

REDACTED – FOR PUBLIC INSPECTION

March 4, 2015

VIA ELECTRONIC FILING

Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Re: *Applications of Comcast Corp., Time Warner Cable Inc., Charter Communications, Inc., and SpinCo for Consent to Assign or Transfer Control of Licenses and Authorizations, MB Docket No. 14-57*
REDACTED – FOR PUBLIC INSPECTION

Dear Ms. Dortch:

Comcast Corporation hereby submits a redacted, public version of the enclosed *ex parte* letter. The [[]] symbols denote where Confidential Information has been redacted, and the {{ }} symbols denote where Highly Confidential Information has been redacted. A Highly Confidential version of the letter has been submitted to the Office of the Secretary pursuant to the Second Amended Modified Joint Protective Order in this proceeding.¹ The Confidential and Highly Confidential versions of this submission will be made available for inspection pursuant to the terms of the Second Amended Modified Joint Protective Order.

Please contact the undersigned should you have any questions regarding this matter.

Respectfully submitted,

/s/ Mia Guizzetti Hayes

Mia Guizzetti Hayes

Counsel for Comcast Corporation

Enclosure

¹ *Applications of Comcast Corp. and Time Warner Cable Inc. for Consent to Assign or Transfer Control of Licenses and Authorizations*, Second Amended Modified Joint Protective Order, 29 FCC Rcd. 13799 (2014) (“Second Amended Modified Joint Protective Order”).



Comcast Corporation
300 New Jersey Avenue, NW
Suite 700
Washington, DC 20001

REDACTED – FOR PUBLIC INSPECTION

March 4, 2015

VIA ELECTRONIC FILING

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: *Applications of Comcast Corp., Time Warner Cable Inc., Charter Communications, Inc., and SpinCo for Consent to Assign or Transfer Control of Licenses and Authorizations, MB Docket No. 14-57*
REDACTED – FOR PUBLIC INSPECTION

Dear Ms. Dortch:

On March 2, 2015, Myrna Soto, Senior Vice President and Chief Information and Infrastructure Security Officer, Lynn Charytan, Rudy Brioché, Julie Laine, and Mary McManus of Comcast Corporation (“Comcast”), Mia Guizzetti Hayes of Willkie Farr & Gallagher LLP, and the undersigned met with the Commission staff copied below regarding the cybersecurity-related benefits of the above transaction. Led by Ms. Soto, we discussed points made in the Applicants’ Public Interest Statement in this proceeding.¹

In particular, we described how the transaction will deliver the benefits of Comcast’s industry-leading cybersecurity and risk management practices to Time Warner Cable Inc. (“TWC”) customers. Over the last five years, Comcast has made substantial investments in network- and consumer-based cyber defense capabilities and cyber threat intelligence-gathering and analysis tools that place it at the forefront of cybersecurity best practices. The transaction will extend the benefits of these investments because TWC has not yet deployed many of the advanced cyber defense capabilities utilized by Comcast. Further, Comcast has developed a broad range of cybersecurity personnel with specialized expertise, thereby providing it with the resources and internal capability to accelerate the extension of these benefits to the TWC network. Moreover,
II

¹ See Applications and Public Interest Statement of Comcast Corporation and Time Warner Cable Inc., MB Docket No. 14-57 (Apr. 8, 2014) (“Public Interest Statement”).

REDACTED – FOR PUBLIC INSPECTION

Marlene H. Dortch
March 4, 2015
Page 2

]] and, in conjunction with the Chief Information and Infrastructure Security Officer, ensures Comcast's focus on cybersecurity excellence.

We explained that the transaction will extend to TWC's network the breadth, depth, and resiliency of Comcast's security operations and specialized cyber expertise.² Comcast's centralized security organization, which operates out of Comcast's Moorestown, NJ 24x7 Security Operations and Security Response Center, [[

]].

We also explained that the benefits of Comcast's enhanced intelligence gathering and deterrence capabilities will extend to the TWC systems through the transaction. Comcast employs network sensors, advanced threat intelligence-gathering capabilities, and internal cybersecurity forensics. Comcast also has a [[

]]. The transaction will allow Comcast to reduce gaps in TWC's current threat intelligence capabilities and to expand the deployment of network sensors throughout the TWC network. Moreover, increased scale and ability to apply shared terminology and common metrics across more potentially affected networks and users will enhance the intelligence gathering, information sharing, and threat dissemination capabilities, and the cyber defense posture, of the combined entity.

We further explained how the TWC network will be enhanced by Comcast's investments in purchasing and developing in-house cyber defense capabilities. At the direction of industry-leading security engineers and software developers, Comcast has designed customized tools and capabilities to enhance the company's ability to detect, respond to, and remediate threats. Among the network-based benefits that will extend to the TWC network are accelerated deployment of DNSSEC and IPv6, along with implementation of [[

]]. We emphasized that Comcast, a leader in the design and implementation of IPv6 security controls, developed significant expertise managing the transition of its own network from IPv4 to IPv6 and will use that expertise to ensure the secure and controlled transition of the TWC network.³

² See Public Interest Statement at 124-26.

³ See *id.*

Marlene H. Dortch
March 4, 2015
Page 3

Comcast customers currently have access to a sophisticated suite of security capabilities and features, including password management, anti-logging and anti-phishing protections, and secure browser and robust bot detection capabilities, and we discussed how the transaction will extend those benefits to TWC customers, who do not currently have access to some of these capabilities or features.⁴ As a result of the transaction, TWC customers will also have access to assistance from Comcast’s specialized customer security assurance group, [[

]].

We described long-term network security risk management plans for the merged entity, including the full integration and assumption of Comcast’s layered cybersecurity model, and the extension of Comcast’s holistic approach to cybersecurity to TWC’s network operations and security practices and personnel. Key milestones will include {{

}}.

In response to questions about how Comcast has identified risks to the TWC network assets and how Comcast will eventually protect those assets, we noted that Comcast [[

]]. Immediately following the closing of the transaction, Comcast {{

}}. Following the closing, Comcast will also extend its standard suite of core security toolsets to the TWC network and will capitalize on already-made strategic investments in its security event and incident monitoring infrastructure to provide expedited analysis of event and incident alert data. Because successful integration necessarily includes adopting “best-of-the-best” practices, we explained that Comcast anticipates {{

}}.

Comcast understands that maintaining the security of the merged entity’s network during the transition period is of critical importance. To that end, we explained that {{

⁴ See *id.* at 125.

REDACTED – FOR PUBLIC INSPECTION

Marlene H. Dortch
March 4, 2015
Page 4

}}.

Finally, we noted that, from a cybersecurity perspective, Comcast expects to achieve
{{
}}.

Please direct any questions to the undersigned.

Respectfully submitted,

/s/ Kathryn A. Zachem

Senior Vice President,
Regulatory and State Legislative Affairs
Comcast Corporation

cc: John Adesalu
Hillary Burchuk
Elizabeth Cuttner
Bill Dever
Lisa Fowlkes
Keith Ingram
Clete Johnson
Lauren Kravetz
Bill Lake

Adam Lazaros
Daniel Meyerson (via telephone)
Vernon Mosley
Linda Pintro (via telephone)
Will Reed
Joel Rabinovitz
Eric Schmidt
Admiral David Simpson
Brenda Villanueva