

OFFICE OF INSPECTOR GENERAL

Washington, D.C. 20554



August 6, 2018

David L. Hunt
Inspector General
Federal Communications Commission

Dear David:

Enclosed is the Office of Investigation's Report of Investigation into alleged multiple distributed denial-of-service attacks involving the FCC's Electronic Comment Filing System.

Also enclosed is a written response from Chairman Pai. Because this report contains significant information relating to FCC computer systems, the public dissemination of which could imperil the security of the systems, upon conclusion of the investigation we distributed drafts of this report to both the Office of General Counsel and the Office of the Chairman in order to ascertain whether our proposed redactions were sufficiently protective. While reviewing the draft, Chairman Pai requested an opportunity to submit the enclosed written response.

Sincerely,

A handwritten signature in blue ink, which appears to read "Jay C. Keithley", is positioned above the printed name.

Jay C. Keithley
Assistant Inspector General-Investigations



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

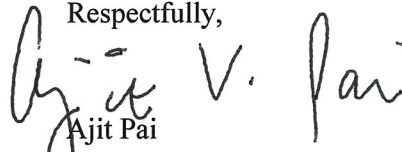
August 3, 2018

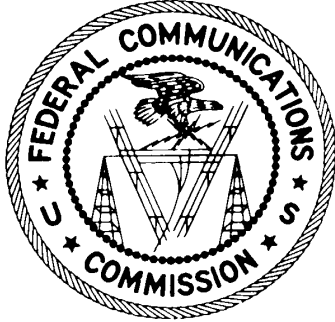
Inspector General David Hunt
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Dear Inspector General Hunt,

I commend the Office of Inspector General for its investigation into the incident involving the Commission's Electronic Comment Filing System (ECFS) that occurred on May 7-8, 2017 and am submitting this statement to provide additional information related to this incident. Specifically, on the afternoon of July 24, 2017, I held a meeting in my office with Tony Summerlin and Christine Calvosa to discuss the status of ECFS. FCC Chief of Staff Matthew Berry also attended this meeting. Among other topics, we discussed the incident that occurred on May 7-8, 2017. During this meeting, consistent with what my office had been repeatedly told by then-Chief Information Officer David Bray, Mr. Summerlin reaffirmed to me that this incident had been caused by bots rather than individuals attempting to file comments with the Commission, and he explained why that was the case. Moreover, during this meeting, neither Mr. Summerlin nor Ms. Calvosa said anything that suggested that they disagreed with the explanation Mr. Bray had provided to my office and to Congress about what happened on May 7-8, 2017. For these reasons, I was surprised and disappointed when I learned of the findings of the Office of Inspector General's investigation.

Respectfully,


Ajit Pai
Chairman
Federal Communications Commission



UNITED STATES GOVERNMENT
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: June 20, 2018

TO: David L. Hunt, Inspector General

FROM: (b) (7)(C) ; (b) (7)(C) ; (b) (7)(C)
(b) (7)(C) ; (b) (7)(C) ;

THROUGH: Jay Keithley, Assistant Inspector General for Investigations; (b) (7)(C)
.

SUBJECT: Alleged Multiple Distributed Denial-Of-Service (DDoS) Attacks involving the FCC's Electronic Comment Filing System (ECFS)

BACKGROUND

On May 7, 2017, at 11:01 p.m. EDT, the Home Box Office (HBO) program "Last Week Tonight with John Oliver" aired a segment in which the host John Oliver discussed the Federal Communications Commission's (Commission or FCC) "Restoring Internet Freedom" (RIF) proceeding (commonly also referred to as the "Net Neutrality proceeding" or Wireline Competition Docket No. 17-108) and encouraged viewers to visit the Commission's Electronic Comment Filing System (ECFS) and file comments. John Oliver provided two URLs registered by the program during the episode. Both of these URLs redirected users to a page within ECFS where comments to the RIF proceeding could be filed. On May 7, 2017, at approximately 11:30 p.m. EDT, the program also used Twitter to send out one of the URLs. On May 8, 2017, at

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

approximately 2:30 a.m. EDT, the program uploaded a recording of the episode on The Last Week Tonight with John Oliver YouTube channel and, at approximately 7:24 a.m. EDT, the program tweeted a link to the uploaded episode on The Last Week Tonight with John Oliver YouTube channel.

On May 7, 2017, at 11:30 pm EDT, the ECFS experienced a significant increase in the level of traffic attempting to access the system, resulting in the disruption of system availability. In fact, information obtained from (b) (7)(E), a contractor providing web performance and cloud security solutions to the FCC, identified a 3,116% increase in traffic to ECFS between May 7 and May 8, 2017.

On May 8, 2017, the FCC issued a press release in which the FCC's former¹ Chief Information Officer (CIO) Dr. David Bray (Bray) provided the following statement regarding the cause of delays experienced by consumers trying to file comments on ECFS:

“Beginning on Sunday night at midnight, our analysis reveals that the FCC was subject to multiple distributed denial-of-service attacks (DDoS)[²]. These were deliberate attempts by external actors to bombard the FCC's comment system with a high amount of traffic to our commercial cloud host. These actors were not attempting to file comments themselves; rather they made it difficult for legitimate commenters to access and file with the FCC. While the comment system remained up and running the entire time, these DDoS events tied up the servers and prevented them from responding to people attempting to submit comments. We have worked with our commercial partners to address this situation and will continue to monitor developments going forward.”

A copy of the full press release is included as Attachment 1. On May 9, 2017, FCC Chairman Ajit Pai (Pai) received a request for information from United States Senators Ron Wyden and Brian Schatz (Wyden-Schatz letter) related to the “multiple distributed denial-of-service attacks” against the ECFS alleged by Bray. A copy of this letter is included as Attachment 2.

Also on May 9, 2017, the FCC Office of Inspector General (OIG) was contacted by Federal

¹ Bray left the FCC and federal service on October 11, 2017.

² A denial-of-service attack (DoS) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

Bureau of Investigation (FBI) Special Agent (SA) (b) (6) to discuss the alleged DDoS attacks and offer assistance to an FCC OIG investigation of these allegations. On May 15, 2017, FCC OIG participated in a teleconference with SA (b) (6) and initiated a preliminary inquiry into the matter.

On June 15, 2017, the FCC responded to the Wyden-Schatz letter in a response signed by Chairman Pai. Bray and the FCC's Information Technology (IT) group were responsible for those sections of the response addressing technical issues. A copy of the response is included as Attachment 3.

Based on information initially gathered by OIG and because the matters discussed in the June 15, 2017 letter to Congress pertain to issues of cybersecurity and possible cybercrimes with the potential of ongoing threats to the integrity of the FCC's computer systems, OIG opened a full investigation on June 21, 2017.

On June 26, 2017, Chairman Pai, FCC Commissioner Mignon Clyburn and FCC Commissioner Michael O'Rielly received a letter from United States Representatives Frank Pallone, Jr., Elijah Cummings, Diana DeGette, Robin Kelly, Mike Doyle, and Gerald Connolly, requesting information about the multiple DDoS attacks alleged by Bray in his press release on May 8, 2017 (House letter). A copy of this letter is included as Attachment 4.

On July 21, 2017, Chairman Pai responded to the House letter. Bray and the FCC's IT group were responsible for those sections of the response addressing technical issues. A copy of the response is included as Attachment 5.

Most recently, on June 11, 2018, Chairman Pai received an additional request for information from Senators Wyden and Schatz related to the multiple DDoS attacks alleged by Bray and about similar allegations involving the FCC's net neutrality proceeding in 2014. A copy of this letter is included as Attachment 6 to this Report of Investigation.

INVESTIGATION

The original incident, as described by Bray in his press release and by the Commission in its first response to Congress, formed the basis of our investigation into this matter. Initially, the investigation focused on whether any computer crimes may have been committed. As the investigation proceeded we expanded the scope of our inquiry to include an examination of: (1) precisely what happened to cause the degradation of the ECFS system availability that began at 11:30 p.m. EDT on May 7, 2017 ("the event"); (2) the steps the Commission took in response to

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

the event; and (3) the Commission's explanation of the event.

To conduct the investigation, FCC OIG investigators: (1) obtained and reviewed email correspondence from FCC staff and contractors involved in responding to the event; (2) made numerous inquiries to the FCC IT group related to (a) the event; (b) the basis for the press release and subsequent responses to Congressional requests for information; and (c) to the actions taken by the FCC IT group in response to the event; (3) corresponded with representatives from (b) (7)(E) to obtain an understanding of their perspective as a web performance and cloud security provider to the FCC; (4) conducted interviews with representatives from the Department of Homeland Security (DHS) United States Computer Emergency Response Team (US-CERT), Federal Bureau of Investigation (FBI), FCC management, and FCC IT Group contractors and staff; and (5) obtained and analyzed ECFS server logs. Specific steps taken during the investigative process were as follows:

1. Obtained and reviewed email correspondence from: Matthew Berry, Chief of Staff in the Office of the Chairman (OCH); Dr. David Bray, former Chief Information Officer (CIO) in the Office of Managing Director (OMD); Leo Wong, Chief Information Security Officer (CISO) in OMD; Tony Summerlin, FCC contractor serving as a "Senior Strategic Advisor" in the Commission's IT Group; Christine Calvosa, Acting³ CIO in OMD; (b) (6)
[REDACTED]
2. Obtained and examined ECFS logs from the period from May 7, 2017 through May 9, 2017. The following logs were obtained and examined:

(b) (7)(E)
[REDACTED]

³ Christine Calvosa became Acting CIO when Bray left the FCC and federal service on October 11, 2017.

⁴ On May 15th, OIG requested information related to the multiple DDoS attacks alleged by Bray including "copies of all the logs and records" used to support the analysis referenced in his press release. We were advised by the IT group that the information we were requesting, including the logs, are "retained and non-modifiable." During the investigation, we became aware that (b) (7)(E) maintained logs for both the web (www.fcc.gov) and ECFS API (ecfsapi.fcc.gov). (b) (7)(E)
[REDACTED]

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

- Logs maintained by the General Services Agency (GSA) related to API submissions to ECFS filed through GSA's data.gov system.
3. Obtained and reviewed ECFS system documentation to obtain an understanding of the Application Programming Interface (API) functionality.
 4. Provided detailed questions to (b) (7) related to the event. Obtained and reviewed responses.
 5. Obtained and reviewed DHS US-CERT reporting requirements.
 6. Obtained and reviewed FCC Standard Operating Procedure (SOP) for Incident Response.
 7. Obtained and reviewed NIST Computer Security Handling Guide.
 8. Obtained and reviewed Presidential Policy Directive (PPD)-41 related to United States Cyber Incident Coordination.
 9. Obtained and reviewed information provided to FCC OIG Audit as part of the FISMA audit.
 10. Interviewed (b) (6) from DHS/NCCIC/US-CERT. A copy of the Memorandum of Interview (MOI) is included as Attachment 7.
 11. Interviewed (b) (6), FCC contractor with (b) (6). (b) (6) works on an engineering team providing support to the IT group. A copy of the MOI without exhibits is included as Attachment 8.
 12. Interviewed FBI Special Agent (SA) (b) (6). A copy of the MOI without exhibits is included as Attachment 9.
 13. Interviewed (b) (6), IT group. A copy of the MOI without exhibits is included as Attachment 10.

(b) (7)(E)

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

14. Interviewed Leo Wong, FCC Chief Information Security Officer (CISO). A copy of the MOI without exhibits is included as Attachment 11.
15. Interviewed Matthew Berry, Chief of Staff. A copy of the MOI without exhibits is included as Attachment 12.
16. Interviewed Tony Summerlin, FCC contractor with Censeo Consulting Group, Inc. Summerlin serves as a Senior Strategic Advisor within the IT group. A copy of the MOI without exhibits is included as Attachment 13.
17. Interviewed Christine Calvosa, Acting Chief Information Officer (CIO). A copy of the MOI without exhibits is included as Attachment 14.

FINDINGS

ISSUE 1- *What caused the degradation of the FCC's ECFS on May 7-8, 2017?*

Multiple Distributed Denial-of Service (DDoS) attacks did not occur

The Federal criminal statute governing distributed denial-of-service attacks against government computer systems is codified in 18 U.S.C § 1030 - Fraud and related activity in connection with computers. 18 U.S.C. § 1030 (a)(5)(A) states that whoever “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer” shall be “punished as provided in subsection (c) of this section.” 18 U.S.C. § 1030 (e)(2)(A) defines the term “protected computer” as a computer “exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government.” 18 U.S.C. § 1030 (e)(8) defines the term “damage” to mean “any impairment to the integrity or availability of data, a program, a system, or information.”

Since Bray alleged the attacks were “deliberate attempts by external actors to bombard the FCC’s comment system” and the external actors were “not attempting to file comments themselves; rather they made it difficult for legitimate commenters to access and file with the FCC,” the initial focus of our investigation was the identification of those groups or individuals who were responsible for the multiple distributed denial-of-service attacks alleged by Bray in the press release.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

Our investigation did not substantiate the allegations of multiple DDoS attacks alleged by Bray. While we identified a small amount of anomalous activity and could not entirely rule out the possibility of individual DoS attempts during the period from May 7 through May 9, 2017, we do not believe this activity resulted in any measurable degradation of system availability given the miniscule scale of the anomalous activity relative to the contemporaneous voluminous viral traffic. In order to assess incoming traffic as a DDoS, we need to identify coordination and intent. Coordination is a key requirement in a DDoS; coordination can occur via a single command and control computer (in the case of a botnet) or preplanned actions from a group online. Evidence of coordination in a DDoS may include identical requests, identical user-agents, or large waves of simultaneous activity. We found no evidence of such coordination. During our discussion with FBI SA (b) (6) on May 15, 2017, we specifically asked if the FBI was aware of any intelligence suggesting there was a coordinated attack, and we were advised the FBI had no such intelligence. Intent is much more difficult to identify; for example, traffic from a single source that may appear to be attempting a DoS could simply be a search-engine or web-crawler. Similarly, oddly formed web-requests could be the result of malicious actors, or they could be the result of an amateur programmer learning how to submit well-formed API requests. Regardless, we did not find any evidence of intent to conduct a DDoS.

The degradation of ECFS system availability was likely the result of a combination of: (1) “flash crowd”⁵ activity resulting from the Last Week Tonight with John Oliver episode that aired on May 7, 2017 through the links provided by that program for filing comments in the proceeding; and (2) high volume traffic resulting from system design issues.

During “The Last Week Tonight with John Oliver” segment pertaining to the Net Neutrality (RIF) proceeding, John Oliver provided two (2) URLs registered by the program (justtellmeifimrelatedtoanazi.com and gofccyourself.com) that redirected users to the page within ECFS where comments could be filed. The redirect URL justtellmeifimrelatedtoanazi.com was mentioned by Oliver at approximately 11:04 p.m. EDT. Although the justtellmeifimrelatedtoanazi.com URL redirected users to the ECFS express comment filing page for the Net Neutrality proceeding, Oliver did not explain that functionality when mentioning the URL during the episode. Oliver mentioned the redirect URL gofccyourself.com at approximately 11:17 p.m. EDT, when he explained the purpose for the

⁵ A “flash crowd” refers to a sudden increase in traffic due to a large number of requests arriving at a web application within a short timeframe. Flash crowds are driven by public interest, sudden popularity, extremely effective marketing or viral social media interest.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

gofccyourself.com URL was to file comments in the Commission's RIF proceeding and encouraged viewers to use the URL to file comments in that proceeding. At approximately 11:29 p.m. EDT, the program used Twitter to send the following tweet⁶ containing the gofccyourself.com URL to approximately 2.71 million Twitter followers.



