

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

In the Matter of)
)
Effects on Broadband Communications Networks) PS Docket No. 10-92
Of Damage to or Failure of Network Equipment)
Or Severe Overload)

NOTICE OF INQUIRY

Adopted: April 21, 2010

Released: April 21, 2010

Comment Date: [45 days from date of publication in the Federal Register]

Reply Comment Date: [75 days from date of publication in the Federal Register]

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

I. INTRODUCTION

1. The American Recovery and Reinvestment Act of 2009 (hereinafter “ARRA”) directed the Commission to prepare a National Broadband Plan (“NBP” or “Plan”) and report that plan to Congress.¹ In particular, ARRA required the Commission to explore ways in which broadband infrastructure and services can “advance consumer welfare...public safety and homeland security...and other national purposes.”²

2. In response to a number of Public Notices issued as part of the NBP proceeding, the Commission received a wealth of commentary on the rapidly increasing importance of wireline and wireless broadband communications networks to consumers, businesses, emergency responders, and government agencies.³ A number of these comments⁴ focused on the importance of broadband survivability.⁵ Based on these comments and independent research conducted by Commission staff, the NBP laid out numerous proposals to ensure that our nation’s critical broadband infrastructure can serve the current and future needs of our citizens in a consistent and reliable fashion.⁶

3. Consistent with the recommendations of the NBP, we adopt this Notice of Inquiry to enhance our understanding of the present state of survivability in broadband communications networks and to explore potential measures to reduce network vulnerability to failures in network equipment or severe over-

¹ Pub. L. No. 111-5, § 6001(k), 123 Stat. 515-16 (2009).

² *Id.* § 6001(k)(2)(D), 123 Stat. at 516.

³ *E.g.*, Alliance for Telecomm. Indus. Solutions comments at 3-4; Center for Individual Freedom comments at 1-2; Joint Nat’l Rural Telecomms. Coop. and DigitalBridge Comm’cns Corp. comments at 1.

⁴ *E.g.*, Telcordia comments at 13-14; ChicagoFIRST reply comments at 2.

⁵ “A property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the device or system will continue to work during and after a natural or man-made disturbance” Newton’s Telecom Dictionary, 20th Edition..

⁶ Omnibus Broadband Initiative, Federal Communications Commission, Connecting America: The National Broadband Plan (2010) at § 16.7.

load conditions, such as would occur in natural disasters, pandemics, and other disasters or events that would restrain our ability to communicate. We seek comment broadly on the ability of existing networks to withstand localized or distributed physical damage, including whether there is adequate network redundancy and the extent of survivability of physical enclosures in which network elements are located, and severe overloads.

II. BACKGROUND

4. Reliance on broadband communications networks is increasing across all elements of our society and all sectors of our economy.⁷ For example, IP-based telephony services have penetrated into the consumer and enterprise markets at a breakneck pace, in many cases without the end-users even knowing that a major technology change has occurred. People are no longer tied to a single public-switched telephone network (PSTN), but communicate through a wide range of interconnected networks (*e.g.*, cable networks, fiber networks, local exchange carriers, licensed wireless broadband communications networks and unlicensed wireless internet service providers). As Americans increasingly rely on broadband communications networks for voice, video, data, and other communications services, the reliability and survivability of broadband communications networks becomes an even more critical factor in the safety, security, and well-being of the American people.⁸

5. We realize that the increasing use of broadband communications networks for telecommunications-type services has blurred the distinction between the PSTN and IP-based broadband communications networks. Consequently, we believe it important that we better understand the implications that this migration will have on the communications survivability of our voice and broadband communications networks.

III. DISCUSSION

6. Consumers, businesses, and government agencies increasingly rely on broadband communications networks to supply voice, video, and data service to fixed and mobile sites. For example, comments received in the National Broadband Plan proceeding indicate levels of broadband adoption ranging from 47% for rural residences to 79% for non-rural businesses.⁹ The network infrastructure required to support these diverse needs is extensive and complicated. In some instances long-term collaboration between telecommunications providers and other major enterprises has led to the development of robust networks with purpose-built survivability features. We are concerned, however, that these features may not adequately ensure the survivability of all types of broadband service throughout the country, including in lesser developed or sparsely populated areas.

