

**Congress of the United States**  
**House of Representatives**  
**Washington, D.C. 20515**

July 7, 2017

The Honorable Gene L. Dodaro  
Comptroller General  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Dodaro:

We write to request that the Government Accountability Office (GAO) undertake a review of the Federal Communications Commission's (FCC) information technology and information security practices. We are requesting this review in light of recent reports regarding the agency's cybersecurity preparedness and problems with the FCC's ability to take public comments in its "net neutrality" proceeding.

Currently, the FCC is conducting a rulemaking proceeding to roll back net neutrality protections.<sup>1</sup> Problems with the FCC's net neutrality docket made headlines in May after comedian John Oliver implored his viewers to file comments about net neutrality with the FCC. Multiple media outlets reported that the FCC's Electronic Comment Filing System (ECFS) "went down"<sup>2</sup> after the John Oliver segment, noting that "the FCC's servers appeared to be overwhelmed by the flood of traffic."<sup>3</sup>

The following day, on May 8, 2017, the FCC's Chief Information Officer (CIO) announced that the FCC "was subject to multiple distributed denial-of-service attacks," a situation that made it "difficult for legitimate commenters to access and file with the FCC."<sup>4</sup> Although the FCC's CIO noted that the agency "worked with our commercial partners to address this situation," we hope to obtain additional information, particularly whether the agency's cyber

---

<sup>1</sup> Federal Communications Commission, *Restoring Internet Freedom*, Notice of Proposed Rulemaking, WC Docket No. 17-108, FCC 17-60 (released May 23, 2017).

<sup>2</sup> Ali Breland, *FCC site crashes after John Oliver segment*, The Hill (May 8, 2017). See also, Sam Gustin, *John Oliver Just Crashed the FCC's Website Over Net Neutrality—Again*, Motherboard (May 8, 2017).

<sup>3</sup> Jeff John Roberts, *John Oliver Gets Fired Up Over Net Neutrality—and FCC's Site Goes Down*, Fortune (May 8, 2017).

<sup>4</sup> Federal Communications Commission, *FCC CIO Statement on Distributed Denial-of-Service Attacks on FCC Electronic Comment Filing System* (May 8, 2017) (press release).

systems can adequately accommodate large volumes of input from the public during high-profile rulemaking proceedings. We are also interested in a general understanding of the adequacy of the FCC's cyber controls and defenses.

Recent reports have also indicated other irregularities in the FCC's net neutrality docket, which raise other questions. These include a report that 150,000 comments from the agency's net neutrality docket may have disappeared,<sup>5</sup> as well as reports that automated comments were submitted to the FCC using names and addresses of real people without their knowledge or consent.<sup>6</sup>

Cybersecurity and other problems can have a direct functional impact on the mission of the FCC. We are concerned that these problems and irregularities raise doubts about the fairness, and perhaps even the legitimacy, of the FCC's process in its net neutrality proceeding. Giving the public an opportunity to comment in an open proceeding such as this one is crucial – so that the FCC can consider the full impact of its proposals, and treat everyone who would be affected fairly. It is also required by law. The FCC must comply with Administrative Procedure Act requirements to give the public notice and an opportunity to comment, as well as to respond to those comments.<sup>7</sup> This is important, particularly where the FCC is considering changing rules that affect everyone who uses the internet.

It is also critical that the FCC take all appropriate measures to secure its networks from cyberattacks. At a minimum, the FCC must meet cybersecurity requirements under the Federal Information Security Modernization Act (FISMA). The Chairman of the FCC is ultimately responsible under FISMA to provide information security protections for the agency.<sup>8</sup> This is especially important given that the FCC's CIO has stated that the agency experienced a cyberattack that made it difficult for members of the public to file comments with it in an open proceeding.<sup>9</sup>

---

<sup>5</sup> John Eggerton, *FCC's Network Neutrality Docket Appears to Shrink*, Broadcasting & Cable (June 8, 2017).

<sup>6</sup> Dominic Rushe, *'Pretty ridiculous': thousands of names stolen to attack net neutrality rules*, The Guardian (May 26, 2017).