On May 8, 2017, at approximately 2:30 a.m. EDT, the program uploaded a recording of the episode on The Last Week Tonight with John Oliver YouTube channel. At approximately 7:24 a.m. EDT, the program tweeted a link to the uploaded episode on The Last Week Tonight with John Oliver YouTube channel.

⁶ The timestamp in the tweet is presented in Pacific Daylight Time (PDT) as 8:29 p.m. PDT (-0700 UTC). Represented in Eastern Daylight Time (EDT), the timestamp is 11:29 p.m. EDT (-0400 UTC).

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)



At 11:30 p.m. EDT, one minute after the gofccyourself.com link was tweeted by The Last Week Tonight with John Oliver program, the FCC's Electronic Comment Filing System (ECFS) experienced a significant increase in the level of traffic attempting to access the system.

OIG Log Analysis

Throughout the Net Neutrality (RIF) proceeding, the FCC provided the public with three methods to submit comments electronically: filling out and submitting the web express comment form directly to ECFS; submitting comments by using the FCC public API with a Data.gov API key⁷; and uploading spreadsheets in CSV format containing multiple comments. Ultimately, each method resulted in comments being posted to ECFS. However, the web form and API method provided users with a direct interface to ECFS as the file upload had a delay in place to enable file scanning and verification of file formatting.

The ECFS system uses (b) (7)(E) as its database for collecting, storing, indexing, and retrieving comments. Interaction with the ECFS database, whether human or machine-generated, is conducted with the (b) (7)(E) API, also referred to as the ECFS API or the

⁷ Users are able to register for a public API key through Data.gov. This public API key allows commenters to use the FCC public API to, respectively, submit and retrieve comments and documents to and from ECFS without having to manually interact with the ECFS webpage. In order to submit a comment via the public API, users must pass a properly formatted JSON document to the ECFS filings domain using their API key. This can be done manually using a command line interface program such as cURL. The FCC user guide for the public API is available at https://www.fcc.gov/ecfs/help/public_api.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

internal API. For example, if a user submits a comment via the web form, a POST request containing the comment formatted as a JSON document is automatically generated and submitted to the ECFS API. If a user were to visit [https://www.fcc.gov/ecfs/search/proceedings?q=name:\(\(17-108\)\)](https://www.fcc.gov/ecfs/search/proceedings?q=name:((17-108))), justtellmeifimrelatedtoanazi.com, or gofccyourself.com, a GET request containing a search for the Net Neutrality (RIF) proceeding would automatically be generated and submitted to the ECFS API. Instead of interacting with the FCC webpage, which converts web forms and searches to requests sent to the ECFS API, users can interact more directly with ECFS with an API key for the Data.gov API, sometimes referred to as the FCC public API or the Data.gov API. With the Data.gov API key, users instead submit their comments by submitting their own JSON documents via POST requests directly to the ECFS API. Similarly, they can retrieve and download comments by submitting GET requests directly to the ECFS API.

Traffic generated by requests using a Data.gov API key is captured in the Data.gov API logs. Since all interaction with ECFS is conducted via the ECFS API, whether it is machine generated through the web form or human generated through the Data.gov API key, all traffic is captured by the (b) (7)(E)

The (b) (7)(E) captures web traffic for the FCC domain (www.fcc.gov). The log captures (b) (7)(E) Based on our understanding of ECFS and the information captured in the various ECFS logs, OIG focused our analysis on the following logs:

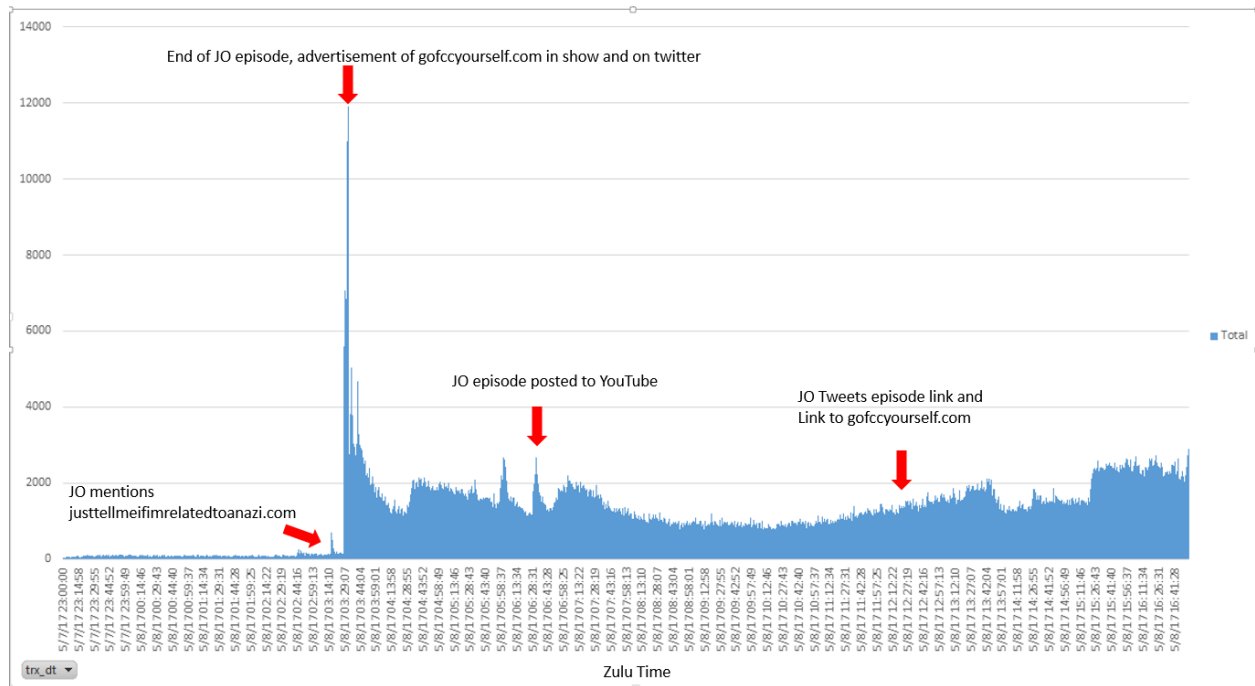
(b) (7)(E)

(b) (7)(E) – The baseline analysis of the (b) (7)(E) for the FCC domain (see Figure 1 below) show spikes in web traffic coinciding exactly with the timing of: (1) the release of information during the Oliver’s episode; (2) the release of the episode on The Last Week Tonight with John Oliver YouTube channel; and (3) tweets about that release. These spikes in traffic are singular rather than sustained, that is, the unique IP addresses that visited the FCC domain and ECFS did not do so over a sustained period of time, at regular intervals (as would be expected during a DDoS).

Figure 1: Transactions in (b) (7)(E), 5/7/2017@23:00-5/8/2017@17:00

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)



(b) (7)(E) - The analysis of the (b) (7)(E) (see Figure 2 below) shows spikes in activity similar to those in the (b) (7)(E) Web Log. API requests initially spiked to coincide with both the justtellmeifimrelatedtoanazi.com link and the gofccyourself.com link. Several spikes in API requests did occur that do not appear in the (b) (7)(E) weblogs; the first of these increases occurs around 5:00 a.m. on May 8, 2017. The majority of these requests received a 503 or 404 response,⁸ many of which are GET⁹ requests to the (b) (7)(E).¹⁰ These spikes are likely the result of ECFS downtime and (b) (7)(E) under its then-current configuration, not sufficiently handling the surge in activity. There are also a series of spikes in API requests that coincide with John Oliver posting the episode to YouTube and then

⁸ A 503 response indicates that a server is unavailable, a 404 response indicates that the server could not locate the requested file.

⁹ Within the Hyper Text Transfer Protocol (HTTP), various request methods are used to communicate between a client and a server. Two of the most common HTTP request methods are GET and POST. A GET request is used when a client requests data from a server, for example, viewing a webpage or downloading a document. A POST request is used to send data to a server, for example, posting a comment to a forum or uploading a file.

¹⁰ (b) (7)(E) is a utility that, when queried, verifies the most efficient route from the requestor to the origin.

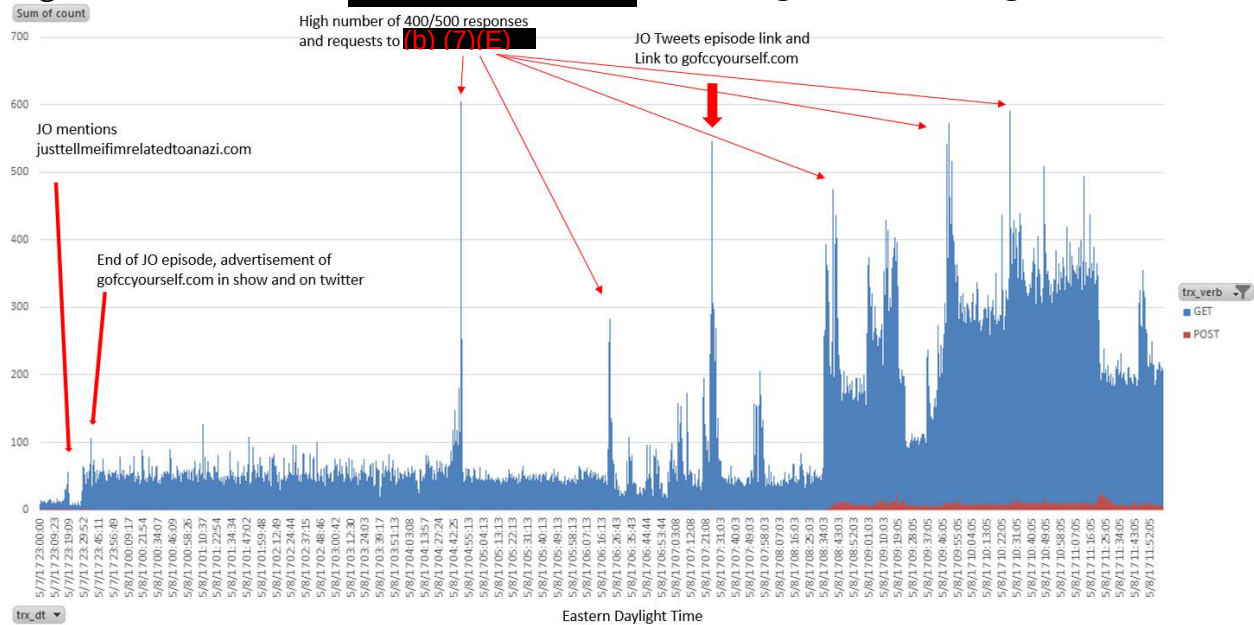
Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS

REPORT OF INVESTIGATION (continuation sheet)

tweeting the gofccyourself.com link. The number of GET requests far outnumber the number of POSTs to ECFS; this was likely caused by many more users visiting the Net Neutrality (RIF) proceeding comment submission page than actually posting a comment.¹¹

Figure 2: Transactions in (b) (7)(E), 5/7/2017@23:00-5/8/2017@12:00



Data.gov API Logs – As stated previously, the traffic generated by requests using a Data.gov API key is captured in the Data.gov API logs. The analysis of the Data.gov API logs (see Figure 3 below) did not show a spike in public API traffic associated with John Oliver show activity. OIG examined the activity associated with the spikes occurring after the John Oliver show activity and determined the spikes are related to the filing of bulk comments through the Data.gov API related to the Net Neutrality (RIF) proceeding and routine data gathering activities.

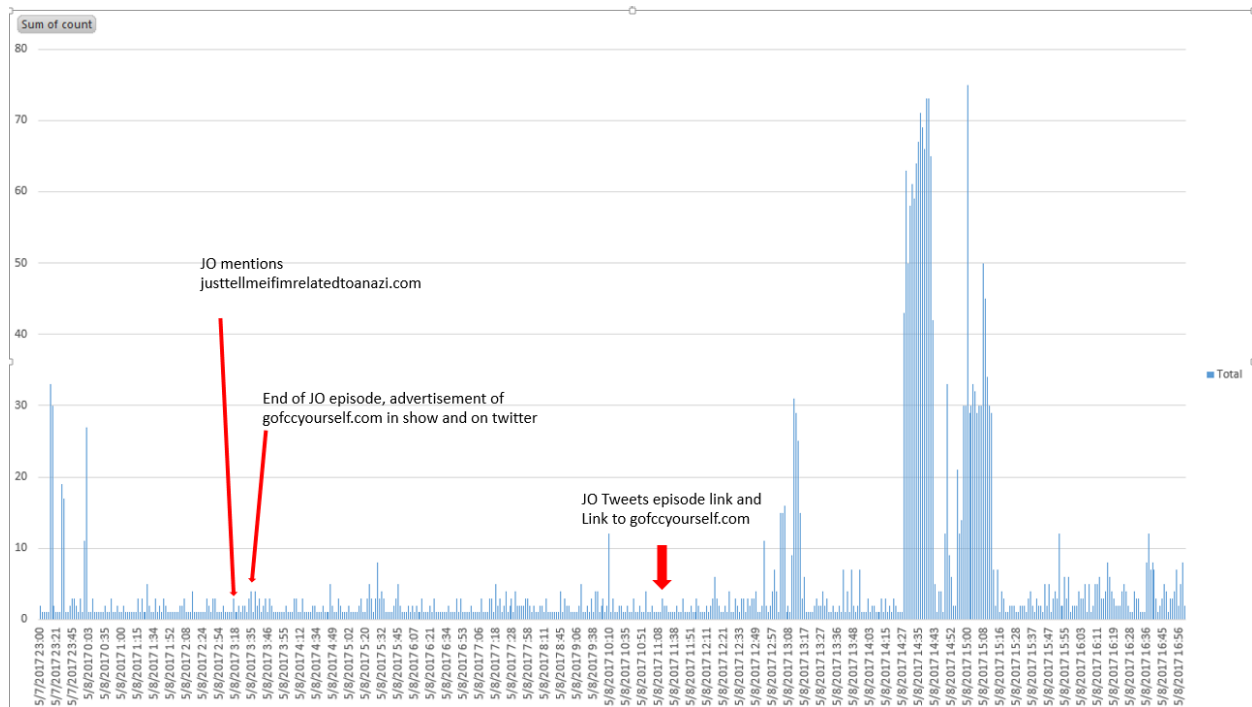
Figure 3: Transactions in Data.gov API Logs, 5/7/2017@23:00-5/8/2017@17:00

¹¹ ECFS uses (b) (7)(E) to store, retrieve, and file comments. (b) (7)(E)

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS

REPORT OF INVESTIGATION (continuation sheet)



Discussions with (b) (7) (E)

In addition to analyzing ECFS logs, OIG contacted (b) (7) (E) to obtain their perspective of the event. On November 15, 2017, FCC OIG sent a series of questions to (b) (7) (E) related to the event, and (b) (7) (E) responded to these questions on December 4, 2017. On December 12, 2017, FCC OIG sent follow-up questions and (b) (7) (E) responded on December 28, 2017. Significant information provided by (b) (7) (E) is as follows:

- (b) (7) (E) began generating the automated high traffic alerts that were sent to the FCC at approximately 11:52pm ET on Sunday, May 7, 2017. These automated alerts were first reviewed by (b) (7) (E) support services team between 8-9am ET on Monday, May 8, 2017.
- (b) (7) (E) FCC customer support team received an email from FCC's designated primary technical point of contact (POC), (b) (6), inquiring if the increased traffic to the ECFS API was coming from specific IP addresses. The email was received at approximately 8:13am ET on Monday, May 8th, and the (b) (7) (E) Services team responded at approximately 9am ET that same day.

