June 15, 2017

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Wyden:

This letter responds to your May 9, 2017, correspondence and questions concerning the Federal Communications Commission's (FCC) response to the May 7-8, 2017, cyber-based attack against its Electronic Comment Filing System (ECFS). I agree that this disruption to ECFS by outside parties was a very serious matter. As a result, my office immediately directed our Chief Information Officer (CIO) to take appropriate measures to secure the integrity of ECFS and to keep us apprised of the situation.

The Commission's CIO has informed me that the FCC's response to the events sufficiently addressed the disruption, and that ECFS is continuing to collect all filed comments. Indeed, as of this date, we have received more than 4.98 million comments in this proceeding— the most the FCC has ever received for any proceeding through ECFS.

Please be assured that I have directed the Commission's Information Technology (IT) staff to continue to closely monitor ECFS and expeditiously address and report any potential issues to my office. IT staff provide regular reports of the current state of our network operations (including any incipient threats), as well as incoming comment numbers and work to provide an uninterrupted, transparent, and quality experience for all stakeholders.

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

Sincerely,

Ajit V. Pai

Enclosure

ATTACHMENT

1. Please provide details as to the nature of the DDoS attacks, including when the attacks began, when they ended, the amount of malicious traffic your network received, and an estimate of the number of devices that were sending malicious traffic to the FCC. To the extent that the FCC already has evidence suggesting which actor(s) may have been responsible for the attacks, please provide that in your response.

We have determined that this disruption is best classified as a non-traditional DDoS attack. Specifically, the disrupters targeted the comment filing system application programming interface (API), which is distinct from the website, and is normally used by automated programs or bots for bulk filings.

Our decision to classify the nature of the attack as a non-traditional DDoS is based on specific data as well as a pattern of disruptions that show abnormal behavior outside the scope of a lobbying surge. As discussed below, we detected an extremely high level of atypical cloud-based traffic accessing the API interface, but very few of these connections actually left comments. These automated programs or bots operated in a way that precluded human user access to the system.

The peak activity triggering the comment system's unavailability to most human filers appears to have started at approximately 11:00 p.m. Eastern Standard Time (EST) on Sunday, May 7, 2017. Bot traffic to the system's API increased exponentially from 11:00 p.m. EST to May 8, 2017, at 1:00 a.m. EST. In fact, the number of hits on the comment filing system's API increased from three to five requests per second to over 160 requests per second, representing a 3,000% increase in normal volume. Moreover, we would note that when John Oliver provided a link to encourage viewers to file comments on the evening of Sunday, May 7, 2017, that link directed traffic to the regular comment filing system and not to the API.

From our analysis of the logs, we believe these automated bot programs appeared to be cloud-based and not associated with IP addresses usually linked to individual human filers. We found that the bots initiated API requests with the system and then via their high-speed, resource-intensive requests, effectively blocked or denied additional web traffic—human or otherwise—to the comment filing system. Since both humans and bots were attempting to access the same system and because bots could make more intensive resource requests much faster than humans, the "bot surge" triggered the comment filing system to queue and ultimately decline new connections. The result was that new human users were blocked from visiting the comment filing system.

By 1:00 a.m. EST on Monday, May 8, 2017, the system effectively reduced the number of new requests it would accept in response to the bot swarm. We believe that these bot swarms continued, peaking at 30,000 requests per minute, or three times the total daily traffic for any day in the previous sixty days. This volume also represented the maximum volume that the commercial, cloud-based API servers could handle.

Unfortunately, it would have been exceedingly difficult by 1:00 a.m. EST for new filers to make a new connection until after we initiated our mitigation efforts at 6:00 a.m. EST and sufficiently increased capacity by the start of business hours at 8:45 a.m. EST. By 8:45 a.m. EST, the Commission had increased the filing system's API capacity to over 400 hits per second.

It is important to note that the Commission did not have the technical option of blocking or removing the bots hitting the API. By increasing API capacity, the Commission permitted the system to respond to new human users who had been denied access since the bots were able to use their speed to make more intensive resource requests than humans.