7. Broadband core networks are generally presumed to be quite survivable. Survivability is generally weaker in segments of communications networks closer to the network edge, however. In light of the ever-growing centrality of broadband communications it is imperative that we understand the resilience and survivability of our national broadband infrastructure. We seek comment, analysis, and information on the present state of broadband network survivability to three broad classes of harm: 1) physical damage (whether due to malevolent acts, accidents, or *force majeure*), 2) inadequate redundancy, and 3) severe network overload. We also seek comment as specifically described below.

A. Legal Authority

8. Enhancing our understanding of the state of survivability in broadband communications networks and exploring potential measures to reduce network vulnerabilities furthers the Commission's core purposes as set forth in section 1 of the Communications Act: (1) the establishment of "a rapid, efficient,

⁷ *Id.* at § 1.

⁸ *Id.*

⁹ Am. Farm Bureau Fed'n comments at 5-6.

Nation-wide and world-wide wire and radio communication service with adequate facilities,” (2) “the national defense,” and (3) “promoting safety of life and property through the use of wire and radio communication.”¹⁰ We seek comment on the strongest sources of authority to act in this regard should we choose to do so, and we ask commenters to address whether different sources of authority would be required with regard to different types of communications providers.

9. For example, we seek comment on whether the Commission has authority under Title II¹¹ and Title III¹² to adopt specific measures to reduce network vulnerabilities should the Commission choose to do so. In addition, we seek comment on whether the Commission could, if necessary, exercise ancillary authority to reduce network vulnerabilities, should the Commission choose to do so.¹³ In particular, we seek comment on the scope of the Commission’s ancillary authority with regard to the matters described in this *Notice* in light of the recent decision of the United States Court of Appeals for the District of Columbia Circuit in *Comcast Corporation v. FCC*.¹⁴

B. Physical Damage

10. We seek comment on the survivability features and risks presented by the physical architecture of current broadband communications networks. What are the major single points of failure in broadband architectures (for example, edge router, gateway router, transport links, cell sites, and VoIP

¹⁰ 47 U.S.C. § 151.

¹¹ For example, section 201(b) requires that all practices of common carriers in connection with interstate or foreign communication by wire or radio be “just and reasonable.” 47 U.S.C. § 201(b). Section 214 authorizes the Commission to require a common carrier “to provide itself with adequate facilities for the expeditious and efficient performance of its service.” *Id.* § 214(d). Section 215 charges the Commission to “examine into transactions entered into by any common carrier which relate to the furnishing of equipment, supplies [or] services” which may affect the carrier’s services, *id.* § 215(a), and section 218 empowers the Commission to inquire “as to technical developments and improvements in wire and radio communications and radio transmission of energy to the end that the benefits of new inventions and developments may be made available to the people of the United States,” *id.* § 218. We note that section 218 casts a relatively wide net, permitting the Commission to obtain such information from a broad range of entities affiliated with carriers subject to the Act.

¹² Under Title III, the Commission has the authority to establish operational obligations for licensees that further the goals and requirements of the Act if the obligations are in the public interest and do not contradict any basic parameters of the agency’s authority. *See, e.g.*, 47 U.S.C. §§ 301 (granting the Commission authority over “radio communications” and “transmission of energy by radio”); 303(b) (authorizing the Commission, subject to what the “public interest, convenience, or necessity requires,” to “[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class”); 303(r) (authorizing the Commission to “prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this Act”); 307(a) (authorizing the issuance of licenses “if public convenience, interest, or necessity will be served thereby”); 309(a) (authorizing the Commission to grant licenses when “the public interest, convenience, and necessity would be served”); 309(j)(3) (in specifying the characteristics of licenses, the Commission must “include safeguards to protect the public interest in the use of the spectrum and shall seek to promote the purposes specified in section 1 of this Act”); 316(a) (authorizing modifications of licenses if “in the judgment of the Commission such action will promote the public interest, convenience, and necessity”). *See also Schurz Communications, Inc. v. FCC*, 982 F.2d 1043, 1048 (7th Cir. 1992) (Communications Act invests Commission with “enormous discretion” in promulgating licensee obligations that the agency determines will serve the public interest). Title III of the Act also empowers the Commission to regulate devices capable of causing “harmful interference to radio communications.” 47 U.S.C. § 302(a).