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS

REPORT OF INVESTIGATION (continuation sheet)

- (b) (7) reviewed traffic reports and security monitoring reports via its (b) (7)(E), and analyzed (b) (7) server logs generated for traffic delivered through (b) (7) on May 7, 2017, 12:00am-11:59pm ET and May 8, 2017, 12:00am-11:59pm ET, for the www.fcc.gov and ecfsapi.fcc.gov hostnames. These internal (b) (7) logs contain (b) (7)(E). (b) (7) also used a network debugging tool to determine relevant IP information such as geographic and network locations associated with the IP addresses from which traffic was originated.
- (b) (7)(E) support services team generated an informal report of the log analysis results for traffic delivered via the ecfsapi.fcc.gov hostname. This report, sent by email to the FCC IT group, included the following information on traffic over the previous two days (May 7-8, 2017):
 - o the top 10 requested IP addresses (client → (b) (7) edge);
 - o origin response codes (b) (7) edge → FCC origin); and
 - o (b) (7) (b) (7) formatted URLs sent to the FCC origin).
- (b) (7) saw a dramatic increase in the traffic levels delivered through (b) (7) during the event. FCC traffic (bytes) delivered increased by 3,116% over normally observed levels. Prior to May 7, 2017, average daily traffic was approximately 172 GB/day. Between May 7 and 8, 2017, the FCC site served approximately 4.5 TB (4,505 GB) of traffic.

The traffic observed appeared to be a mix of “human” and automated traffic. One item in particular is worth noting regarding the impact of the FCC’s site design on traffic levels during high traffic events such as was experienced in the May 7th event. (b) (7)(E)

Specific examples of the traffic observed is provided in greater detail below.

(b) (7)(E)

(b) (7)(E)

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS

REPORT OF INVESTIGATION (continuation sheet)

(b) (7)(E)

- (b) (7)(E) saw a combination of live and automated traffic. Based upon (b) (7)(E) review of the internal log files associated with the May 7th incident, (b) (7)(E) believes that the majority of the traffic observed during the incident was a combination of “flash crowd” activity and increased traffic volume resulting from (b) (7)(E) site design issues discussed in the previous response.

With respect to the system design issue identified during the discussion with (b) (7)(E) OIG investigators questioned (b) (6) about site design issues during his interview. (b) (6) with the FCC IT group and is recognized within the IT group as a subject matter expert for ECFS. (b) (6) confirmed ECFS had a design flaw such that (b) (7)(E) (b) (6) further explained that, while his team remedied this issue, they later noted similar issues on May 17, 2017, involving traffic from a site called ComeAstroturf.com, which conducted a name search on ECFS (b) (7)(E).¹²

ISSUE 2 – *How did the FCC respond to the event?*

The FCC did not respond to the event internally in a manner consistent with the severity of the event as stated in the press release.

As noted above, the original objective of the OIG investigation was to identify the individuals and/or organizations responsible for the multiple DDoS attacks alleged by Bray. To determine those individuals and/or organizations that may have been culpable, we expected to rely on work

¹² ComCastroturf is a website that describes its purpose as helping individuals find out whether their identities were stolen to post anti-net neutrality comments to the FCC. It provides a form that runs on a search on the FCC’s ECFS system. The website was created on May 15, 2017.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

performed by Commission staff or contractors in response to the event. (b) (7)(E)

[REDACTED]

To do that, we expected to obtain and review the analysis referenced by Bray in the press release and to obtain and review logs and supporting documents for that and subsequent analyses. However, we learned very quickly that there was no analysis supporting the conclusion in the press release, there were no subsequent analyses performed, and logs and other material were not readily available. As a result, we devoted a significant amount of time reviewing email correspondence, corresponding with IT staff and contractors, and finally conducting interviews. During that process, we determined the FCC did not respond to the event internally in a manner consistent with the severity of the event suggested in the press release.

FCC Management was aware The Last Week Tonight with John Oliver program was considering an episode on the Net Neutrality proceeding but did not share that information with the CIO or IT group.

During our review of email correspondence related to the event, OIG identified an email message from (b) (6) to MediaRelations@fcc.gov in which (b) (6) states "I'm a producer with Last Week Tonight with John Oliver. We may be doing a piece this week about net neutrality and the NPRM about possibly undoing the classification of ISPs under Title II" and "We don't have an exact script yet but I wanted to give you an early heads up to make sure we can allot some time for a call later this week -- perhaps Thurs or Fri. Let me know some times that might work on your end." The individual monitoring the MediaRelations@fcc.gov email account forwarded this message to Matthew Berry (Berry), Chief of Staff, (b) (6)

[REDACTED] We identified additional internal discussions related to (b) (6) including a series of questions from (b) (6) related to the net neutrality proceeding. Ultimately, the FCC decided not to respond to her.

In addition to the message from the Last Week Tonight with John Oliver program, OIG identified a Politico Pro article from May 2, 2017 with the headline "John Oliver returning to net neutrality debate" that was circulating in the Office of Media Relations and the Office of the Chairman. This article states that the program is "working on a new net neutrality segment, focused on current Chairman Ajit Pai's effort to undo the rules that could run as early as Sunday, according to sources familiar with the show's plans."

We were not able to find definitive evidence that management shared information about the

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE INFORMATION
FCC Office of Inspector General
Page 16 of 46

REPORT OF INVESTIGATION (continuation sheet)

planned episode with anyone in the IT group. During our interview with Berry, Berry told us he may have made IT aware of the Oliver episode but he wasn't sure. No one in the IT group recalled receiving such a notice/heads-up regarding an Oliver Net Neutrality segment. During our interview with Tony Summerlin (Summerlin), Summerlin said "Bray was furious that he had not been informed about the John Oliver episode."

The conclusion that the event involved multiple DDoS attacks was not based on substantive analysis and ran counter to other opinions including those of the ECFS subject matter expert and the Chief of Staff.

In the press release, Bray states that "our analysis" revealed the FCC was subject to multiple DDoS attacks and the "attacks were deliberate attempts by external actors to bombard the FCC's comment system with a high amount of traffic." On May 15, 2017, OIG requested the analysis referenced by Bray in the press release as well as copies of all of the logs and records used to support the analysis (including email correspondence); names and contact information for all of the FCC and contractor personnel who were involved in that analysis; and the results of any analysis (including supporting records) performed subsequent to the press release. OIG first became concerned about the veracity of the analysis referenced by Bray in the press release during a teleconference with Leo Wong (Wong) and Summerlin on June 20, 2017. During the teleconference, OIG was advised by Wong that no document was prepared summarizing the analysis referenced in the press release. Wong further stated that "analysis" would be a strong word to describe the work done to support the conclusion that Bray made in the press release and that "preliminary assessment" would be a better way to describe the work that was done. Wong explained that FCC IT group staff "analyzed the logs¹³" and identified a large number of API hits that did not result in comments being filed. They also analyzed where the "bots" and/or API calls were originating and determined they were coming from Cloud providers (e.g., (b) (7)(E) etc.). Wong explained that this analysis was the basis for Bray's statement. OIG was further advised that no additional analysis or after-action work has been done related to the alleged DDoS.

On June 30, 2017, OIG received copies of Outlook mailboxes for Bray, Wong, Berry, and Summerlin. When we reviewed email correspondence for the period immediately preceding the alleged DDoS attacks and up to the time the press release was issued, we did not identify any evidence of substantive analysis supporting the conclusion that multiple DDoS attacks were the cause of the disruption. In fact, we identified email correspondence showing that (b) (6), the ECFS subject matter expert, believed the disruption was a result of the John Oliver episode (an

¹³ We subsequently determined that no log analysis was ever performed by FCC staff.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

opinion he communicated to Bray and others). We did not identify any email correspondence questioning this opinion or requesting additional analysis. We also identified email correspondence between Berry and Bray prior to the issuance of the press release in which Berry requested confirmation that this “wasn’t a bunch of John Oliver viewers attempting to comment at the same time that did this but rather some external folks deliberately trying to tie-up the server” and Bray provided that confirmation. Significant email correspondence from the email chains are as follows:

<u>Date</u>	<u>Time</u>	<u>From:</u>	<u>To:</u>	<u>Message</u>
5/8/2017	9:01:53 am	Tony Summerlin	(b) (6)	Where are these requests coming from? This is ridiculous.
5/8/2017	9:14:04 am	(b) (6)	Tony Summerlin	Working with (b) (7) on that.
5/8/2017	10:39:27 am	David Bray	(b) (6) (b) (6) Matthew Berry (b) (6) Brian Hart	Closing the loop on this – as of 0845 the system was stabilized to address the increased high traffic. If asked, the system was never down – it was always up and running. However some external folks attempted to send high traffic in an attempt to tie-up the server from responding to others, which unfortunately makes it appear unavailable to everyone attempting to get through the queue. [(emphasis added)] We should be prepared for more attempts like this. There is also the Box.com instance for bulk filers too as a backup should the system appear unavailable.
5/8/2017	10:43:49 am	(b) (6)	David Bray (b) (6)	Not sure there are heavy talkers currently. The gofccyourself.com (John Oliver page) causes the user to be redirected to FCC so we are likely being hit with few requests per IP but from many IPs. [(emphasis added)] We are investigating what we can do to identify the traffic and make the requests/submissions more efficient. We peaked at about 35K web requests and 30K API request per minute. Few minutes ago, we were at 20K API requests per minute with a <1 second response time.
5/8/2017	10:43:55 am	Matthew Berry	David Bray (b) (6) (b) (6) Brian Hart	I’d like to be able to get an explanation out to the press so let’s discuss ASAP. Are you confident that it wasn’t a bunch of John Oliver viewers attempting to comment at the same time that did this but rather some external folks deliberately trying to tie-up the server? [(emphasis added)]

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS

REPORT OF INVESTIGATION (continuation sheet)

5/8/2017	10:49:54 am	David Bray	Matthew Berry (b) (6) [REDACTED] Brian Hart	I can meet now – shall I head up? (I'll call you). Yes, we're 99.9% confident this was external folks deliberately trying to tie-up the server to prevent others from commenting and/or create a spectacle. Jon Oliver invited the "trolls" – to include 4Chan (which is a group affiliated with Anonymous and the hacking community). His video triggered the trolls. Normal folks cannot manually file a comment in less than a millisecond over and over and over again, so this was definitely high traffic targeting ECFS to make it appear unresponsive to others. [(emphasis added)] The good news was (b) (7) helped us identify some of the heavy talkers hitting us before its "normal business hours" (9 to 5pm apparently?).
5/8/2017	10:56:50 am	(b) (6)	David Bray	Just quick update so we can be on the same page. ECFS status will go out around noon. The John Oliver gofccyourself.com page is likely causing us some headaches. Since the users are being re-directed to FCC the source IP is that of the user and not a central server. [(emphasis added)] We are looking for ways to identify the traffic and to make the comment submission less taxing on our API servers. Use of a static page specifically for 17-108 express submission should be seriously considered. Alternatively, we are identifying a deep link to the express submission for 17-108. Peak at 35K web requests and 30K API request per minute. We are currently stable at 20K API requests per minute with < 1 second response time. (b) (7)(E) [REDACTED] -We are looking for ways to improve caching at (b) (7) and/or (b) (7). -Waiting room is not yet working. -The API server logs are growing at 1GB per hour

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS

REPORT OF INVESTIGATION (continuation sheet)

				which is not sustainable. Working on fixing this. Result of not fixing it is a crash of the API server – we want to avoid this.
5/8/2017	11:08:25 am	(b) (6)	Tony Summerlin	John Oliver’s gofccyourself.com page. But the user is being redirected so it is hard to identify it as the source. We’re working on it. [(emphasis added)]
5/8/2017	12:48:18 pm	(b) (6)	Tony Summerlin	<u>Not really, we can’t really identify what comes via gofccyourself.com (easier to explain in person).</u> [(emphasis added)] However; I do believe I have a potential solution: The gofccyourself.com redirect the user to the 17-108 proceeding URL. If we create a static page (no APIs, plain static html page) that looks like the express comment form, we can have (b) (7) or (b) return that page instead and the users will be able to submit a comment into 17-108 with just one API call (when the user hits submit). That will eliminate the numerous API calls which is killing us. Not sure what it may break but I’ll try to figure that out. Badly architected this thing. [(emphasis added)]

During our interview with (b) (6), we asked (b) (6) specifically about the analysis referenced by Bray in the press release. (b) (6) explained that (b) (6) team provided Bray with statistics regarding ECFS on May 7, but did not conduct log analysis or any other form of analysis. (b) (6) stated (b) (6) “did not agree with Bray’s understanding of the definition of a DDoS attack” and (b) (6) “did not view the ratio of comments to overall web traffic as very problematic.” (b) (6) further stated that (b) (6) would not come to the same conclusions as Bray did “so easily.”

During our interview with Berry, we asked Berry about his request for confirmation from Bray that this “wasn’t a bunch of John Oliver viewers attempting to comment at the same time that did this but rather some external folks deliberately trying to tie-up the server.” Berry stated he “assumed the Oliver segment was the cause of the increased traffic on ECFS, but Bray told him that wasn’t so.” Berry acknowledged he questioned Bray about the possibility that the event was caused by the result of the gofccyourself.com URL that the Oliver program had established, and he relied on Bray’s response that the event was not the result of that URL.

The FCC did not define the event as a cyber security incident, did not refer the matter to US-CERT in accordance with federal policy, and did not implement internal processes for responding to cyber security incidents.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

Because the FCC determined that the severity of this event warranted a press release and given the level of congressional and media attention to the event, we assumed the FCC would have classified the event internally as a cyber security incident and that they would have followed federal guidelines as well as FCC policies and procedures as part of the incident response process. As we attempted to collect available information related to the event, we discovered the FCC had not defined the event internally as a cyber security incident, that the matter had not been referred to US-CERT, and that none of the documents required under the FCC's Standard Operating Procedures (SOP) for Incident Response had been prepared.