In addition to the basic findings above, our IT staff found other markers of potential malicious intent. For instance, the bots included API calls that were structured—that is, API calls designed not to submit comments, but merely to create an artificial demand for additional resources on the cloud-based system. This appears to have been designed to impede the performance of the comment filing system's components. Later analysis showed the perpetrators requested multiple keys associated with individual IP addresses. This action bypassed the normal protection that prevents such a surge from denying access to human users.

We are unable to determine the total amount of malicious traffic experienced, but we continue to research the number of devices involved in and the origin of the bot swarms. Since the bot traffic emanated from cloud providers, determining the actual source is more difficult than finding that of individual submittals tied to an IP address used by humans.

Importantly, the system remained secure and nothing was hacked. In addition, the FCC successfully received more than two million comments in 10 days, versus more than two million comments over 110 days in the related 2014-15 proceeding. This number includes a one-day record of more than 400,000 comments on Thursday, May 11, 2017. We continue to research additional solutions to strengthen ECFS' controls to further protect the system.

2. Has the FCC sought assistance from other federal agencies in investigating and responding to these attacks? Which agencies have you sought assistance from? Have you received all of the help you have requested?

Following this attack, the FCC CIO directed the Chief Information Security Officer (CISO) to consult with the FBI. In speaking with the FBI, the conclusion was reached that, given the facts currently known, the attack did not appear to rise to the level of a major incident that would trigger further FBI involvement. The FCC and FBI agreed to have further discussions if additional events or the discovery of additional evidence warrant consultation.

3. Several federal agencies utilize commercial services to protect their websites from DDoS attacks. Does the FCC use a commercial DDoS protection service? If not, why not? To the extent that the FCC utilizes commercial DDoS protection products, did these work as expected? If not, why not?

Yes, the FCC has several commercially provided services and tools to protect its systems from DDoS attacks as well as all forms of cyber-attacks. The non-traditional DDoS that we

experienced is quite different than typical attacks in that it used legitimate commercial providers to introduce bots and poorly structured queries to overload the system.

Because the FCC is required to accept comments in virtually any form and from any source, our commercial providers are severely limited in the actions they may take to shut down what are perceived as inappropriate or malicious bots accessing system resources. However, the FCC did implement a rate limit on its API to prevent any one bot from draining excessive system resources. But this rate is tied to a key, and if bots requested multiple keys, they could bypass the limit. We believe there were instances where a single IP address requested multiple keys, thus bypassing the rate limit.

The FCC IT team is considering more advanced solutions to preclude this situation in the future. To be sure, the products and providers that we used performed as expected. But this type of problem is ongoing in nature and requires focused resources to keep up with malicious players seeking to disrupt our work. The FCC will continue to use its available resources to respond to these attempts to disrupt our systems.

4. How many concurrent visitors is the FCC's website designed to be able to handle?

The exact number is unknown, as cloud-based systems are not built with a set number of "visitors"—either human or automated programs (bots). Also, what the visitors are doing while they visit a website, such as the size of visitor inputs to and output requests from the system, influences the potential drain on system resources.

The FCC moved ECFS to a cloud infrastructure to allow for scaling in the event of a large number of inputs and requests. This scaling still requires human involvement in load-balancing and related activities. The FCC successfully received a record of more than 400,000 comments in one day on Thursday, May 11, 2017—showing the system can scale to accommodate a large number of visitors when other external factors are not present. An average day sees closer to 10,000 comments a day, which is why ECFS is cloud-based—to address sudden surges.

    A. Has the FCC performed stress testing of its own website to ensure that it can cope as intended?

The FCC stress tests to the extent possible, but cannot anticipate all scenarios. The system has operated as intended when malicious acts are not being committed to disrupt its operations.

    B. Has the FCC identified which elements of its website are performance bottlenecks that limit the number of maximum concurrent visitors?

Access to the website was not the issue, so the number count on the front of the website was not relevant. In this case, the problem arose through the misuse of an API that is available on the FCC's website.