¹³ The Commission may exercise ancillary authority over a matter when it falls within the agency’s general statutory grant of jurisdiction under Title I and the regulation is reasonably ancillary to the effective performance of the Commission’s statutory responsibilities. *United States v. Southwestern Cable Co.*, 392 U.S. 157, 172–73 (1968); *accord United States v. Midwest Video Corp.*, 406 U.S. 649, 662 (1972). *See also American Library Ass’n. v. F.C.C.*, 406 F.3d 689, 691–92 (D.C. Cir. 2005).

¹⁴ No. 08-1291, 2010 WL 1286658 (D.C. Cir. April 6, 2010).

servers)? What are the impacts of failure these points? What measures do communications providers take to minimize the presence of single points of failure in broadband architectures? Under what conditions might these measures not be followed? What operational awareness do broadband service providers have on these dependencies? For example is the state of transport link diversity generally known and tracked by a broadband service provider? Do service providers account vulnerability of assets to specific threats? Is the incidence of single points of failure greater or lesser for small service providers and/or network operators? What special provisions are made to ensure the survivability of network services to critical response agencies like public safety answering points (PSAPs)? What provisions are made to ensure the survivability of cell sites relied on by first responders? Should traffic to critical response agencies or for critical services be prioritized? What other aspects of physical architecture create vulnerabilities in broadband communications networks? Besides single points of failure, are there dual failures that could impact a large number of users for an extended period of time? What should be the FCC's role in reducing single points of failure in broadband communications networks? What should the FCC's role be in increasing the level of redundancy in broadband communications networks taking into consideration the tradeoffs between potential regulatory burdens and the benefits of increased survivability?

11. In addition to network architecture, we seek comment on the survivability of physical facilities in which network elements are located. At the outset, we note that the Network Reliability and Interoperability Council (NRIC) adopted a set of best practices for communications physical security. What are the most effective and widely deployed NRIC physical security best practices? What policies are typically put in place to ensure adherence to relevant NRIC physical security best practices? How are decisions made about when not to apply NRIC best practices? Is the present level of protection adequate, and, if so, by what measure? If not, what else should be done and how should this be accomplished? In addition, what other structural, mechanical, environmental or electrical standards are utilized in the construction of facilities that house broadband network elements? What should the FCC's role be in encouraging the implementation of security best practices?

12. We also seek comment on the risks posed by network facility co-location. For example, does the co-location of network hardware in "carrier hotels" or "SuperNodes" represent a significant vulnerability of networks to physical attack or natural disaster?¹⁵ How widespread is this practice? What steps have been taken to ensure redundancy and diversity of physical network links to and from these facilities? Are these redundancies adequate at the metro, national, and international scales? Are security standards at these facilities adequate and uniformly enforced? What should the FCC's role be in the utilization of security standards for co-located network hardware? Finally, are the network elements¹⁶ housed in such facilities commonly protected by redundant elements in physically separated locations and will adequate power be available in an emergency? If not, how widespread is the lack of redundancy? What should the FCC's role be in increasing the level of redundancy for co-located network elements?

C. Inadequate or Ineffective Redundancy

13. Redundancy is used in communications networks to improve survivability. Redundancy failures occur when a network is unable to route traffic over an alternate link when the primary or most desirable link is down. In the public-switched telephone network (PSTN), for example, switches, routers, and multiplexers often protect against service interruption due to one or more physical link failures by intelligently re-routing traffic around the failed link although calls that are in progress may be lost. Traditional telecommunications networks use monitoring and alarms to verify redundancy. Occasionally the re-routing fails to occur because the monitoring equipment does not recognize the physical link failure or because the re-routing equipment fails to execute the re-route. In addition, the cause of the initial link failure may also affect the redundant link, resulting in its failure. We are concerned that the level of re-

¹⁵ PRESIDENT'S NAT'L SECURITY TELECOMMS. ADVISORY COMM., (hereinafter "NSTAC") VULNERABILITIES TASK FORCE REPORT [ON] CONCENTRATION OF ASSETS: TELECOM HOTELS 2-3 (2003).