On July 12, 2017, OIG requested a large volume of information related to the event, including various documents described in the FCC's SOP for Incident Response. In response to that request, we were instructed by Wong to discuss the matter with the OIG team conducting the FY 2017 Integrated FISMA¹⁴ and Financial Statements Audit. We were advised by the FISMA auditors that they had participated in a meeting with IT staff including Wong and Summerlin on July 6, 2017 and that, during that meeting, Summerlin advised the OIG auditors that the FCC had not classified the event as a cyber security incident and did not report the incident to US-CERT. Summerlin provided the following explanation (taken from notes prepared by (b) (7)(E) [REDACTED], the contractor conducting the audit):

"There were individuals using legitimate IP addresses to open as many sessions as they could to leave comments to the FCC. People were opening comments without posting anything which caused blank sessions to be opened up. There was nothing in the agreement with (b) (7)(E) [REDACTED] for expanding space, and therefore the FCC did not have sufficient resources to handle it. In the broadest sense, this was a denial of service attack because it denied people service due to overuse of the application and took up all of the resources that they had. FCC elected not to report it to US-CERT because although the application was shut down for 8 hours, individuals have a total of 60 days to file a comment. Overall, it was just an IT consequence of not having enough resources."

ISSUE 3- Did the FCC misrepresent facts and provide misleading responses to Congressional inquiries related to the incident?

As detailed above, OIG examined the statement made in the press release and the responses made to Congressional requests for information to determine how the FCC reached the conclusion that multiple DDoS attacks occurred and to identify sources of evidence of the DDoS

¹⁴ Federal Information Security Management Act (FISMA)

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

attacks. We requested support for statements made by the FCC in the press release and Congressional responses, reviewed email correspondence, and interviewed FCC staff and contractor to determine how the DDoS attacks were identified, how the FCC responded to attacks, and how the FCC prepared responses to Congressional inquiries. As a result of our reviews and the findings articulated above, we determined the FCC, relying on Bray's explanation of the events, misrepresented facts and provided misleading responses to Congressional inquiries related to this incident.

In its response to the Wyden-Schatz letter, the FCC made several specific statements that we believe misrepresent facts about the event or provide misleading information. Following are statements in the letter we believe misrepresent facts or provide misleading information:

Statement 1 (in FCC Response to Question #1 about the nature of the DDoS attacks) - "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."

This statement is not accurate. This statement makes a distinction between the web-based ECFS interface and the API interface and claims the API interface was targeted during the event. As explained above, we found no evidence that the API interface was targeted during the event. While we recognize it was the level of API activity that ultimately resulted in the disruption to ECFS during the event, we determined this API activity was generated through the web-based ECFS interface.

During our interview with (b) (6), we asked (b) (6) for (b) (6) reaction to this statement in the letter. (b) (6) stated (b) (6) has "never seen this language before and I would hesitate to make such a statement without evidence."

Statement 2 (in FCC Response to Question #1 about the nature of the DDoS attacks) - "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."

This statement is not accurate. As stated previously, we determined the increased activity disrupting ECFS started at 11:30 p.m. EDT (not 11:00 p.m. EST) on May 7, 2017. We made this determination by reviewing system logs as discussed above, reviewing email correspondence, and interviewing IT group staff and contractors.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

During interviews with FCC IT staff and contractors, OIG investigators asked about the timing of the start of the disruption. (b) (6) confirmed (b) (6) sent an email message containing a chart showing the number of hits/second for ECFS API increased from 5 hits/second to 150 hits/second starting at 11:30 p.m. and that the information in the email message was accurate. With respect to a comment made by Bray in an email to Summerlin on May 9, 2017 in which Bray referenced a “different chart that made it look like the hits started before 1130pm (possibly before 11pm),” (b) (6) stated (b) (6) is not aware of any such chart. When presented with this email chain during his interview, (b) (6) stated that (b) (6) team saw a sharp spike in web traffic “starting at 11:30 p.m., not 11 p.m.” During the Summerlin interview, Summerlin stated he “had far too little information in the way of event logs to make any thorough determination or analysis of the event” and that his lack of data was the reason he stated the event occurred at 11pm instead of 11:30 pm. He further indicated Bray “kept stating the event occurred at 11 and not 11:30, so I attempted to find evidence to back up that claim, but was unable to gather any evidence period, due to the limited log availability.”

In a series of email messages with Wong and the others from the FCC IT group, OIG asked Wong to confirm that the increased activity started at 11:30 p.m. and why, if the activity started at 11:30 p.m., the response to Senators Wyden and Schatz stated that it started at “approximately 11:00 p.m.” In the response, Wong confirmed the activity started at 11:30 p.m. and stated “At the time the letter was prepared we did not have full confidence as to the exact time and thought that a response with an approximate time would be sufficient.”

*Statement 3 (in FCC Response to Question #1 about the nature of the DDoS attacks) -
“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.”*

This statement is misleading. With this statement, the FCC accurately reports that the links provided by the John Oliver program (gofccyourself.com and justtellmeifimrelatedtoanazi.com) redirect users to the “regular comment filing system” (i.e., the web-based ECFS interface at www.fcc.gov/ecfs) instead of the Data.gov API component of ECFS, where bulk comments can be filed. However, the implication in this statement is that the event must not have been related to the John Oliver episode because: (1) it was the level of Data.gov API activity that increased significantly and disrupted the availability of ECFS; and (2) this API activity originated from the Data.gov API interface rather than the web-based ECFS interface where John Oliver directed viewers to comment. Through our investigation, we have determined that the redirect URLs provided by the Last Week Tonight with John Oliver program did, in fact, generate a significant amount of internal API activity and it was this internal API activity (not Data.gov API activity),

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

combined with the system design issues addressed in the section “Discussions with (b) (7)(E) above, that was likely the reason for the degradation of ECFS availability.

OIG investigators first became aware of the interaction between the redirect URLs and API activity during an interview with (b) (6) on November 7, 2017. During that interview, (b) (6) indicated the [https://www.fcc.gov/ecfs/search/proceedings?q=name:\(\(17-108\)\)](https://www.fcc.gov/ecfs/search/proceedings?q=name:((17-108))) URL (the redirect associated with both gofccyourself.com and justtellyourself.com) would make an API call (i.e., request for information or resources) and the request would generate (b) (7)(E) API calls.¹⁵ (b) (7)(E)

(b) (7)(E)

In email message on November 16, 2017, the FCC indicated it became aware of this situation “after further research.” We asked the IT group to provide information on the “research” that was performed. We were ultimately told that no further research was done, that the ECFS Subject Matter Experts (SME) assumed this (that the Oliver URLs would create API activity) was “common knowledge,” and that Bray was advised on this sometime on or after May 8th and well before the June 15th and July 27th letters through “informal discussions.”

Statement 4 (in FCC Response to Question #1 about the nature of the DDoS attacks) – “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” and “In addition to the basic findings above, our IT staff found other markers of potential malicious intent.”

These statements are not accurate and raise questions about the accuracy of additional statements the FCC made about the event. We were not able to identify any evidence that FCC staff or contractors analyzed server logs or conducted any substantive analysis. Based on our discussions with (b) (7)(E), we recognize that (b) (7) technicians analyzed (b) (7) server logs and an “informal report of the log analysis results for traffic delivered via the ecfsapi.fcc.gov hostname” was prepared and provided to the FCC. However, this analysis provided only summary information including top 10 request IP addresses (client → (b) (7) edge) origin response codes ((b) (7) edge → FCC origin), and (b) (7) (b) (7) formatted URLs sent to the FCC origin). In addition, and as explained above, (b) (7) believes the majority of the

¹⁵ At the time of the interview, OIG investigators believed that the URL would generate between (b) (7)(E)

(b) (7)(E)

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

traffic observed during the incident was a combination of “flash crowd” activity and increased traffic volume resulting from the site design issues. (b) (7) offered to provide a post event briefing to the FCC IT group, but no briefing was conducted.

During our investigation, we obtained and reviewed email correspondence related to the event and requested all of the relevant server logs. From our review of email, we know the server logs we requested were not obtained until after the response to the Wyden-Schatz letter was sent. Further, we interviewed (b) (6), the contractor who maintains the logs and who would have been the individual most likely tasked with reviewing the logs, and (b) (6) stated (b) (6) did not review the logs and is not aware of any log review having been performed.

During our interview with (b) (6), we asked about Bray’s claim of analysis supporting the malicious usage of bots. (b) (6) stated that while bots were one possible explanation, there was no analysis of which (b) (6) was aware to support those conclusions¹⁶.

Statement 5 (in FCC Response to Question #2 about the FCC requesting assistance from other federal agencies in investigating and responding to the attacks) - “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.”

This statement is not accurate. Although Wong did participate in a teleconference with FBI SA (b) (6) on May 10, 2017, the response does not accurately characterize that conversation. As part of our investigation, we interviewed SA (b) (6) to discuss the matter. SA (b) (6) denies that a “conclusion was reached that ... the attack does not appear to rise to the level of a major incident that would trigger FBI involvement.” SA (b) (6) explained that: (1) the only conversation (b) (6) had with Wong, or with anyone outside of the OIG at the FCC, was the May 10, 2017 phone call described above; (2) (b) (6) is unaware of any other FBI contacts with the FCC in this matter; and (3) “from a criminal standpoint,” (b) (6) does not consider cyber matters in terms of “major” or not. In short, (b) (6) said (b) (6) would not have agreed to anything in these terms.

In the response to the House letter, the FCC responded to a similar question related to its

¹⁶ (b) (6) thought Bray may have been referencing the statistics his team provided [(b) (7) information] but there was no log analysis conducted. However, (b) (6) also indicated that (b) (6) office would have handled any request for the logs or for analysis and (b) (6) would therefore have been aware of any analysis conducted.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

consultation with the FBI and stated “(t)he FCC consulted with the FBI following this incident, and it was agreed that this was not a “significant cyber incident” consistent with the definition contained in Presidential Policy Directive-41 (PPD-41).”

This statement is not accurate. As with the response to question #2 in the Wyden-Schatz letter, SA (b) (6) would not confirm the accuracy of the quote. During our interview with (b) (6), SA (b) (6) reiterated that “all that matters is was a crime committed or not.” SA (b) (6) does not consider cyber incidents in terms of “significant” or not. Regardless, SA (b) (6) said (b) (6) did not have enough information to reach any conclusion, especially since (b) (6) did not have any information regarding what was in the logs. SA (b) (6) also stated (b) (6) never discussed Presidential Policy Directive-41 at any time with Wong, and until OIG investigators forwarded him the July 21st letter, (b) (6) was not familiar with Presidential Policy Directive-41.

During our interview with Wong, we asked Wong to review the responses to both Wyden-Schatz and House letters related to his conversation with the FBI. Wong stated both summaries were accurate. We informed Wong that we had conducted an interview with SA (b) (6) and that SA (b) (6) disputed the FCC’s characterization of that conversation.

In response to each of the discrepancies we noted Wong replied simply with “Okay.” Wong stated there may have been a misunderstanding between himself and the FBI agent, and he [Wong] was only making the point that he did not have any evidence to characterize the May 7th incident as a major incident that would require a US-CERT response. We asked Wong whether he informed the FBI agent that he [Wong] did not have access to the logs. Wong stated he did not inform him because the FBI agent didn’t ask. Wong acknowledged he did not distinguish between a lack of evidence and evidence showing that no major incident occurred, and that this distinction may not have been clear on his part.

Violation of 18 U.S.C. § 1001

The Federal criminal statute governing False Statements is codified in 18 U.S.C. § 1001 - Statements or entries generally. 18 U.S.C § 1001 (a) states that “whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; (2) makes any materially false, fictitious, or fraudulent statement or representation; or (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry; shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331), imprisoned not more than 8 years, or both. If the matter relates to

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

an offense under chapter 109A, 109B, 110, or 117, or section 1591, then the term of imprisonment imposed under this section shall be not more than 8 years.”

Because of the possible criminal ramifications associated with false statements to Congress, FCC OIG formally referred this matter to the Fraud and Public Corruption Section of the United States Attorney’s Office for the District of Columbia (USAO-DC) on January 4, 2018 and provided a briefing to the Chief of the Fraud and Public Corruption Section USAO-DC on January 18, 2018. On June 7, 2018, after reviewing additional information and interviews, USAO-DC declined prosecution.

Conclusion

The May 7-8, 2016 degradation of the FCC’s ECFS was not, as reported to the public and to Congress, the result of a DDoS attack. At best, the published reports were the result of a rush to judgment and the failure to conduct analyses needed to identify the true cause of the disruption to system availability. Rather than engaging in a concerted effort to understand better the systematic reasons for the incident, certain managers and staff at the Commission mischaracterized the event to the Office of the Chairman as resulting from a criminal act, rather than apparent shortcomings in the system. While several in the Commission were on notice that “Last Week Tonight with John Oliver” was planning to air a segment that could generate a significant public response, that information did not reach the FCC IT group. Had such notice been provided, the IT group may have been able to take steps to ameliorate or prevent ECFS system degradation.

Recommendations

OIG is referring this matter to OCH for review and appropriate action.

Appendices

Appendix – Correspondence with (b) (7)

Attachments

Attachment 1 – May 7, 2017 FCC Press Release “FCC CIO Statement on Distributed Denial-of-Service Attacks on FCC Electronic Comment Filing System.”

Attachment 2 – May 9, 2017 letter from United States Senators Ron Wyden and Brian Schatz to

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

FCC Chairman Ajit Pai requesting information about the multiple DDoS attacks alleged by Dr. Bray in his press release on May 8, 2017.

Attachment 3 – June 15, 2017 letter from FCC Chairman Pai to United States Senators Ron Wyden and Brian Schatz responding to questions raised in their May 9, 2017 letter.

Attachment 4 – June 26, 2017 letter from United States Representatives Frank Pallone Jr., Elijah Cummings, Diana DeGette, Robin Kelly, Mike Doyle, and Gerald Connolly to FCC Chairman Ajit Pai, FCC Commissioner Mignon Clyburn, and FCC Commissioner Michael O’Rielly requesting information about the multiple DDoS attacks alleged by Dr. Bray in his press release on May 8, 2017.

Attachment 5 – July 21, 2017 letter from Pai to United States Representatives Frank Pallone Jr., Elijah Cummings, Diana DeGette, Robin Kelly, Mike Doyle, and Gerald Connolly responding to questions raised in their June 26, 2017 letter.

Attachment 6 – June 11, 2018 letter from United States Senators Ron Wyden and Brian Schatz to FCC Chairman Pai related to the multiple DDoS attacks alleged by Dr. Bray and about similar allegations involving the FCC’s net neutrality proceeding in 2014.

Attachment 7 – Memorandum of Interview (MOI) for interview with (b) (6), DHS/NCCIC/US-CERT, dated November 1, 2017.

Attachment 8 – MOI for interview with (b) (6), dated November 7, 2017.

Attachment 9 – MOI for interview with FBI SA (b) (6), dated February 8, 2018.

Attachment 10 – MOI for interview with (b) (6), dated February 15, 2018

Attachment 11 – MOI for interview with Leo Wong, FCC Chief Information Security Officer (CISO), dated March 19, 2018.

Attachment 12 – MOI for interview with Matthew Berry, Chief of Staff, dated March 30, 2018.