    C. Has the FCC sought to mitigate these bottlenecks? If not, why not?

Yes. The FCC has committed resources to mitigate the issue that occurred. The FCC will commit more hardware resources to handle requests that threaten the ability of the system to be responsive. The FCC also will continue to investigate newer and better technologies to identify and prevent resources from being occupied at the expense of legitimate filers.

5. Did the DDoS attacks prevent the public from being able to submit comments through the FCC website? If so, do you have an estimate of how many individuals were unable to access the FCC website or submit comments during the attacks? Were any comments lost or otherwise affected?

During the bot swarms, which peaked in the early hours of May 8, 2017, the FCC addressed the problem to bring the system back to an acceptable level of performance within hours of the disruption. While we cannot count the number of "individuals" who might have been delayed in their attempt to file comments during that time frame, we believe that the impact was mitigated by addressing the bot swarms promptly on May 8, 2017. Potential commenters would have been able to file later in the day or in the days that followed. Importantly, the comment cycle is still open, which means comments can still be filed. At this stage, we have received 4.98 million comments, so the comment filing system is clearly facilitating widespread participation in this proceeding.

6. Will commenters who successfully submitted a comment—but did not receive a response, as your press release indicates—receive a response once your staff have addressed the DDoS and related technical issues?

When a commenter files comments through the standard ECFS system, the commenter receives an immediate confirmation number on the screen. Commenters who did not record their number or are unsure if their comments have been received may initiate a name search to confirm that their comments have been filed. If the commenter's name does not appear in the system, the commenter should refile and record the confirmation number.

7. Does the FCC have all of the resources and expertise it needs in order to combat attacks like those that occurred on May 8?

Although the FCC has demonstrated the resiliency of its systems, we must be consistently vigilant in safeguarding IT assets to ensure system availability for all constituents. The FCC is dependent upon its IT team to deal with any issues that may occur going forward and they are continuing to explore potential improvements to the system. If the Commission needs additional resources to address system and cybersecurity issues, we will work with OMB and the Appropriations Committees to ensure that we have the funds to undertake essential upgrades.

June 15, 2017

The Honorable Brian Schatz
United States Senate
722 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Schatz:

This letter responds to your May 9, 2017, correspondence and questions concerning the Federal Communications Commission's (FCC) response to the May 7-8, 2017, cyber-based attack against its Electronic Comment Filing System (ECFS). I agree that this disruption to ECFS by outside parties was a very serious matter. As a result, my office immediately directed our Chief Information Officer (CIO) to take appropriate measures to secure the integrity of ECFS and to keep us apprised of the situation.

The Commission's CIO has informed me that the FCC's response to the events sufficiently addressed the disruption, and that ECFS is continuing to collect all filed comments. Indeed, as of this date, we have received more than 4.98 million comments in this proceeding— the most the FCC has ever received for any proceeding through ECFS.

Please be assured that I have directed the Commission's Information Technology (IT) staff to continue to closely monitor ECFS and expeditiously address and report any potential issues to my office. IT staff provide regular reports of the current state of our network operations (including any incipient threats), as well as incoming comment numbers and work to provide an uninterrupted, transparent, and quality experience for all stakeholders.

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

Sincerely,

Ajit V. Pai

Enclosure

ATTACHMENT

1. Please provide details as to the nature of the DDoS attacks, including when the attacks began, when they ended, the amount of malicious traffic your network received, and an estimate of the number of devices that were sending malicious traffic to the FCC. To the extent that the FCC already has evidence suggesting which actor(s) may have been responsible for the attacks, please provide that in your response.

We have determined that this disruption is best classified as a non-traditional DDoS attack. Specifically, the disrupters targeted the comment filing system application programming interface (API), which is distinct from the website, and is normally used by automated programs or bots for bulk filings.

Our decision to classify the nature of the attack as a non-traditional DDoS is based on specific data as well as a pattern of disruptions that show abnormal behavior outside the scope of a lobbying surge. As discussed below, we detected an extremely high level of atypical cloud-based traffic accessing the API interface, but very few of these connections actually left comments. These automated programs or bots operated in a way that precluded human user access to the system.

