matters are also of vital importance as we transition to and implement Next Generation 9-1-1, which is a priority for this Commission.

Finally, this inquiry implements a key energy recommendation of the National Broadband Plan by considering matters related to giving utilities the certainty they need to use commercial networks for smart grid communications.

This Notice of Inquiry takes an important step forward to examine all of these matters. While we of course strive to prevent and minimize the impact of major emergencies, we also know that they are inevitable. This Inquiry is about ensuring that our communications infrastructure is prepared when disaster strikes. Recent events remind us of the powerful importance of this effort.

**STATEMENT OF  
COMMISSIONER MICHAEL J. COPPS**

Re: *Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket No. 11-60, *Effects on Broadband Communications Networks of Damage or Failure of Network Equipment or Severe Overload*, PS Docket No. 10-92, *Independent Panel Viewing the Impact of Hurricane Katrina on Communications Networks*, EB Docket No. 06-119, Notice of Inquiry.

As we launch today's proceeding on the reliability and continuity of America's communications networks, the images of the devastation along the Gulf Coast from Hurricane Katrina come rushing back. I remember very well traveling with then-Chairman Martin to survey the damage first-hand. We saw communities ripped apart by wind and water, lives uprooted and families divided, and communications networks essential to responding and recovering destroyed. Immediately after, we started looking at ways to improve the reliability, redundancy and survivability of our critical communications infrastructure, and I renewed my call for the creation of the Public Safety and Homeland Security Bureau. So, I take great pleasure in seeing today's Notice of Inquiry presented by just such a Bureau.

We—the Commission, industry and public safety—learned a number of lessons from Katrina about the impact that disasters can have on networks. We've made some progress in implementing them, but our work was never close to done. And new challenges confront us. Not only is every emergency event different, but our technology tools are different, too. As communications networks migrate from legacy technologies to IP-based services over broadband, we need to make sure that we understand how this impacts service reliability and resiliency. We need to be as prepared as we can possibly be to ensure that public safety responders, the energy and finance sectors, and ordinary citizens can stay connected during times of emergency. After all, it's not a question of if another disaster will strike, but when.

I commend the Public Safety and Homeland Security Bureau for teeing up so many key questions in this Notice of Inquiry and thank particularly the Chairman for all the hard work he is doing to enhance the safety of our people. Given the importance of this proceeding, I encourage all interested parties to make detailed comments for our consideration. It's going to be a critically-important record for how we go about the job of protecting our critical communications infrastructure.

**STATEMENT OF  
COMMISSIONER ROBERT M. McDOWELL**

Re: Reliability and Continuity of Communications Networks, Including Broadband Technologies,  
*Notice of Inquiry*, PS Docket No. 11-60, FCC 11-55

I support today's inquiry into the reliability, resiliency and continuity of our nation's communications networks and technologies during emergencies. I am especially gratified that we are proposing terminating two open proceedings in favor of the comprehensive approach set forth in today's *NOI*. I thank Chairman Genachowski for creating a more efficient procedure for those interested in participating.

I have a particular interest in learning more about our legal authority in this area, especially as it pertains to more discrete matters such as back up power mandates, an issue the Commission has struggled with over the years. In addition, I will look for information on whether and how public safety entities may use commercial off-the-shelf equipment and technologies. I understand that the public safety community has historically opposed reliance upon commercial products due to concerns over lack of coverage, reliability and security. A consensus may be emerging among them, however, that commercial technologies may provide significant benefits, at least for non-mission critical applications. I hope to learn more about this important issue from both public safety and industry. I have long emphasized the beneficial economies of scale associated with greater use of commercial services and technologies in the public safety sector.

Finally, I want to acknowledge our colleague in the Public Safety and Homeland Security Bureau, Gary Thayer. I understand that Gary postponed his retirement to help launch this proceeding today. Thank you, Gary, for your work in this proceeding, as well as for your twenty-four years of service here at the Commission. I wish you the best and congratulate you!

**STATEMENT OF  
FCC COMMISSIONER MIGNON L. CLYBURN**

**Re:** *Notice of Inquiry in the Matter of Reliability and Continuity of Communications Networks, Including Broadband Technologies (PS Docket No. 11-60; FCC 11-55).*

It is almost impossible these days to turn on the television, listen to the radio, or surf the Internet, without hearing news about the heartbreaking situation in Japan. While we all continue to pray for a speedy recovery for that Nation, it is important to note that the devastation could have been even worse without the country's advanced communications capabilities. Reports indicate that numerous lives were saved through television and cell phone alerts, issued by Japan's emergency warning system, which afforded citizens time to prepare. The Internet also played a key role, allowing many to communicate with families and friends via Twitter, Facebook, and Skype.

This unfortunate event underscores the need for examining the continuity and reliability of communications networks here in the United States. It is imperative that, during large-scale disasters, citizens are able to obtain vital information from public safety officials and communicate with loved ones.

Our Nation's own experiences, in the aftermath of disasters such as Hurricane Katrina, and violent storms like the one which struck my parent's neighborhood in South Carolina this week, highlight the importance of having our networks protected from potential failures. The NOI asks important questions about critical features in preventing the outages such as the need for backup power, and backhaul redundancy.

I am also pleased to see that the NOI engages in a comprehensive inquiry on the continuity and reliability of our broadband networks. Critical sectors such as public safety, energy, and finance, are migrating from older, legacy, technologies to broadband. Consumers of communications services at all levels may not know much about the technological platform used to deliver their communications services. But these consumers expect the same level of quality and reliability regardless of the platform. We must take steps now to see whether these IP based networks have the high carrier grade standards of legacy systems.

In my opinion, the best way to address these issues is to gather input from the widest possible array of stakeholders. Such collaboration allows us to fashion solutions that achieve important policy initiatives without imposing unreasonable burdens on any communications companies. It is possible the industry leadership has developed high quality standards that are necessary to address reliability concerns, for legacy and broadband networks. This proceeding will help shed light on best practices and allow the Commission to take a proper approach to encourage adoption of those standards.

I look forward to reviewing recommendations on ways to ensure continual, reliable service on all communications networks during major emergencies. In addition, I commend the Public Safety and Homeland Security Bureau, for its excellent work and leadership on this important issue.

**STATEMENT OF  
COMMISSIONER MEREDITH ATTWELL BAKER**

**Re:** *Reliability and Continuity of Communications Networks, Including Broadband Technologies (PS Docket No. 11-60); Effects on Broadband Communications Networks for Damage or Failure of Network Equipment of Severe Overload (PS Docket No. 10-92); Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks (EB Docket No. 06-119)*

The American people deserve the highest degree of continuity, reliability, and resiliency in their communications networks. All segments of our society, from national security to consumer welfare, increasingly depend on them. This is particularly true in the event of a disaster, regardless of whether it is natural or man-made. Exploring the capabilities and deficiencies of our networks is critical to determining any improvements needed to them. The inquiry we launch today will help us understand how and if we can use our authority to promote these improvements as our Nation's technologies and systems continue to evolve. I look forward to learning more as we work together to analyze this essential infrastructure.