Attachment 13 – MOI for interview with Tony Summerlin, an FCC contractor who serves as a Senior Strategic Advisor within IT, dated April 27, 2018.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

Attachment 14 – MOI for interview with Christine Calvosa, Acting Chief Information Officer (CIO), dated May 4, 2018

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE INFORMATION
FCC Office of Inspector General
Page 29 of 46

REPORT OF INVESTIGATION (continuation sheet)

Appendix – Correspondence with (b) (7)(F)

(b) (7)(F) provides web performance and cloud security services under contract with the FCC. In that capacity, (b) (7)(F) was in a position to evaluate the traffic that caused the disruption. As part of our investigation, OIG provided a series of questions to (b) (7)(F) on November 15, 2017 and (b) (7)(F) responded to these questions on December 4, 2017. OIG provided follow-up questions to (b) (7)(F) on December 12, 2017 and (b) (7)(F) responded to the follow-up questions on December 28, 2017. Complete copies of the questions and responses are provided below.

Questions provided to (b) (7)(F) on November 15, 2017 and responses from (b) (7)(F) obtained on December 4, 2017 (responses are provided in *italics*):

General Questions related to the alleged DDoS attacks:

Please provide a general description of (b) (7)(E) role in responding to the incident on May 7th?

By way of background, the U.S. Federal Communications Commission (FCC) has purchased web performance and cloud security solutions from (b) (7)(F). Specifically, to improve site performance, the FCC uses (b) (7)(E) Secure solution. To improve the security of its sites and associated applications, the FCC uses (b) (7)(E)

(b) (7)(F) As an (b) (7)(F) customer, the FCC also receives standard support and access to the (b) (7)(E) for service administration, traffic and service usage monitoring, and service alerts.

For purposes of review of the May 7th incident, the primary FCC domains are www.fcc.gov and ecfsapi.fcc.gov. Beginning on May 7th when the traffic levels to these sites exceeded customer thresholds previously designated by the Commission, automated traffic alerts were triggered and sent by email to FCC designated recipients. Additionally, beginning on May 8th, (b) (7)(E) support services team responded by email to customer inquiries from Commission staff related to the increased traffic levels and alerts.

- When (specifically) did (b) (7)(F) become aware of the incident?

(b) (7)(F) began generating the automated high traffic alerts that were sent to the FCC at approximately 11:52pm ET on Sunday, May 7, 2017. These automated alerts were first reviewed by (b) (7)(E) support services team between 8-9am ET on Monday, May 8, 2017.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

- How did (b) (7) become aware of the incident?

(b) (7)(E) customer support team for the FCC received an email from FCC's designated primary technical point of contact (POC) (b) (6), inquiring if the increased traffic to the ECFS API was coming from specific IP addresses. The email was received at approximately 8:13am ET on Monday, May 8th, and the (b) (7) Services team responded at approximately 9am ET that same day.

- What information (logs or otherwise) did (b) (7) review related to the incident?

(b) (7) reviewed traffic reports and security monitoring reports via its (b) (7)(E) and analyzed (b) (7) server logs generated for traffic delivered through (b) (7) on May 7, 2017, 12:00am-11:59pm ET and May 8, 2017, 12:00am-11:59pm ET, for the www.fcc.gov and ecfsapi.fcc.gov hostnames. These internal (b) (7) logs contain http requests and responses, including [http header](#) details, to and from the designated websites. (b) (7) also used a network debugging tool to determine relevant IP information such as geographic and network locations associated with the IP addresses from which traffic was originated.

- Did (b) (7) prepare any formal or informal reports, documents, or briefings summarizing the incident response or the results of any analyses performed as part of the response? Please provide copies of those reports or documents.

(b) (7)(E) support services team generated an informal report of the log analysis results for traffic delivered via the ecfsapi.fcc.gov hostname. This report included the following information on traffic over the previous two days (May 7-8, 2017):

- the top 10 request IP addresses (client -> (b) (7) edge);
 - origin response codes (b) (7) edge -> FCC origin); and
 - (b) (7) (b) (7) formatted URLs sent to the FCC origin).
- If (b) (7) prepared any reports, documents, or briefings, were these reports, documents, or briefings provided to the FCC? If so, who received this material at the FCC and when was it provided?

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

The informal report described above was delivered via email to the FCC's designated primary technical point of contact, (b) (6). Two additional FCC staff members were copied on the email (b) (6).

On May 10, 2017 at 1459 hrs. EDT, (b) (6) sent the following email message to David Bray, FCC CIO.

I understand that (b) (6) (Account Executive supporting FCC) reached out to you yesterday.

If there is anything you need from us please let me know – my team is standing by.

We are prepared to give you / your team a “post event” briefing on the events that we saw from our vantage point and also additional insight on what can be done to mitigate such an event moving forward. Example- we have a traffic rate limiter that throttles the in-coming traffic that prevents server from being over loaded so site stays up.

Be more than happy to brief you on this and other capabilities. In fact, I would be more than happy to have FCC leverage the technology now (no cost trial) as you evaluate it.

- Did (b) (7) prepare a “post event” briefing? If so, did (b) (7) provide the briefing and what FCC staff attended and/or participated? Please provide a copy of the briefing. If not, why not?

No. While (b) (7) did offer to conduct a “post event brief”, one was never scheduled, so no documentation was created.

- Please describe what (b) (7) “saw from our vantage point.”

Based upon our analysis of the logs and information discussed above, (b) (7) saw a dramatic increase in the traffic levels delivered through (b) (7) during the event. FCC traffic (bytes) delivered increased by 3,116% over normally observed levels. Prior to May 7, 2017, average daily traffic was approximately 172 GB/day. Between May 7 and 8, 2017, the FCC site served approximately 4.5 TB (4,505 GB) of traffic.

The traffic observed appeared to be a mix of “human” and automated traffic. One item in particular is worth noting regarding the impact of the FCC's site design on traffic levels during high traffic events such as was experienced in the May 7th event. (b) (7)(E)

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

(b) (7)(E)

This is true even in the case of legitimate comment traffic. Specific examples of the traffic observed is provided in greater detail below.

- (b) (7)(E)

[Redacted]

- Example request patterns:

(b) (7)(E)

[Redacted]

(b) (7)(E)

[Redacted]

Note: Legitimate uses of the input form will generate requests of this form. Illegitimate uses of the form will likely not trigger these requests.

Note: This request format shows up in the public FCC API documentation for using the API with CURL: <https://www.fcc.gov/ecfs/public-api-docs.html> (b) (7)(E)

[Redacted]

- Approximately 8% of requests, between May 7, 2017 4pm ET and May 8, 2017 7pm ET, observed on ecfsapi.fcc.gov may have come from automated sources.

- Example IP and User Agent strings are below:

- IP: (b) (6)

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

- **User Agent:**
(b) (7)(E)
○ *Observation:* 65k repeat edge requests for mostly two URLs: (b) (7)(E). A blank referer header is present on each request.
- **IP:** (b) (6)
○ *User Agent:*
(b) (7)(E)
○ *Observation:* (b) (7)(C).
- **IP:** (b) (6)
○ *User Agent:*
(b) (7)(E)
○ *Observation:* (b) (7)(E). A blank referer header is present on each request.
- **IP:** (b) (6)
○ *User Agent:*
(b) (7)(E)
○ *Observation:* (b) (7)(E). A blank referer header is present on every request.
- **IP:** (b) (6)
○ *User Agent:* (b) (7)(E)
○ *Observation:* (b) (7)(E)

Case Number:
OIG-I-17-0011

Case Title:	ECFS DDoS
-------------	-----------

REPORT OF INVESTIGATION (continuation sheet)

(b) (7)(E)

- IP: (b) (7)(E)
 - User Agent: <N/A>
 - Observation: (b) (7)(E)

- IP: (b) (6)
 - User Agent: (b) (7)(E)
 - Observation: (b) (7)(E)

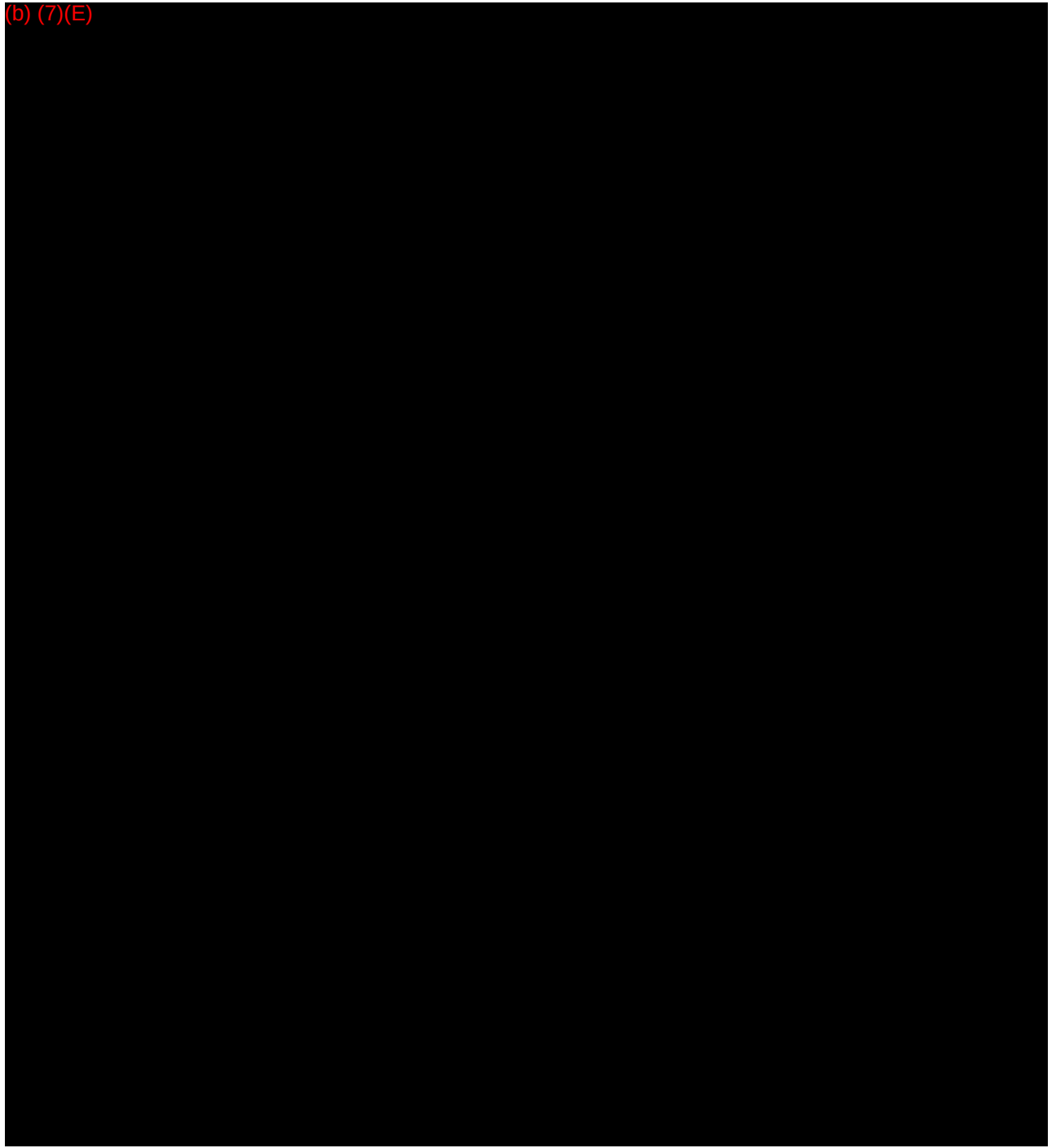
(b) (7)(E)

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS

REPORT OF INVESTIGATION (continuation sheet)

(b) (7)(E)



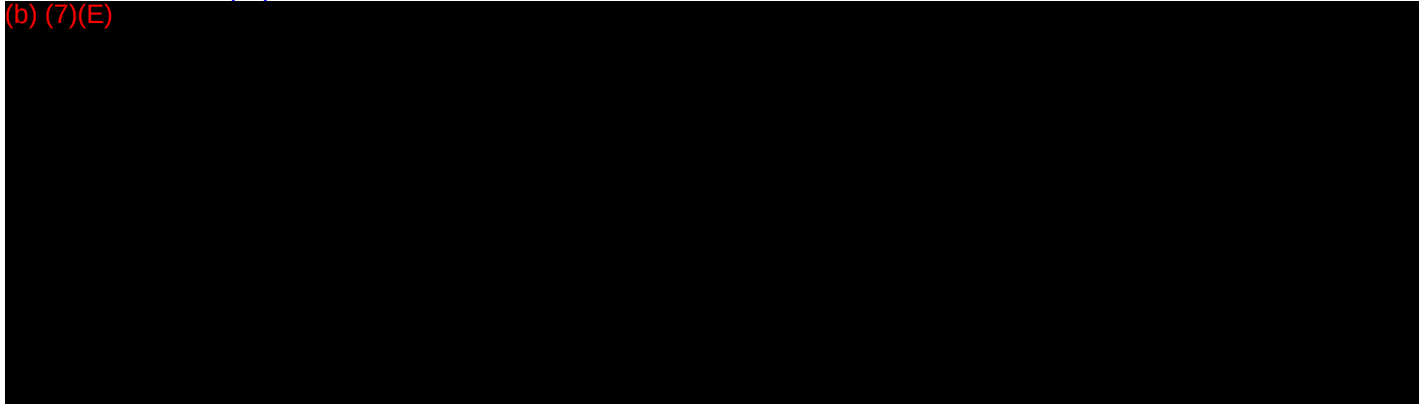
Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

References for recommendations to handle flash crowds and DDoS events:

White papers:

(b) (7)(E)



- Please describe how the “traffic rate limiter” would have prevented the ECFS from being overloaded.

In high traffic situations, (b) (7)(E) (these are referred to in (b) (7)(E)) would limit the rate at which requests are permitted to reach www.fcc.gov/ecfs or ecfsapi.fcc.gov based on a defined percentage of traffic threshold set by the FCC. This capability allows the FCC, when the overall traffic to the protected site(s) exceeds the established threshold, to redirect a percentage of users requesting the site to a “Please Wait” or “Maintenance” page for a set period of time thus reducing total simultaneous traffic to help prevent overload of the site. For example, the FCC could determine to redirect 50% of users to a Please Wait page for five minutes and the other 50% would be permitted to access the site.

- Why wasn’t the traffic rate limiter enabled for ECFS?

(b) (7)(E) were added to the FCC’s contract on a proof of concept basis (no cost evaluation) for the period April 26, 2017 to July 24, 2017 to permit the FCC to configure these features to respond to high traffic. (b) (7)(E) had enabled the (b) (7)(E) in (b) (7)(E) staging environment (used for testing), but did not receive FCC approval to enable in (b) (7)(E) production environment until May 8th. The (b) (7)(E) had not been enabled in either environment pending FCC approval to proceed with this work.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

Specific questions related to the (b) (7)(E) logs:

How does (b) (7)(E) capture and categorize traffic generated via redirect?

(b) (7)(E) uses the [HTTP referer field](#) to identify the address of the web page that linked to the resource being requested by the end user client. (b) (7)(E) logs an existing referer header for each HTTP request in the customer's (b) (7)(E) configuration (if the customer has configured the (b) (7)(E)).

(b) (7)(E) responds to and logs [HTTP response codes](#) for requests/responses delivered for hostnames delivered by (b) (7)(E). In HTTP, a redirection is triggered by the server by sending special responses to a request: redirects. HTTP redirects are responses with a status code of 3xx.

How can we differentiate between traffic generated from visits to gofccyourself.com or justtellmeifimrelatedtoanazi.com and other methods such as a direct traffic?