The peak activity triggering the comment system's unavailability to most human filers appears to have started at approximately 11:00 p.m. Eastern Standard Time (EST) on Sunday, May 7, 2017. Bot traffic to the system's API increased exponentially from 11:00 p.m. EST to May 8, 2017, at 1:00 a.m. EST. In fact, the number of hits on the comment filing system's API increased from three to five requests per second to over 160 requests per second, representing a 3,000% increase in normal volume. Moreover, we would note that when John Oliver provided a link to encourage viewers to file comments on the evening of Sunday, May 7, 2017, that link directed traffic to the regular comment filing system and not to the API.

From our analysis of the logs, we believe these automated bot programs appeared to be cloud-based and not associated with IP addresses usually linked to individual human filers. We found that the bots initiated API requests with the system and then via their high-speed, resource-intensive requests, effectively blocked or denied additional web traffic—human or otherwise—to the comment filing system. Since both humans and bots were attempting to access the same system and because bots could make more intensive resource requests much faster than humans, the "bot surge" triggered the comment filing system to queue and ultimately decline new connections. The result was that new human users were blocked from visiting the comment filing system.

By 1:00 a.m. EST on Monday, May 8, 2017, the system effectively reduced the number of new requests it would accept in response to the bot swarm. We believe that these bot swarms continued, peaking at 30,000 requests per minute, or three times the total daily traffic for any day in the previous sixty days. This volume also represented the maximum volume that the commercial, cloud-based API servers could handle.

Unfortunately, it would have been exceedingly difficult by 1:00 a.m. EST for new filers to make a new connection until after we initiated our mitigation efforts at 6:00 a.m. EST and sufficiently increased capacity by the start of business hours at 8:45 a.m. EST. By 8:45 a.m. EST, the Commission had increased the filing system's API capacity to over 400 hits per second.

It is important to note that the Commission did not have the technical option of blocking or removing the bots hitting the API. By increasing API capacity, the Commission permitted the system to respond to new human users who had been denied access since the bots were able to use their speed to make more intensive resource requests than humans.

In addition to the basic findings above, our IT staff found other markers of potential malicious intent. For instance, the bots included API calls that were structured—that is, API calls designed not to submit comments, but merely to create an artificial demand for additional resources on the cloud-based system. This appears to have been designed to impede the performance of the comment filing system's components. Later analysis showed the perpetrators requested multiple keys associated with individual IP addresses. This action bypassed the normal protection that prevents such a surge from denying access to human users.

We are unable to determine the total amount of malicious traffic experienced, but we continue to research the number of devices involved in and the origin of the bot swarms. Since the bot traffic emanated from cloud providers, determining the actual source is more difficult than finding that of individual submittals tied to an IP address used by humans.

Importantly, the system remained secure and nothing was hacked. In addition, the FCC successfully received more than two million comments in 10 days, versus more than two million comments over 110 days in the related 2014-15 proceeding. This number includes a one-day record of more than 400,000 comments on Thursday, May 11, 2017. We continue to research additional solutions to strengthen ECFS' controls to further protect the system.

2. Has the FCC sought assistance from other federal agencies in investigating and responding to these attacks? Which agencies have you sought assistance from? Have you received all of the help you have requested?

Following this attack, the FCC CIO directed the Chief Information Security Officer (CISO) to consult with the FBI. In speaking with the FBI, the conclusion was reached that, given the facts currently known, the attack did not appear to rise to the level of a major incident that would trigger further FBI involvement. The FCC and FBI agreed to have further discussions if additional events or the discovery of additional evidence warrant consultation.

3. Several federal agencies utilize commercial services to protect their websites from DDoS attacks. Does the FCC use a commercial DDoS protection service? If not, why not? To the extent that the FCC utilizes commercial DDoS protection products, did these work as expected? If not, why not?

Yes, the FCC has several commercially provided services and tools to protect its systems from DDoS attacks as well as all forms of cyber-attacks. The non-traditional DDoS that we

experienced is quite different than typical attacks in that it used legitimate commercial providers to introduce bots and poorly structured queries to overload the system.