<sup>7</sup> 5 U.S.C. § 553. See, e.g., *Am. Radio Relay League, Inc. v. FCC*, 524 F.3d 227 (D.C. Cir.) (2007) (remanding final rule to the FCC after finding the FCC had failed to comply with obligation under the Administrative Procedure Act to give interested parties notice and a reasonable opportunity to comment in the rulemaking process); *Home Box Office, Inc. v. FCC*, 567 F.2d 9 (D.C. Cir.) (1977) (vacating rule for failure of the FCC to comply with the Administrative Procedure Act's notice and comment requirements that are intended to "provide fair treatment for persons affected by a rule.").

<sup>8</sup> 44 U.S.C. § 3554(a).

<sup>9</sup> FCC Press Release, *supra* n. 3.

We therefore request that GAO examine the FCC's overall cybersecurity preparedness, as well as the FCC's recent reported website failures that have impeded a core function of the FCC to gather comments from the public during rulemaking proceedings. In particular, we would like GAO to:

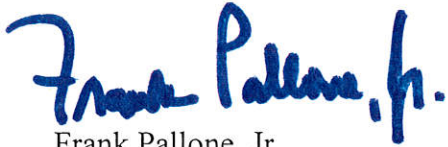
1. Identify how many visitors the FCC's comment-filing website is designed to accommodate at the same time.
2. Identify how many visitors were unable to access the FCC's website and file comments during the time the system experienced a "high amount of traffic."<sup>10</sup>
3. Identify the systems that are in place to ensure that the FCC is able to accommodate people attempting to file comments during high-profile proceedings, and determine whether the FCC has sufficient resources for that purpose.
4. Determine what analyses the FCC used to conclude on May 8, 2017, that the FCC experienced denial-of-service attacks, and assess the sufficiency of those analyses.
5. Determine whether the cause of the incident the FCC announced on May 8, 2017, was due to a cyberattack, and if so, whether the steps the agency took to deal with the alleged attack was sufficient.
6. Determine and assess what measures, if any, the FCC is taking to protect its networks, especially ECFS, from denial-of-service attacks, and the sufficiency of those measures.
7. Determine to what extent the FCC is coordinating with other federal agencies, such as the Department of Homeland Security, to investigate and to respond to the incident it announced on May 8, 2017.
8. Make, as appropriate, any recommendations for improving the security, resiliency, and capabilities, of the FCC's ECFS.

Thank you for your prompt attention to this request. If you have any questions, please contact the minority committee staff of the House Energy and Commerce Committee at (202) 225-3641, and the minority committee staff of the House Oversight and Government Reform Committee at (202) 225-5051.

Sincerely,

---

<sup>10</sup> FCC Press Release, *supra* n. 1.



Frank Pallone, Jr.  
Ranking Member  
Committee on Energy  
and Commerce



Elijah E. Cummings  
Ranking Member  
Committee on Oversight  
and Government Reform



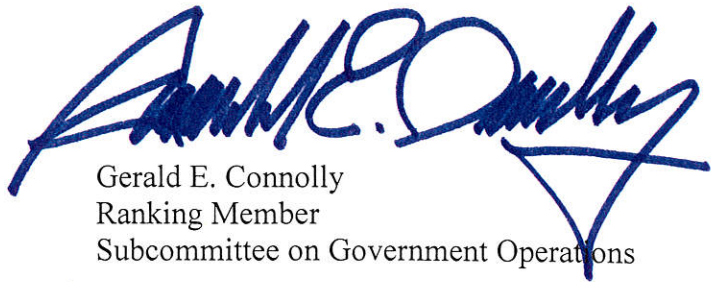
Diana DeGette  
Ranking Member  
Subcommittee on Oversight  
and Investigations



Robin L. Kelly  
Ranking Member  
Subcommittee on Information Technology



Mike Doyle  
Ranking Member  
Subcommittee on Communications  
and Technology



Gerald E. Connolly  
Ranking Member  
Subcommittee on Government Operations

Cc: The Honorable Greg Walden, Chairman  
House Committee on Energy and Commerce

The Honorable Trey Gowdy, Chairman  
House Committee on Oversight and Government Reform