(b) (7)(E) uses the [HTTP referer field](#) to identify the address of the webpage that linked to the resource being requested. Note, however, that Referer Headers can be lost, removed, or spoofed (spoofing use cases include testing, security analysis and malicious tools). It is possible, therefore, that the web administrator for a linking site (e.g., gofccyourself.com) requested that browsers not send referer headers for links visited from their site.

How can we differentiate between an original and unique request or visits to the FCC Domain and any automatically generated requests, such as individual items in a webpage?

(b) (7)(E) uses the [HTTP User-Agent request header](#), which contains a characteristic string that allows identification of the application type, operating system, software vendor or software version of the requesting software user agent (e.g. browser). This can provide insight into the requesting operating system and browser (but note that some of the values can be spoofed by a sophisticated actor; other spoofing use cases include testing and security analysis).

How does (b) (7)(E) capture and categorize API traffic, whether it is originating from a foreign IP or is automatically generated as part of a query within the FCC ECFS?

(b) (7)(E) uses the Network layer IP address to identify the originating IP address of a client.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

(b) (7) creates an HTTP request header, called "True Client IP", with the value of the client's Network layer IP address. This header is added to HTTP requests from (b) (7) servers to the FCC web infrastructure. This network layer client IP is available in (b) (7)(E) (b) reports and logged in (b) (7)(E) logs (both (b) (7)(E) logs for customers and internal (b) (7) edge server logs) for each HTTP request. Additionally, the standard [HTTP X-Forwarded-For header](#) is available to identify the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer. However, the HTTP X-Forwarded-For header value can be spoofed. (b) (7) recommends referencing the True Client IP header.

How does (b) (7) handle incoming traffic differently depending on the originating foreign IP (e.g., cloud-hosted)?

(b) (7) has developed a highly configurable system that permits its customers to set controls for differentiated treatment of traffic based upon their specific policies and objectives. For example, customers may decide to restrict access based upon IP address, geographic origin, or other factors. Each customer has the opportunity to customize and tune their settings as they see fit.

How does (b) (7) capture and categorize incoming traffic from links in social media applications in mobile devices as compared to links in social media from mobile and desktop web browsers (e.g., the Twitter mobile application for iPhone or Android compared to Twitter via Chrome or Firefox on a mobile device or desktop)?

As noted above, (b) (7) uses the HTTP referer field to identify the address of a linking webpage and the HTTP User-Agent request header to identify the requesting application type, operating system, software vendor or software version. These fields will often allow categorization between mobile and desktop traffic.

In what instances would incoming traffic to the FCC domain not be captured within (b) (7) logs or handled via (b) (7)(E) infrastructure?

HTTP traffic that has not been designated by the customer for delivery by (b) (7) (i.e. the customer has not "CNAME'd" a hostname to (b) (7) via DNS records) would not be delivered via (b) (7) and therefore would not be captured within (b) (7)(E) logs. Additionally, any hostname that has been designated for delivery via (b) (7) but that has not yet been enabled by an associated (b) (7) configuration file would not be captured within

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

(b) (7) logs. (b) (7)(E)

these products are not in use by FCC.

With respect to certain types of DDoS attacks, (Network Layers 3 & 4) are automatically dropped and not logged. This is due to that fact that the (b) (7)(E) is architected as a reverse HTTP proxy and, therefore, only accepts traffic on ports 80 (HTTP) and 443 (HTTPS). This affects many DDoS attack traffic types including ICMP, SYN, ACK, RESET, and UDP floods, as well as UDP fragments.

Finally, customers may set up different routing via DNS for internal and external users. In these cases, internal users may be delivered directly to the customer's site infrastructure without using (b) (7) (E). In these case, such internal traffic would not be captured and logged by (b) (7) (E).

What are (b) (7)(E) processes and procedures in the event of an unanticipated exponential spike in incoming traffic?

As discussed above, (b) (7)(E) infrastructure is designed to be highly customer configurable so that the customer is able to set traffic controls based upon its own policies, resources, architecture, risk tolerance, and related factors and considerations. While the system is designed to provide automatic scalability and site optimization in order to support (and absorb) unanticipated large spikes in traffic, the customer is in the best position to decide and explain decisions made regarding specific settings to tune the services and address specific risks. (b) (7) (E) services do not mandate any set processes or procedures for dealing with such events as every customer has different requirements and needs. In the event of unanticipated traffic spikes, (b) (7)(E) services team responds to customer inquiries, answers questions and provides technical guidance on (b) (7) (E) configuration adjustments to implement in order to improve the user experience and/or offload traffic from the origin infrastructure.

What are (b) (7)(E) processes and procedures in the event of an unanticipated exponential spike in direct traffic to a webpage that does not typically receive requests from foreign IPs via direct link (i.e., no referrer)?

Please see the response to the prior question.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

During unanticipated spikes in traffic, how does (b) (7) (E) differentiate between a legitimate viral event and malicious activity?

As discussed above, (b) (7) (E) infrastructure provides automatic scalability on demand in order to support (and absorb) unanticipated large spikes in traffic (both legitimate and malicious). The (b) (7) (E) platform, in general, does not react differently to large spikes in traffic, as the dynamic mapping will continue to direct user requests for application content to an optimal (i.e. not subject to excessive load) (b) (7) (E) edge server. As a result, the spikes in traffic are spread and absorbed throughout the infrastructure. Customers, however, may customize settings to differentiate between traffic types based upon their needs.

In order to address events that could impact the (b) (7) (E) network on a large scale basis, (b) (7) (E) Network Operations Control Center (NOCC) and Security Operations Control Center (SOCC) continuously monitor the health of the platform and alerts will trigger if too many (b) (7) (E) servers (out of >240k) are under excessive load or some threshold of web application firewall rules are triggered. The NOCC/SOCC follows their internal (b) (7) (E) procedures to investigate, troubleshoot and react to such alerts. Given the scale of the platform, however, a traffic event such as FCC's would not have been sufficiently large to have triggered an (b) (7) (E) platform event.

In general, flash crowds and normal high traffic events do not behave the same as a DoS or DDoS attack. (b) (7) (E) has the ability to apply rate controlling technology on both an IP or session basis. Normal flash traffic is high volume traffic (but normal) from many different sources distributed across a fairly large geographical space. This normally won't trigger rate controls on an IP when configured correctly due in part to traffic spread and the fact that a single user's traffic should not be seen as a flood due to number of requests and volume. Caching on a per user basis also lowers the request volume, even for those people refreshing content quickly. For DDoS, they can operate in different ways, but what we will generally see is a quick high volume or large sustained volume of requests coming from a smaller number of requesters that are less geographically dispersed. Some DDoS attacks are low and slow which require other mitigations, but do not relate to this question and would not trigger the volumetric controls by themselves.

What are (b) (7) (E) processes and procedures in the event of malicious activity such as an HTTP flood attack?

(b) (7) (E) infrastructure is designed for automatic scalability such that unanticipated spikes,

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

including many forms of volumetric attacks (like an HTTP flood attack), are spread out to optimal edge servers resulting in many attacks simply being absorbed. Customers utilizing (b) (7)(E) benefit from this design when their content is cached onto (b) (7)(E) servers closer to the end user.

(b) (7)(E) Web Application Firewall, also used by the FCC, provides protection against DDoS and web application attacks. The service includes a collection of pre-defined configurable application-layer firewall protections or rule sets that can be automatically applied. (b) (7)(E) maintains these rules with regular updates for threat categories such as: protocol, request limit, and HTTP policy violations, malicious robots, generic and command injection attacks, Trojan backdoors, and outbound content leakage. These rules are collectively referred to as the (b) (7)(E). Customers will enable individual rules in either alert or deny mode, and configure them based on their defined thresholds. When triggered in deny mode, requests will be denied automatically at the (b) (7)(E) edge server. Additionally, (b) (7)(E) portal provides reporting and configurable alerting functionality used by the customer in monitoring and responding to attacks.

(b) (7)(E) also makes available support services to assist customers in mitigating and responding to attacks and events and to help customers optimize their service configurations.

As part of our investigation, we have interviewed the FCC contractor who obtained the logs from (b) (7)(E) (b) (7)(E)

- Were API logs created by (b) (7)(E) during this event?

(b) (7)(E) generates internal logs for all requests and responses for traffic delivered over (b) (7)(E) infrastructure. (b) (7)(E). Customers have access to logs for traffic for their own site(s) via (b) (7)(E) (b) (7)(E)

- (b) (7)(E)

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

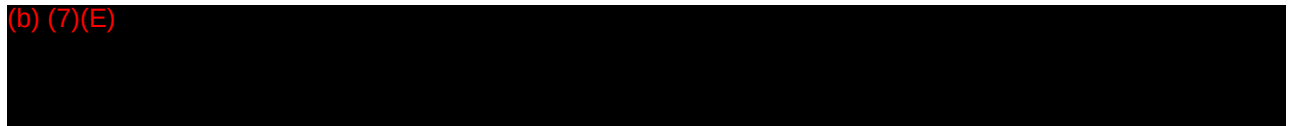
(b) (7)(E)



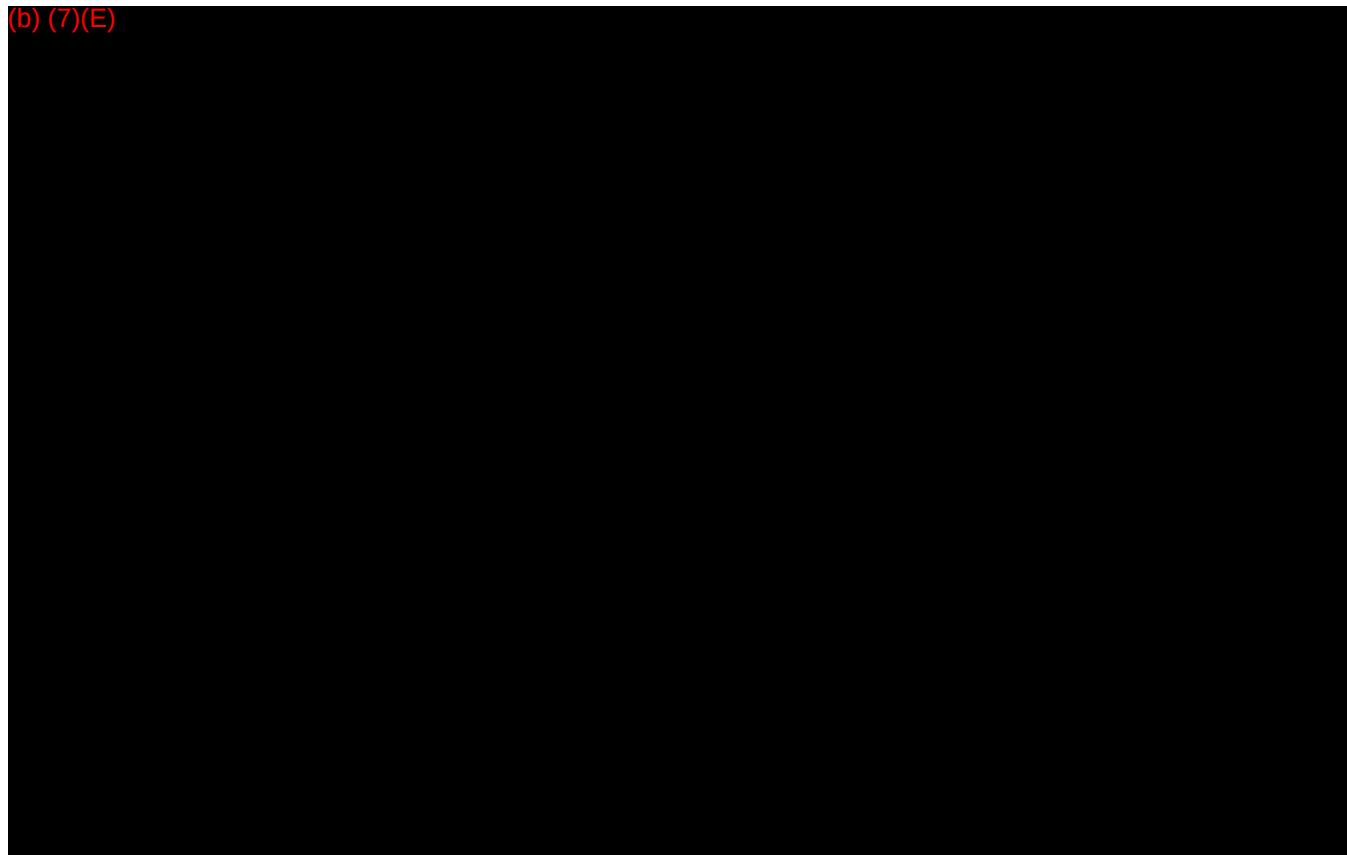
- What information was captured by these logs?

(b) (7)(E) log formats are in either W3C or Combined Log Format. The format is configurable when enabling (b) (7)(E) in the (b) (7)(E). Please refer to the (b) (7)(E) User Guide for details on log fields.

(b) (7)(E)



(b) (7)(E)



Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

The contractor was able not able to address (b) (7) caching during the event. Can you please provide a description of caching on the (b) (7) side during the event.

As noted above, the (b) (7) platform is designed to be highly configurable so that the customer may configure settings to meet its policies and requirements and to determine the best performance for its users. The decisions around caching configuration are numerous and can be complex, so the customer is in the best position to explain the choices made and configuration settings implemented. The relevant configuration files during the event may be accessed and reviewed via the FCC's (b) (7)(E) account (Accessible by FCC (b) (7)(E) admin(s)). The relevant files are as follows:

(b) (7)(E)

Follow-up questions provided to (b) (7) on December 12 2017 and responses from (b) (7) obtained on December 28, 2017 (responses provided in *italics*):

In (b) (7)(E) view and based on (b) (7)(E) assessment, was the incident on May 7th a “flash crowd” or multiple DDoS attacks as alleged by Dr. Bray in his press release on May 8th?

As noted in the previous responses, (b) (7) saw a combination of live and automated traffic. Based upon (b) (7)(E) review of the internal log files associated with the May 7th incident, (b) (7) believes that the majority of the traffic observed during the incident was a combination of “flash crowd” activity and increased traffic volume resulting from the site design issues discussed in the previous response.

As you are likely aware, the incident on May 7th coincided with a broadcast of the HBO program Last Week Tonight with John Oliver during which John Oliver discussed the FCC’s plan to repeal Net Neutrality. During the broadcast, Mr. Oliver provided two URLs registered by the program that were redirects to the ECFS page where comments for the net neutrality proceeding are filed ([https://www.fcc.gov/ecfs/search/proceedings?q=name:\(\(17-108\)\)\)](https://www.fcc.gov/ecfs/search/proceedings?q=name:((17-108))))). At 11:20pm EDT, the program tweeted one of the redirect URLs (gofccyourself.com). According to our analysis (and consistent with graphs obtained from the FCC) the spike in API activity that has been identified as the activity that affected ECFS availability started at 11:30pm EDT. During our investigation, we learned that the URL redirect provided by The Last Week Tonight with John

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

Oliver program would generate API activity (b) (7)(E) [REDACTED]. Would (b) (7) [REDACTED] characterize activity associated with this URL redirect as “flash crowd” activity?