¹⁶ *E.g.*, switches, routers, multiplexers, transponders, power-feed equipment, etc.

dundancy and the effectiveness of that redundancy in routing around failures may be inadequate in broadband communications networks. We are also concerned that the quality of service (QoS) for the rerouted traffic is adequate.

14. We therefore seek comment on the risk of physical link failures along with the resulting risk of redundancy failures in broadband communications networks. For example, to what extent are core and edge network links protected with “dark” backup links? Are there instances where backup circuit paths occupy the same physical link as a primary circuit path? If so, how prevalent is this practice and what information, systems, or procedures might help to eliminate it? How best can the FCC help to prevent or resolve such problems? To what extent is switching and routing capacity in broadband communications networks protected by redundant systems or reserve switching capacity? Does good business practice dictate some minimum level of reserve switching capacity for a given network? If so, how is that capacity derived? Are the protection mechanisms themselves in broadband communications networks reliable? Are there failure mechanisms that will affect both the primary path and the back-up path? Finally, how can the FCC enhance the chances that redundancy works in broadband communications networks without unduly burdening network operators?

D. Severe Overloads

15. Large-scale events such as pandemics or bioterror attacks may cause dramatic changes in broadband usage patterns as traffic that is ordinarily confined within enterprise or academic networks or passed between enterprise-grade access networks suddenly shifts onto residential-access networks. If residential access networks are unprepared or insufficiently resourced for such changes, the resulting network congestion could threaten the orderly functioning of our economy and prevent citizens from accessing critical public safety services such as 911 call centers. What can be learned from recent events that, while not catastrophic, resulted in a surge of telecommuting (e.g., the recent heavy snowstorms in the Mid-Atlantic States)?

16. In order to better understand the risks associated with sudden shifts of network traffic during pandemics and similar events, we seek comment on the ability of broadband access networks (i.e., cable, DSL, fiber-to-the-home, etc.) to maintain effective operation during severe network congestion or overload. For example, is the capacity of residential access networks sufficient to handle sudden surges in use? To what degree? To the extent that network capacity is insufficient or networks are “oversubscribed,” what methods and procedures are in place to handle these overloads and to rapidly apply network resources to where they are needed? What are the limits to these network management techniques? For example, is there a need for ways to prioritize broadband traffic during emergencies? Are some network segments or geographic areas more vulnerable than others? We also seek detailed data on past instances: When outbreaks of influenza have closed schools in a given area, what changes were observed in residential access network traffic, and how did these changes affect the networks? Should the FCC collect data on network usage during such events?

IV. CONCLUSION

17. As our broadband infrastructure continues to grow and mature, we are committed to ensuring that it stands ready to support the myriad uses dreamed up by American innovators and enterprises. This Notice of Inquiry is a critical first step toward understanding survivability of our broadband communications networks to all types of failures and severe traffic overloads. We look forward to collaborating with consumers, businesses, and network operators to improve and secure our broadband infrastructure for the future.

V. PROCEDURAL MATTERS

A. Comment Filing Procedures

18. Pursuant to sections 1.415, 1.419 and 1.430 of the Commission's rules, 47 CFR §§ 1.415, 1.419, 1.430, 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. See *Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998). 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. Section 0.459. Redacted versions of confidential submissions may be filed via ECFS.

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

B. Accessible Formats

19. 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 or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

VI. ORDERING CLAUSES

20. Accordingly, IT IS ORDERED that, pursuant to sections 1, 4(i), 4(j), 4(o) and 7(b) of the Communications Act of 1934, 47 U.S.C. §§ 151, 154(i)-(j) & (o), and 157(b) (2006), this Notice of Inquiry IS ADOPTED.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch,
Secretary

**STATEMENT OF
CHAIRMAN JULIUS GENACHOWSKI**

Re: *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

Today we begin an inquiry on the survivability and reliability of broadband communications networks, implementing a recommendation of the National Broadband Plan to further public safety and homeland security. As Americans are increasingly relying on broadband networks for voice, video, data, and other communications services, the reliability and survivability of broadband communications networks becomes an even more critical factor in the safety, security, and well-being of the American people. And as network attacks and the level of risks and costs increase, it is beyond important that we fully understand the implications of this evolution in communications, and that we take all necessary and appropriate steps to ensure the survivability of our voice and broadband communications networks.

