FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

July 21, 2017

The Honorable Mike Doyle
Ranking Member
Subcommittee on Communications and Technology
Committee on Energy and Commerce
U.S. House of Representatives
239 Cannon House Office Building
Washington, D.C. 20515

Dear Congressman Doyle:

Thank you for your June 26, 2017 letter and questions concerning the Federal Communications Commission's (FCC's or Commission's) cybersecurity preparedness and its impact on the FCC's ability to accept comments from the public in ongoing proceedings.

I consider any disruption of the FCC's systems by outside parties to be a very serious matter. That's why our Information Technology (IT) staff immediately addressed the disruption to the FCC's Electronic Comment Filing System (ECFS) that began late in the evening on May 7 and mitigated the impact on filers by the morning of the following day, May 8. And following the events of May 7-8, I directed our Chief Information Officer (CIO) to take appropriate measures to continue securing the comment filing system and to report back to my staff routinely on this work. I also directed the CIO to fully assist in any official inquiries related this matter and to comply with all applicable federal guidelines and laws governing such incidents.

This work was successful and from Monday, May 8 to Friday, May 12, we received more than 2.1 million comments. To put this number in perspective, the FCC usually averages 10,000 comments per day in total for all our proceedings combined.

Moreover, during the past two months, the Commission's IT staff has taken additional steps to prevent potential disruptions similar to the May 7-8 event as well as to ensure the ongoing integrity and resiliency of the system. And ECFS has performed well during the comment period following the adoption of the *Restoring Internet Freedom Notice of Proposed Rulemaking*. The docket now contains more than 10 million comments overall, demonstrating that our processes are facilitating widespread public participation in this proceeding. Indeed, the system did not experience any difficulties in the leadup to the deadline for initial comments, which was earlier this week.

Although I cannot guarantee that we will not experience further attempts to disrupt our systems, our staff is constantly monitoring and reviewing the situation so that that everyone seeking to comment on our proceedings will be afforded the opportunity to do so. We are committed to this goal and will continue to foster a transparent process that encourages public participation in our proceedings.

The CIO has provided me with the attached answers to the list of questions in your letter. Please let me know if I can be of any further assistance.

Sincerely,

Ajit V. Pai

Ajit Pai

Enclosure

Responses to Inquiry from the House Energy & Commerce and Government Reform Committees

1. **According to the FCC's response to Senators Wyden and Schatz, the May 2017 incident was a "non-traditional DDoS attack" where bot traffic "increased exponentially" between 11pm EST on May 7, 2017 until 1pm EST on May 8, 2017, representing a "3,000% increase in normal volume." What "additional solutions" is the FCC pursuing to "further protect the system," as mentioned in the FCC's response?**

   First, for your records, please note the following correction to your question above concerning the timing of this event. As we stated in our earlier response to Senators Wyden and Schatz, bot traffic increased exponentially from 11:00 p.m. to 1:00 a.m., EST – not 1:00 p.m. We provided this timeline to assist in understanding the nature of the attack.

   Given the ongoing nature of the threats to disrupt the Commission's electronic comment filing system, it would undermine our system's security to provide a specific roadmap of the additional solutions to which we have referred. However, we can state that the FCC's IT staff has worked with commercial cloud providers to implement internet-based solutions to limit the amount of disruptive bot-related activity if another bot-driven event occurs.

   The FCC also instituted a more predictive model for assessing the number of incoming comments and bot driven activity to ensure we will have more cloud-based resources available within a shorter time period to respond to potential surges in activity. In addition, the FCC implemented a control feature that recognizes when there is heavy bot traffic. This improvement allows humans (as opposed to bots) to continue to access the electronic comment filing system even if a large amount of bot activity is also present.

2. **According to the FCC, the alleged cyberattacks blocked "new human visitors . . . from visiting the comment filing system." Yet, the FCC, consulting with the FBI, determined that "the attack did not rise to the level of a major incident that would trigger further FBI involvement." What analysis did the FCC and the FBI conduct to determine that this was not a "major incident?"**

   The FCC consulted with the FBI following this incident, and it was agreed this was not a "significant cyber incident" consistent with the definition contained in Presidential Policy Directive-41 (PPD-41). Equally, it is important to note the May 7-8 disruption was not a system "hack" or intrusion and at no point was the Commission's network cybersecurity breached.

3. **What specific "hardware resources" will the FCC commit to accommodate people attempting to file comments during high-profile proceedings? Does the FCC have sufficient resources for that purpose?**

   The Commission's Electronic Comment Filing System is commercially cloud-based, so our "hardware resources" are provided by our commercial partners. While it would undermine our system security to provide a specific roadmap of what we are doing, we can state that FCC IT staff has notified its cloud providers of the need to have sufficient "hardware resources" available to accommodate high-profile proceedings. In addition, FCC IT staff has worked with commercial cloud providers to implement internet-based solutions to limit the amount of disruptive bot-related activity if another bot-driven event occurs.

4. **Is the FCC making alternative ways available for members of the public to file comments in the net neutrality proceeding?**

   Yes, filers always have four alternatives for submitting comments: sending a written document, filing through the normal web interface, filing through the API, or submitting through the electronic inbox using the Bulk Upload Template.

5. **Did the FCC contact the National Cybersecurity and Communication Integration Center's Hunt and Incident Response Team (HIRT) at the U.S. Department of Homeland Security to investigate the May 8th, 2017 incident, and if so, which date(s) was such contact made? If the FCC did not contact HIRT to investigate the May 8th, 2017 incident, please explain why it did not do so.**

   The FCC did not contact HIRT because this event was not categorized as a "significant cyber incident" under PPD-41.

6. **What were the findings from any forensic investigative analyses or reports concerning the May 8th, 2017 incident, including how and why a denial-of-service attacks were declared, and from what attack vectors they came?**

   Our response to Senators Wyden and Schatz describes why we have categorized this incident as a non-traditional DDoS attack. Otherwise, the investigation is ongoing at this stage.

7. **Did the FCC notify Congress of the May 8th, 2017 incidents as provided by FISMA? And if so, how did the FCC notify Congress? If not, why not?**

   Although I have been advised that the FCC's Office of Legislative Affairs provided background information on this matter to the committee offices, we did not provide a FISMA-based notification. We determined that this event was not a "major incident" under the Office of Management and Budget's (OMB) definition and hence it did not meet the criteria of a reportable incident to Congress under OMB's FISMA guidance.

   Our rationale was based on the OMB guidance on FISMA contained in M-17-05, which provides instructions to agencies on when and how to report a "major incident" to Congress. Under OMB's FISMA guidance, a "major incident" is automatically a "significant cyber incident" per PPD-41, and the definitions of the two terms are closely related. As discussed in the response to question number 2, this event was not categorized as a "significant cyber incident" per PPD-41.

8. **Did the FCC notify its Office of the Inspector General (OIG) of the May 8th, 2017 incidents, and if so, when did it notify the OIG?**

   The Office of the Inspector General contacted FCC's management on May 10, 2017, and we have provided information to them about the incident.