Yes, to the extent that the observed high levels of traffic was generated by legitimate users (e.g. different comments, names, and posts), it would be considered “flash crowd” activity rather than DDoS attack traffic.

Did (b) (7) [REDACTED] perform an assessment to determine the extent to which this URL redirect impacted ECFS performance? If so, could you please provide the results of that assessment.

No. (b) (7) [REDACTED] was not asked to provide such an assessment. Rather we produced the informal report discussed previously. This report was the only assessment provided.

What were the customer thresholds previously designated by the Commission for traffic on www.fcc.gov and ecfsapi.fcc.gov?

(b) (7) [REDACTED] does not generally maintain a historical record of such thresholds set by customers. The current settings are as follows:

(b) (7)(E) [REDACTED]

These may have been changed by the customer admins during the time following the May 7th event.

Who at the FCC would have received the automated high traffic alerts that were sent at approximately 11:52pm ET on Sunday, May 7, 2017?

(b) (7) [REDACTED] does not generally maintain a historical record of such settings set by customers. The customer’s current configuration settings specify the following FCC email addresses for the receipt of alerts:

(b) (6) [REDACTED]

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

REPORT OF INVESTIGATION (continuation sheet)

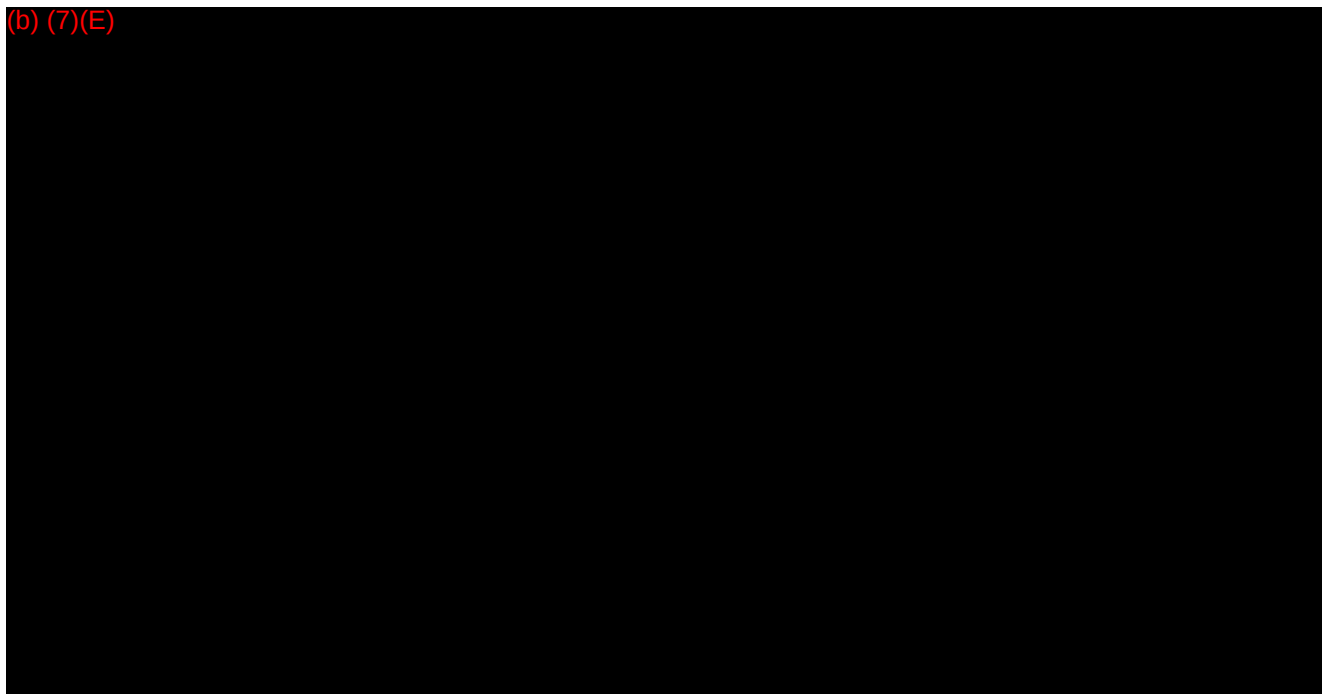
Can you please explain the difference between legitimate and illegitimate uses of the input form. How would we distinguish between a legitimate and illegitimate use of the form and why would illegitimate uses of the form not trigger these requests?

A "legitimate use" is one that uses a normal web browser as would be the case when a real user visits the site to submit comments. An "illegitimate use" refers to a flood of attack traffic to the form submission URL that bypasses the use of a normal browser.

How would ECFS system performance have been different if the (b) (7)(E) had been enabled in the production environment during the alleged DDoS event?

The (b) (7)(E) is designed to limit the rate at which requests are permitted to reach the targeted sites. (b) (7) cannot speak to the actual performance of the FCC sites, but the procedure would have been to set initial thresholds and then tune the cloudlet based upon actual traffic patterns when the customer or host determined the site to be under duress. Assuming that the tuning had been completed, the (b) (7) may have reduced simultaneous traffic levels to the sites.

(b) (7)(E)



Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------



Media Contact:

Mark Wigfield, (202) 418-0253
mark.wigfield@fcc.gov

For Immediate Release

**FCC CIO STATEMENT ON DISTRIBUTED DENIAL-OF-SERVICE
ATTACKS ON FCC ELECTRONIC COMMENT FILING SYSTEM**

WASHINGTON, May 8, 2017 – Federal Communications Commission Chief Information Officer Dr. David Bray issued the following statement today regarding the cause of delays experienced by consumers recently trying to file comments on the FCC’s Electronic Comment Filing System (ECFS):

“Beginning on Sunday night at midnight, our analysis reveals that the FCC was subject to multiple distributed denial-of-service attacks (DDoS). These were deliberate attempts by external actors to bombard the FCC’s comment system with a high amount of traffic to our commercial cloud host. These actors were not attempting to file comments themselves; rather they made it difficult for legitimate commenters to access and file with the FCC. While the comment system remained up and running the entire time, these DDoS events tied up the servers and prevented them from responding to people attempting to submit comments. We have worked with our commercial partners to address this situation and will continue to monitor developments going forward.”

###

Office of Media Relations: (202) 418-0500
ASL Videophone: (844) 432-2275
TTY: (888) 835-5322
Twitter: @FCC
www.fcc.gov/office-media-relations

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC, 515 F.2d 385 (D.C. Cir. 1974).

May 9, 2017

The Honorable Ajit Pai
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Chairman Pai:

According to your May 8 press release, you claim the Federal Communications Commission (FCC) has recently been the victim of “multiple distributed denial-of-service attacks (DDoS)”. DDoS attacks against federal agencies are serious—and doubly so if the attack may have prevented Americans from being able to weigh in on your proposal to roll back net neutrality protections.

As you know, it is critical to the rulemaking and regulatory process that the public be able to take part without unnecessary technical or administrative burdens. A denial-of-service attack against the FCC’s website can prevent the public from being able to contribute to this process and have their voices heard. Any potentially hostile cyber activities that prevent Americans from being able to participate in a fair and transparent process must be treated as a serious issue. As such, we ask you to keep Congress fully briefed as to your investigation. Please, by June 8, 2017 answer the following questions.

In the meantime, please make available alternative ways for the public to comment; for example, a dedicated email account on the net neutrality proceeding as was done in 2014.

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.
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?
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?

4. How many concurrent visitors is the FCC's website designed to be able to handle? Has the FCC performed stress testing of its own website to ensure that it can cope as intended? Has the FCC identified which elements of its website are performance bottlenecks that limit the number of maximum concurrent visitors? Has the FCC sought to mitigate these bottlenecks? If not, why not?
5. Did the DDoS attacks prevent the public from being able to submit comments through the FCC's 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?
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?
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?

Sincerely.



RON WYDEN
United States Senator



BRIAN SCHATZ
United States Senator



OFFICE OF
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

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,

A handwritten signature in blue ink, which appears to read "Ajit V. Pai", is positioned above the printed name.

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.

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

June 26, 2017

The Honorable Ajit V. Pai
Chairman
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

The Honorable Mignon L. Clyburn
Commissioner
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

The Honorable Michael O’Rielly
Commissioner
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

Dear Chairman Pai, Commissioner Clyburn, and Commissioner O’Rielly:

We write to express concerns about the Federal Communications Commission’s (FCC) cybersecurity preparedness, and the multiple reported problems with the FCC’s website in taking public comments in the net neutrality proceeding. Recent events have raised questions about the security of the FCC’s network, and we have serious concerns that the FCC’s website failures deprive the public of opportunities to comment on net neutrality – an issue that affects everyone who uses the internet.

Problems with the FCC’s net neutrality docket made headlines last month 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 “went down”¹ after the segment, noting that “the FCC’s servers appeared to be overwhelmed by the flood of traffic.”²

The following day, on May 8, 2017, the FCC’s Chief Information Officer announced that the FCC “was subject to multiple distributed denial-of-service attacks,” a situation that made it

¹ 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).

² Jeff John Roberts, *John Oliver Gets Fired Up Over Net Neutrality—and FCC’s Site Goes Down*, Fortune (May 8, 2017).

The Honorable Ajit V. Pai
The Honorable Mignon L. Clyburn
The Honorable Michael O'Rielly
June 26, 2017
Page 2

“difficult for legitimate commenters to access and file with the FCC.”³ In response to an inquiry from Senators Wyden and Schatz, the FCC recently released more information about the alleged cyberattacks.⁴ Yet the FCC’s response raises additional questions, and there are other areas of concern about the net neutrality docket for which we seek answers.

For example, recent reports have also indicated that as many as 150,000 comments had disappeared from the FCC’s net neutrality docket,⁵ and that automated comments were submitted to the FCC using names and addresses of real people without their knowledge or consent.⁶ Even with all of these problems and irregularities, the FCC has given only until the middle of August for the public to provide initial comments on the FCC’s net neutrality proposal, despite receiving calls to extend the deadline.⁷ Further, Republican Congressional leaders have not held hearings to examine these issues, despite receiving calls to do so.⁸

We ask you to examine these serious problems and irregularities that 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

³ Federal Communications Commission, *FCC CIO Statement on Distributed Denial-of-Service Attacks on FCC Electronic Comment Filing System* (May 8, 2017) (press release).

⁴ Letter from Ajit V. Pai, Chairman, Federal Communications Commission, to Senators Wyden and Schatz (June 15, 2017) (<https://www.politicopro.com/f/?id=0000015c-d59b-de74-a17f-ddbba4380001>) (FCC Response).

⁵ John Eggerton, *FCC’s Network Neutrality Docket Appears to Shrink*, Broadcasting & Cable (June 8, 2017).

⁶ Dominic Rushe, *‘Pretty ridiculous’: thousands of names stolen to attack net neutrality rules*, The Guardian (May 26, 2017).

⁷ Letter from Rep. Frank Pallone, Jr., Ranking Member, House Committee on Energy and Commerce, and Rep. Mike Doyle, Ranking Member, Subcommittee on Communications and Technology, House Committee on Energy and Commerce, to Ajit V. Pai, Chairman, Federal Communications Commission (May 11, 2017).

⁸ Letter from Rep. Frank Pallone, Jr., Ranking Member, House Committee on Energy and Commerce, Rep. Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce, Rep. Mike Doyle, Ranking Member, Subcommittee on Communications and Technology, House Committee on Energy and Commerce, and Yvette Clarke, Member of Congress, to Rep. Greg Walden, Chairman, House Committee on Energy and Commerce, Rep. Tim Murphy, Chairman, Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce, and Rep. Marsha Blackburn, Chairman, Subcommittee on Communications and Technology, House Committee on Energy and Commerce (May 17, 2017).

Procedure Act requirements to give the public notice and an opportunity to comment, as well as to respond to those comments.⁹ This is important, especially 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.¹⁰ This is especially important given that the FCC’s Chief Information Officer stated that the FCC experienced a cyberattack that made it difficult for members of the public to file comments with the agency in an open proceeding.¹¹ We therefore request responses to the following questions by July 17, 2017:

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.”¹² What “additional solutions” is the FCC pursuing to “further protect the system,” as was mentioned in the FCC’s response?¹³
2. According to the FCC, the alleged cyberattacks blocked “new human visitors.... from visiting the comment filing system.”¹⁴ 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.”¹⁵ What analysis did the FCC and the FBI conduct to determine that this was not a “major incident?”

⁹ 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.”).

¹⁰ 44 U.S.C. § 3554(a).

¹¹ FCC Press Release, *supra* n. 3.

¹² FCC Response, *supra* n. 4.

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

The Honorable Ajit V. Pai
The Honorable Mignon L. Clyburn
The Honorable Michael O'Rielly
June 26, 2017
Page 4

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?
4. Is the FCC making alternative ways available for members of the public to file comments in the net neutrality proceeding?
5. Did the FCC contact the National Cybersecurity and Communications Integration Center's Hunt and Incident Response Team (HIRT) at the U.S. Department of Homeland Security to investigate the May 8, 2017 incident, and if so, on which date(s) was such contact made? If the FCC did not contact HIRT to investigate the May 8, 2017 incident, please explain why it did not do so.
6. What were the findings from any forensic investigative analyses or reports concerning the May 8, 2017 incident, including how and why a denial-of-service attacks were declared, and from what attack vectors they came?
7. Did the FCC notify Congress of the May 8, 2017 incidents as provided by FISMA?¹⁶ If so, how did the FCC notify Congress? If not, why not?
8. Did the FCC notify its Office of Inspector General (OIG) of the May 8, 2017 incidents, and if so, when did it notify the OIG?

Your assistance in this matter is greatly appreciated, and we look forward to receiving a response. 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,



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



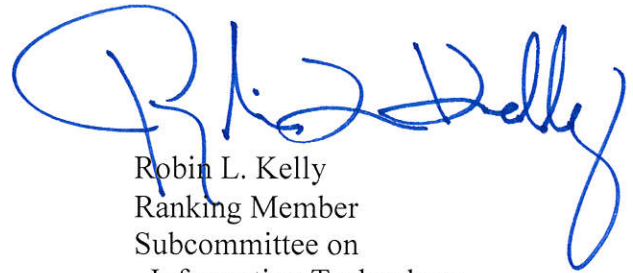
Elijah E. Cummings
Ranking Member
Committee on Oversight
and Government Reform

¹⁶ 44 U.S.C. § 3554(b)(7)(C)(iii)(III).

The Honorable Ajit V. Pai
The Honorable Mignon L. Clyburn
The Honorable Michael O'Rielly
June 26, 2017
Page 5



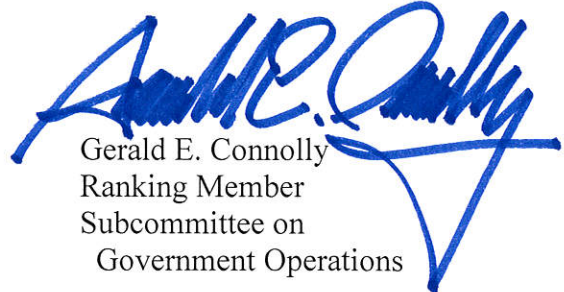
Diana DeGette
Ranking Member
Subcommittee on Oversight and
Investigations



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 Trey Gowdy, Chairman
House Committee on Oversight and Government Reform

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

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

July 21, 2017

OFFICE OF
THE CHAIRMAN

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 Pai

Enclosure

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.