This NOI examines the survivability of broadband infrastructure by seeking comment on the ability of existing broadband communications networks to withstand disasters, including whether there is adequate network redundancy, whether our networks can function in times of service overload, and whether physical network facilities can withstand harm. This is a vitally important step in ensuring, first, that the Commission has all the facts and data it needs with respect to the survivability of our broadband communications networks, and second, that the Commission quickly take all necessary actions to ensure ongoing broadband communications in times of disaster or crisis.

**STATEMENT OF
COMMISSIONER MICHAEL J. COPPS**

Re: In the Matters 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

I commend Chairman Genachowski for launching this examination of broadband network survivability and our Public Safety and Homeland Security Bureau for their hard work in fleshing out this important item. We all learned the hard way that natural disasters and man-made attacks can have devastating effects on our communications infrastructure and how integral communications are to our safety and security in a dangerous world. Network survivability has a lot to do with national survivability when tragedy strikes. The Commission has worked hard in recent years, especially starting with our follow-up to Hurricane Katrina under Chairman Martin, to improve the reliability, redundancy and security of our nation's network infrastructure. Under the new Commission we are moving even closer to an integrated approach to public safety communications. That's exactly what we should be doing because, as my old boss Senator Fritz Hollings often reminded me, the safety of the people is always the first obligation of the public servant.

Today, consistent with recommendations in the National Broadband Plan, we begin a focused look on the impact of physical damage (whether natural or man-made), inadequate redundancy, and severe network overloads on IP-based broadband networks. I look forward to working with the Bureau and with my colleagues on this critical inquiry—based on what I hope to be, and expect to be, a robust record with comprehensive input from industry, security experts and all concerned citizens.

**STATEMENT OF
COMMISSIONER ROBERT M. McDOWELL**

Re: *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

Our work to enhance our understanding of the state of survivability in broadband communications networks and to explore potential measures to reduce vulnerability to failures in network equipment or server overload conditions, such as during a natural disaster, pandemic or terror attack, will be beneficial. The timing is excellent given that hurricane season is a mere six weeks away. I thank industry in advance for your assistance in this important endeavor.

I look forward to engaging with interested parties and to gaining a better understanding about the status of our nation's broadband networks. I also want to explore further what the Commission's role can and should be with fostering further developments.

Thank you to Jamie Barnett and your entire team. This is a critically important area and I appreciate the work you are doing.

**STATEMENT OF
COMMISSIONER MIGNON L. CLYBURN**

Re: *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*

As the National Broadband Plan makes abundantly clear, given the pace at which Americans are increasing their reliance on broadband services, we should expect broadband networks to soon become the primary medium through which we communicate. With that understanding, one of the federal government's highest priorities must be to employ all measures necessary to protect each aspect of our broadband networks from every form of potential failure. I was particularly pleased to see that the Notice of Inquiry seeks comment on the survivability features of the entire architecture of broadband networks in *all* communities, including those that are lesser developed and sparsely populated. I thank the Chairman and the Public Safety and Homeland Security Bureau for initiating this inquiry and look forward to reviewing the recommendations on how we can ensure the reliability of our broadband networks.

**STATEMENT OF
COMMISSIONER MEREDITH ATTWELL BAKER**

Re: *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

This proceeding is a natural outgrowth of the work of the Broadband Team to assess and collect data on threats and potential gaps affecting our broadband infrastructure. As we now turn to consideration of the Plan's recommendations, we should be careful not to fix ourselves every challenge that relates in some form to broadband. Indeed, I am pleased that we have not prejudged any affirmative regulatory role for the Commission in addressing network survivability. It is in the clear commercial interest of all network operators to ensure their operations are reliable and resilient. It is appropriate for the Commission to evaluate the current conditions of networks, their vulnerabilities, and the potential for the Commission to facilitate best practices or otherwise contribute to the resiliency of our broadband networks. I think this proceeding is another area in which we should work in close conjunction with the Communications Security, Reliability, and Interoperability Council (CSRIC).