1099 NEW YORK AVENUE NW SUITE 900 WASHINGTON, DC 20001-4412

JENNER&BLOCK LLP

John L. Flynn
Tel +1 202 639 6007
jflynn@jenner.com

December 15, 2015

VIA ECFS

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: *Applications of Charter Communications, Inc., Time Warner Cable Inc., and Advance/Newhouse Partnership for Consent to the Transfer of Control of Cable Television Relay Service Applications*, MB Docket No. 15-149[1]

Dear Ms. Dortch:

On December 11, 2015, representatives of Charter Communications, Inc. ("Charter") met with Federal Communications Commission ("Commission") staff copied at the bottom of this letter to discuss the transaction referenced above. Participating for Charter were Scott Weber, Executive Vice President, Network Operations; Jay Rolls, Senior Vice President, Chief Technology Officer; Charlotte Field, Senior Vice President, Application Platform Operations; Alex Hoehn-Saric, Senior Vice President, Government Affairs; Christianna Barnhart, Vice President, Regulatory Affairs; Mary Haynes, Senior Director, Network Security Operations; and Nancy Libin and the undersigned of Jenner & Block LLP. This letter provides an overview of issues discussed at the meeting and additional information that the Commission requested from Charter.

During the meeting, Charter discussed its current cybersecurity risk management program and internal controls, and its goals with respect to cybersecurity for the combined entity

[1] *See* Applications of Charter Communications, Inc., Time Warner Cable Inc., and Advance/Newhouse Partnership for Consent to the Transfer of Control of Cable Television Relay Service Applications, MB Docket No. 15-149 (June 25, 2015).

("New Charter").[2] Specifically, Charter described steps taken to date to evaluate the cybersecurity postures of Time Warner Cable ("TWC") and Bright House Networks ("BHN"). It also explained how combining investments, resources, and talented personnel of all three companies will improve cybersecurity protections for New Charter's network and its customers, as well as the larger broadband ecosystem.

Charter is proactive about cybersecurity and uses several unique cybersecurity programs, including an organization dedicated solely to the security of its network and services. Charter has spent millions on this organization, which has implemented threat and risk management processes; security and event monitoring capabilities; detailed incident response plans; and other advanced detection, prevention, and protection capabilities, including practices and tools to monitor and mitigate insider threats.[3] Charter has implemented **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION]
Through these efforts, Charter has implemented valuable security tools necessary to protect their customers' communications.

Charter also has a sophisticated distributed denial of service ("DDoS") attack protection program that exceeds the recommendations of the CSRIC IV DDoS Working group. **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION] and Charter plans to **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]** **[END HIGHLY CONFIDENTIAL INFORMATION]** Charter's program **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION] New Charter plans to **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]** **[END HIGHLY CONFIDENTIAL INFORMATION]**

---

[2] *See id.* at 17-42; Applicants' Opposition to Petitions to Deny and Reply to Comments, at 1-32 and Exhibits A and B.

[3] With respect to spending on cybersecurity generally, in 2015, Charter budgeted **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION]

In addition, Charter's botnet notification program **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION] Charter's program provides customers with **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]** **[END HIGHLY CONFIDENTIAL INFORMATION]** as opposed to requiring **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION]

Moreover, Charter has been active in trying to protect customers and the network from the risk posed by OpenDNS resolvers. Earlier this year, Charter's network security department **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION] As a result, **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION]

Charter also has strong risk management and governance frameworks. It has adopted and is in the process of implementing the NIST cybersecurity framework throughout the company and is adopting a number of CSRIC IV recommendations, including those recommendations that align and adapt the NIST framework to the cable industry. In addition, Charter's governance framework ensures that senior management and the board of directors are regularly briefed about cybersecurity issues and can make informed decisions about them. Charter has **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION] The **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]** **[END HIGHLY CONFIDENTIAL INFORMATION]**—which is responsible for reviewing security incidents, threats, and risks—has a direct line to the board of directors, a member of which is an experienced technologist with cybersecurity expertise, and **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION]

During the meeting, Charter explained that it has met with TWC and BHN and has begun to identify the "best-of-the-best" cybersecurity practices at each company that New Charter will implement across the new combined entity. For example, Charter plans to implement **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

---

[4] Board reports and minutes regarding cybersecurity can be found at Bates CHR-DOJ-0001555934; CHR-FCC-0000197855; CHR2-DOJ-00000651021; CHR2-DOJ-00000659560; CHR2-DOJ-00000538208; CHR2-DOJ-00000005253; CHR2-DOJ-00000005307; CHR2-DOJ-00000005344; and CHR2-DOJ-00000657690.

[END HIGHLY CONFIDENTIAL INFORMATION] Similarly, Charter has identified capabilities at TWC that it intends to implement at New Charter. For instance, **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION]

New Charter also intends to take advantage of the investments that both Charter and TWC have made in adopting the NIST cybersecurity framework, which will remain the risk management framework at New Charter. This includes utilizing standards recommended in the NIST cybersecurity framework core, which maps the core functions, and underlying categories and subcategories, to various standards, **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]** **[END HIGHLY CONFIDENTIAL INFORMATION]** and others. In addition, New Charter will establish a corporate governance structure that ensures both its board and its management are actively engaged in oversight and implementation of the company's cybersecurity program.

As mentioned above, New Charter also will leverage the combined resources and personnel of all three entities to enhance the level of cybersecurity programs beyond what the three companies could maintain on their own. Charter expects this process to go smoothly, as the leading cybersecurity personnel at the three companies interact regularly through working groups in which they participate and in which they will continue to participate at New Charter.

Finally, Charter explained how it will maintain security at the three companies during the transition to New Charter. As an initial matter, Charter intends to **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION] During this period, **[BEGIN HIGHLY CONFIDENTIAL INFORMATION]**

[END HIGHLY CONFIDENTIAL INFORMATION]

Please contact me if you have any questions.

Sincerely,

/s/ John L. Flynn

John L. Flynn

cc: Owen Kendler
Elizabeth McIntyre
Michael Saperstein
Jennifer Salhus
Christopher Sova
Elizabeth Cuttner
Vernon Mosley
Soumitra Das
Brenda Villanueva
Lauren Kravetz
David Simpson
Jeffery Goldthorp
Peter Shroyer
Emily Talaga
Jamila Bess Johnson
Jerry Stanshine
Christopher Clark
Joel Rabinovitz
Lisa Hone