

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

In the Matter of)
)
Reliability and Continuity of Communications) PS Docket No. 11-60
Networks, Including Broadband Technologies)
)

**COMMENTS OF
USTELECOM – THE BROADBAND ASSOCIATION**

USTelecom — The Broadband Association (USTelecom)¹ submits these comments to confirm its members’ experience of meaningful coordination amongst backhaul and wireless providers during times of disaster.² USTelecom supports the Public Safety and Homeland Security Bureau’s (“Bureau”) ongoing evaluation of ways to improve wireless resiliency, including through this *Public Notice*. To the extent further improvements are necessary, the Commission should focus on improving existing methods of coordination and incorporating the industry’s recent experience into the wealth of available best practices that already meaningfully promote the resiliency of backhaul networks.

Many USTelecom members are in the business of providing backhaul services to wireless service providers (and some USTelecom members are themselves wireless service providers). Their combined experience shows that backhaul providers will provide reliable networks and services to wireless providers who value reliability for their customers. And experience shows that when a backhaul network becomes unavailable, service provider

¹ USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives – all providing advanced communications service to both urban and rural markets.

² *Public Safety and Homeland Security Bureau Seeks Comment on Improving Wireless Network Resiliency to Promote Coordination Through Backhaul Providers*, PS Docket No. 11-60, Public Notice, DA-18-1238 (PSHSB Dec. 10, 2018) (*Public Notice*).

coordination to maintain and restore service is paramount for consumers.

USTelecom members thus disagree with any premise that there is a “lack of coordination on restoration efforts among backhaul providers and wireless carriers”³, As previously stated in the record and described in the *Public Notice*, it is standard practice for backhaul providers to coordinate with one another, wireless providers and other stakeholders during disasters under existing Department of Homeland Security (DHS) programs and platforms.⁴ The work of the DHS National Coordination Center for Communications (NCC), via its Emergency Support Function #2 is particularly important, serving as a hub of continued coordination. As the Bureau notes, the NCC “coordinates daily calls with providers and other relevant stakeholders to facilitate restoration status and updates on ongoing recovery efforts” in addition to “provid[ing] backhaul restoration information to stakeholders upon request.”⁵ The *Public Notice* also correctly notes that the Communications Information Sharing Analysis Center (COMM ISAC), run in coordination with DHS, serves as a “resource for carrier contact and situational awareness information.”

The *Public Notice* further describes the Service Level Agreements between wireless service providers and their backhaul providers that “address other information sharing and escalation processes for restoration.”⁶ Such coordination is a standard component of industry best practices relevant to backhaul network reliability. These and other relevant practices account for coordination, redundancy, and other reliability features already addressed through contractual arrangements. Thus, stakeholder coordination takes place during disasters not only at the NCC, but as a matter of course pursuant to normal business practices.

³ *Id.* at 1.

⁴ *Public Notice* at n.6.

⁵ *Id.*

⁶ *Id.*

Given the success the NCC has had in its role as a convener of affected stakeholders during disasters, the Bureau should be careful not to interject duplicative processes that would waste or divert scarce resources during a disaster. To the extent that the Bureau identifies a specific breakdown occurring in coordination amongst backhaul providers that can improve public safety—for example sharing with state emergency operations centers or localities—it should seek to correct it via the existing platforms for coordination.

With respect to whether backhaul providers should be included within the Wireless Resiliency Framework, there are many intricacies—technical, contractual, and marketplace—that prevent an easy answer to this question. Backhaul providers reflect a broad cross section of the industry and diverse network technologies. The inquiry is further complicated because backhaul service is not in and of itself a finished product to the consumer—it is a vendor relationship and input like many others that contribute to the overall provision of wireless service. And wireless provider customers vary in size, resources and business models. The Commission has recently delegated the task of “developing best practices for coordination among wireless providers, backhaul providers, and power companies during and after a disaster” to the Disaster Response and Recovery Working Group of the Broadband Deployment Advisory Committee (BDAC).⁷ This BDAC Working Group is the appropriate place to vet these best practices and determine whether it makes sense to incorporate backhaul providers into the Wireless Resiliency Framework. The Bureau should defer its inquiry until the BDAC completes its study; it can then seek comment on BDAC’s proposals.

Communications resiliency planning also involves coordinating with other critical infrastructure providers, most notably the electric companies that power the communications networks and share other infrastructure resources. In being mindful of the need to avoid

⁷ *Id.*

duplicative efforts, the Bureau should also be aware that DHS’s recently formed National Risk Management Center⁸ is currently studying systemic risk among critical infrastructure sectors, particularly focusing on the critical functions and dependencies of the communications, energy, and finance sectors in a disaster scenario.⁹ The Commission should ensure that resiliency planning policy is aligned within the federal government.

In summary, USTelecom’s backhaul provider members are committed to effective coordination and planning and have already taken extensive steps to facilitate and participate in these efforts. We stand ready to work with the Bureau and DHS to apply the industry’s recent experience in disaster events to the wealth of best practices that address backhaul reliability.

Respectfully submitted,

By: 

Michael Saperstein
USTelecom Association
601 New Jersey Avenue, N.W.
Suite 600
Washington, D.C. 20001
(202) 326-7300

February 8, 2019

⁸ DHS Cybersecurity and Infrastructure Security Agency, National Risk Management Center, <https://www.dhs.gov/cisa/national-risk-management-center> (last visited Jan. 7, 2019) (“The National Risk Management Center (NRMC) is housed within the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA). The NRMC is a planning, analysis, and collaboration center working to identify and address the most significant risks to our nation’s critical infrastructure. The NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: Identify; Analyze; Prioritize; and Manage the most strategic risks to our National Critical Functions — the functions so vital that an attack or interruption to services within the government and the private sector could have devastating consequences to our national security, economic security, national public health and safety, or any combination thereof.”).

⁹ DHS, National Critical Functions Fact Sheet, <https://www.dhs.gov/publication/national-critical-functions-fact-sheet> (last visited Jan. 7, 2019).