Because the FCC is required to accept comments in virtually any form and from any source, our commercial providers are severely limited in the actions they may take to shut down what are perceived as inappropriate or malicious bots accessing system resources. However, the FCC did implement a rate limit on its API to prevent any one bot from draining excessive system resources. But this rate is tied to a key, and if bots requested multiple keys, they could bypass the limit. We believe there were instances where a single IP address requested multiple keys, thus bypassing the rate limit.

The FCC IT team is considering more advanced solutions to preclude this situation in the future. To be sure, the products and providers that we used performed as expected. But this type of problem is ongoing in nature and requires focused resources to keep up with malicious players seeking to disrupt our work. The FCC will continue to use its available resources to respond to these attempts to disrupt our systems.

4. How many concurrent visitors is the FCC's website designed to be able to handle?

The exact number is unknown, as cloud-based systems are not built with a set number of "visitors"—either human or automated programs (bots). Also, what the visitors are doing while they visit a website, such as the size of visitor inputs to and output requests from the system, influences the potential drain on system resources.

The FCC moved ECFS to a cloud infrastructure to allow for scaling in the event of a large number of inputs and requests. This scaling still requires human involvement in load-balancing and related activities. The FCC successfully received a record of more than 400,000 comments in one day on Thursday, May 11, 2017—showing the system can scale to accommodate a large number of visitors when other external factors are not present. An average day sees closer to 10,000 comments a day, which is why ECFS is cloud-based—to address sudden surges.

   A. Has the FCC performed stress testing of its own website to ensure that it can cope as intended?

The FCC stress tests to the extent possible, but cannot anticipate all scenarios. The system has operated as intended when malicious acts are not being committed to disrupt its operations.

   B. Has the FCC identified which elements of its website are performance bottlenecks that limit the number of maximum concurrent visitors?

Access to the website was not the issue, so the number count on the front of the website was not relevant. In this case, the problem arose through the misuse of an API that is available on the FCC's website.

   C. Has the FCC sought to mitigate these bottlenecks? If not, why not?

Yes. The FCC has committed resources to mitigate the issue that occurred. The FCC will commit more hardware resources to handle requests that threaten the ability of the system to be responsive. The FCC also will continue to investigate newer and better technologies to identify and prevent resources from being occupied at the expense of legitimate filers.

5. Did the DDoS attacks prevent the public from being able to submit comments through the FCC website? If so, do you have an estimate of how many individuals were unable to access the FCC website or submit comments during the attacks? Were any comments lost or otherwise affected?

During the bot swarms, which peaked in the early hours of May 8, 2017, the FCC addressed the problem to bring the system back to an acceptable level of performance within hours of the disruption. While we cannot count the number of "individuals" who might have been delayed in their attempt to file comments during that time frame, we believe that the impact was mitigated by addressing the bot swarms promptly on May 8, 2017. Potential commenters would have been able to file later in the day or in the days that followed. Importantly, the comment cycle is still open, which means comments can still be filed. At this stage, we have received 4.98 million comments, so the comment filing system is clearly facilitating widespread participation in this proceeding.

6. Will commenters who successfully submitted a comment—but did not receive a response, as your press release indicates—receive a response once your staff have addressed the DDoS and related technical issues?

When a commenter files comments through the standard ECFS system, the commenter receives an immediate confirmation number on the screen. Commenters who did not record their number or are unsure if their comments have been received may initiate a name search to confirm that their comments have been filed. If the commenter's name does not appear in the system, the commenter should refile and record the confirmation number.

7. Does the FCC have all of the resources and expertise it needs in order to combat attacks like those that occurred on May 8?

Although the FCC has demonstrated the resiliency of its systems, we must be consistently vigilant in safeguarding IT assets to ensure system availability for all constituents. The FCC is dependent upon its IT team to deal with any issues that may occur going forward and they are continuing to explore potential improvements to the system. If the Commission needs additional resources to address system and cybersecurity issues, we will work with OMB and the Appropriations Committees to ensure that we have the funds to undertake essential upgrades.