United States Senate
WASHINGTON, DC 20510

June 11, 2018

The Honorable Ajit Pai
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Chairman Pai:

On May 9, 2017, we sent you a letter regarding alleged cyberattacks on the Federal Communication Commission's Electronic Comment Filing System during that month. There was also an ECFS issue involving the net neutrality proceeding in 2014. In our letter we asked that you keep Congress fully briefed as to your investigation.

Beyond your initial internal analyses that you reference in your June 15, 2017, response, have any subsequent FCC or third-party (e.g., vendor, contractor, or government agency) analyses or investigations verified that a cyberattack on ECFS occurred in 2017 and, if so, that the attack is best classified as a DDoS attack? If not, why was no investigation conducted? Please provide any and all reports, findings, and other relevant details of any such investigations.

In response to our May 2017 letter you provided information to us about the 2017 event. We request that you update, revise, and/or reaffirm in their entirety the responses that you previously provided. In addition, clarify whether you continue to classify the May 7-8, 2017, event as a DDoS attack and the basis for your classification.

Does the FCC classify the 2014 event as a DDoS attack or attacks? If so, please describe the nature of the attack and the basis for classifying it as a DDoS attack.

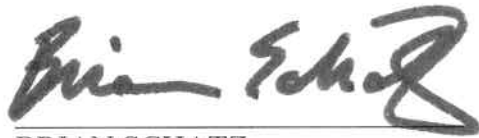
Have any FCC or third-party (e.g., vendor, contractor, or government agency) analyses or investigations concluded that a cyberattack occurred in 2014? Please provide any and all reports, findings, and other relevant details of any such investigations.

Is the FCC fully cooperating with the Government Accountability Office review and evaluation of the FCC's ECFS security and vulnerability to attack, including full access to the FCC's accounts and data from any incidents as well as cooperation from relevant current and former FCC staff?

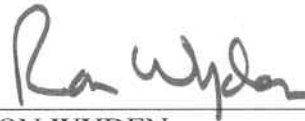
Please answer these questions in writing by June 27, 2018. If you need to withhold any responsive information because it is confidential or classified please contact Andy Heiman and

Eric Einhorn in our offices to schedule a briefing or make other appropriate arrangements regarding that information.

Sincerely,

A handwritten signature in dark ink, appearing to read "Brian Schatz", written over a horizontal line.

BRIAN SCHATZ
United States Senator

A handwritten signature in dark ink, appearing to read "Ron Wyden", written over a horizontal line.

RON WYDEN
United States Senator



Federal Communications Commission
Office of Inspector General

Memorandum of Interview

Type of Activity: ☐ Personal Interview ☒ Telephone Interview ☐ Other	Interview Date and Time: November 1, 2017, 12:30 p.m.
Interview of: (b) (6)	Location of Interview: Telephone Interview
Report Date: November 1, 2017	Conducted By: (b) (7)(C), FCC OIG

Subject Matter/Remarks

On May 8, 2017, the FCC issued a press release containing a statement from Dr. David BRAY, FCC's Chief Information Officer, regarding the cause of delays experienced by consumers "recently trying to file comments on the FCC's Electronic Comment Filing System (ECFS)." In that statement, BRAY reported that these were "deliberate attempts by external actors to bombard the FCC's comment system, and the external actors were "not attempting to file comments themselves; rather they made it difficult for legitimate commenters to access and file with the FCC." Immediately before the multiple DDoS attacks alleged by BRAY started, the HBO program "Last Week Tonight with John Oliver" aired a segment in which the host John OLIVER discussed the Commission's Net Neutrality proceeding and encouraged viewers to visit the Commission's ECFS and file comments about that proceeding. OLIVER also provided two (2) URLs registered by the program (gofccyourself.com and justtellmeifimrelatedtoanazi.com) that were actually redirects (i.e., they provided access to the web page within ECFS where comments about that filing can be made). The program also sent out a link on twitter at 11:29pm EDT that included the link gofccyourself.com. ECFS logs appear to show that the activity attributed to multiple DDoS attacks started at 11:30pm EDT.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

On November 1, 2017, Federal Communications Commission (FCC) Office of Inspector General (OIG) (b) (7)(C) participated in a telephone interview with (b) (6), DHS/NCCIC/US-CERT. The purpose of the interview was to obtain an understanding of the US-CERT Federal Incident Reporting Guidelines. Prior to the interview, (b) (7)(C) prepared an outline of the ECFS DDoS incident, the Commission's stated reasons for not reporting the incident, and US-CERT guidelines for incident reporting. A copy of this outline is attached to this Memorandum of Interview.

(b) (7)(C) began the interview by briefly describing the ECFS DDoS incident and the Commission's press release describing the incident as "multiple distributed denial-of-service attacks (DDoS)" and stating that "(t)hese were deliberate attempts by external actors to bombard the FCC's comment system with a high amount of traffic¹." (b) (7)(C) also indicated that the Commission determined that the "multiple distributed denial-of-service attacks (DDoS)" did not warrant reporting to US-CERT and provided the basis for this determination (included in the outline attached to this MOI).

(b) (7)(C) indicated that the Commission has quoted Federal Incident Reporting Guidelines that appear to have expired and provided the quoted sections of the guidelines. (b) (6) confirmed that the guidelines quoted by Leo WONG, FCC Chief Information Security Office (CISO), in an email message on October 2, 2017, have expired. (b) (6) stated that new guidelines were effective as of April 1, 2017.

In the October 2, 2017 email message, WONG quoted the following definition of the Denial of Service (DoS):

"An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS" and indicates that the reporting timeframe is "(w)ithin two (2) hours of discovery/detection **if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.**"

(b) (7)(C) explained that the Commission was able to mitigate the activity fairly quickly after it was discovered by adding more instances of API servers in the cloud environment hosting ECFS. (b) (6) stated the current Federal Incident Reporting Guidelines no longer include this language and no longer limit reporting DDoS attacks to ongoing attacks in which the agency has been unable to successfully mitigate activity (i.e., all DDoS attacks meeting the definition

¹ "Beginning on Sunday night at midnight, our analysis reveals that the FCC was subject to multiple distributed denial-of-service attacks (DDoS). These were deliberate attempts by external actors to bombard the FCC's comment system with a high amount of traffic to our commercial cloud host. These actors were not attempting to file comments themselves; rather they made it difficult for legitimate commenters to access and file with the FCC. While the comment system remained up and running the entire time, these DDoS events tied up the servers and prevented them from responding to people attempting to submit comments. We have worked with our commercial partners to address this situation and will continue to monitor developments going forward."

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

provided in the Federal Incident Reporting Guidelines effective April 1, 2017 should be reported).

(b) (7)(C) explained that the Commission offered additional mitigating factors (e.g., sessions were coming from legitimate IP addresses, no attempt to breach, no harm to systems or individuals, not a mission critical system, outside of business hours, etc.). (b) (6) explained that agencies are provided some leeway in defining an incident in their environment (i.e., what loss of integrity, confidentiality, or availability mean in the unique environment of an agency). (b) (6) stated that these considerations would be governed by the agencies internal policy for defining an incident. (b) (7)(E) asked if the ECFS DDoS incident meets the current definition of an incident in the US-CERT Federal Incident Reporting Guidelines and if the incident should have been reported. (b) (6) stated that it does meet the definition of an incident in the Federal Incident Reporting Guidelines effective April 1, 2017 and should have been reported to US-CERT.

(b) (7)(C) explained that the ECFS DDoS attacks have been characterized as unusual Layer 7 (application layer) attacks similar to the distributed denial-of-service attack against Pokémon Go in July 2016². (b) (6) indicated US-CERT would have been interested in obtaining information about this incident particularly given its unusual nature. US-CERT would also have been able to use resources available to US-CERT to “take a closer look at this incident.” US-CERT would also have been able to share information about this incident with other Government organizations and to determine if there have been other, similar attacks. (b) (6) stated it would probably not be useful now for US-CERT to look into the incident because so much time has passed.

(b) (7)(C) asked if there are consequences for an agency if they fail to report security incidents. (b) (6) stated that US-CERT does not have an enforcement mechanism but the matter might be of interest to the Office of Management and Budget (OMB).

(b) (6) indicated US-CERT would be happy to discuss this matter further if there are additional questions and that the best way to contact US-CERT is soc@us-cert.gov.

The interview ended at approximately 12:50 p.m.

² From Ars Technica article published on May 23, 2017 with the title “Examining the FCC claim that DDoS attacks hit net neutrality comment system.”

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------



Federal Communications Commission
Office of Inspector General

Memorandum of Interview

Type of Activity: ☒ Personal Interview ☐ Telephone Interview ☐ Other	Interview Date and Time: November 7, 2017, 1:00 p.m.
Interview of: (b) (6)	Location of Interview: FCC Headquarters 445 12 th Street, S.W. (b) (6)
Report Date: November 7, 2017	Conducted By: (b) (7)(C)

Subject Matter/Remarks

On May 8, 2017, the FCC issued a press release containing a statement from Dr. David BRAY, FCC's Chief Information Officer, regarding the "cause of delays experienced by consumers recently trying to file comments on the FCC's Electronic Comment Filing System (ECFS)." In that statement, BRAY reported that the FCC was "subject to multiple distributed denial-of-service attacks (DDoS)" and that these were "deliberate attempts by external actors to bombard the FCC's comment system, and the external actors were "not attempting to file comments themselves; rather they made it difficult for legitimate commenters to access and file with the FCC." Immediately before the multiple DDoS attacks alleged by BRAY started, the Home Box Office (HBO) program "Last Week Tonight with John Oliver" aired a segment in which the host John OLIVER discussed the Commission's Net Neutrality proceeding and encouraged viewers to visit the Commission's ECFS and file comments about that proceeding. OLIVER also provided two (2) URLs registered by the program (gofccyourself.com and justtellingmeifimrelatedtoanazi.com) that were actually redirects (i.e., they provided access to the web page within ECFS where comments about that filing can be made). The program also sent out a link on twitter at 11:29pm EDT that included the link gofccyourself.com. ECFS logs appear to show that the activity attributed to multiple DDoS attacks started at 11:30pm EDT.

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS

MEMORANDUM OF INTERVIEW (continuation sheet)

On November 7, 2017, Federal Communications Commission (FCC or “Commission”) Office of Inspector General (OIG) Agents (b) (7)(C) conducted an interview with (b) (6) regarding allegations that multiple distributed denial-of-service (DDoS) attacks were directed at the Commission’s Electronic Comments Filing System (ECFS) on the evening of May 7, 2017. (b) (7)(C) is the author of this report and (b) (7) contributed to this report. Prior to the interview, (b) (7)(C) prepared an interview outline. A copy of that outline is attached to this Memorandum of Interview.

(b) (7)(C) began the interview by briefly describing the OIG investigation of the ECFS DDoS incident and the Commission’s press release describing the incident as “multiple distributed denial-of-service attacks” and stating that “(t)hese were deliberate attempts by external actors to bombard the FCC’s comment system with a high amount of traffic¹.” (b) (7)(C) explained that the purpose of the interview was to obtain background information, discuss (b) (6) involvement in responding to the ECFS DDoS incident, and discuss specific issues with the (b) (7) logs and other logs that were provided to OIG related to the incident².

(b) (6) is an employee with (b) (6) has been the contractor providing engineering support to ITC for approximately (b) (6). Prior to (b) (6) receiving the contract, (b) (6) was the contractor providing engineering support and (b) (6) was an employee of (b) (6) worked for (b) (6) at the time of the ECFS DDoS incident. (b) (6) is the Contracting Officer’s Representative on the (b) (6) contract. [NOTE: (b) (6) works in the (b) (6) team within the Commission’s Information Technology Center (ITC).]

(b) (6) has worked at the Commission “on and off” since (b) (6). When (b) (6) started at the Commission, he worked on the (b) (6). (b) (6) has been back at the Commission for approximately (b) (6).

(b) (6) works on the engineering team and provides solutions for the FCC engineering team (b) (6) duty station is 445 12th Street, S.W., Room (b) (6), Washington, DC 20554. (b) (6) supervisor is (b) (6) contract and his supervisor was (b) (6).

¹ On May 8, 2017, the FCC Issued a Press Release with the title “FCC CIO STATEMENT ON DSITRIBUTED DENIAL-OR-SERVICE ATTACKS ON FCC ELECTRONIC COMMENT FILING SYSTEM” and including the following statement: “Beginning on Sunday night at midnight, our analysis reveals that the FCC was subject to multiple distributed denial-of-service attacks (DDoS). These were deliberate attempts by external actors to bombard the FCC’s comment system with a high amount of traffic to our commercial cloud host. These actors were not attempting to file comments themselves; rather they made it difficult for legitimate commenters to access and file with the FCC. While the comment system remained up and running the entire time, these DDoS events tied up the servers and prevented them from responding to people attempting to submit comments. We have worked with our commercial partners to address this situation and will continue to monitor developments going forward.”

² ITC has provided (b) (7)(E)

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS

MEMORANDUM OF INTERVIEW (continuation sheet)

(b) (7)(C) asked (b) (6) to describe his duties and responsibilities as they relate to ECFS and as they related to the alleged DDOS attacks on May 7th. (b) (6) is responsible for setting up, maintaining, and daily operation of ECFS on the infrastructure side (as opposed to the operations side).

(b) (6) became involved in responding to the alleged DDoS attacks on the morning of Monday, May 8th, when (b) (6) received an alert that the “system was not working.” (b) (6) determined that the “API logs” showed a large number of API³ requests. The latency⁴ issue was addressed by adding more instances of the API server (from four (4) instances to twenty (20) instances). It took approximately one (1) hour or so to “ramp up” the response and address the latency issue. The Commission was able to “ramp up” additional API servers without involving (b) (7)(E) and (b) (6) does not recall speaking with representatives from (b) (6). (b) (6) does recall speaking with representatives from (b) (7)(E) who also reported seeing heavy API activity.

(b) (7)(C) asked if the URL redirect created by the Last Week Tonight with John Oliver program ([https://www.fcc.gov/ecfs/search/proceedings?q=name:\(\(17-108\)\)](https://www.fcc.gov/ecfs/search/proceedings?q=name:((17-108)))) resulting from the gofccyourself.com or justtellmeifimrelatedtoanazi.com URLs registered by the program), would have generated API activity. (b) (6) indicated they would have generated API activity. (b) (7) and (b) (6) discussed the level of API that would have resulted from the redirect. (b) (6) indicated (b) (6) does not know the level of activity) and where in the logs that activity would be identified ((b) (7) logs and (b) (7)(E) logs). (b) (6) is not aware of any log analysis by the Commission related to the alleged DDoS attacks. (b) (6) was involved in ensuring that the logs were saved, but not in any analysis.

(b) (7)(C) provided an email message dated June 9, 2017 at 0917 hrs. EDT from (b) (6) to Tony SUMMERLIN (contractor) with the Subject Line “ECFS API starts before May 7th” (email is attached). This email message is as follows:

³ An Application Programming Interface (API) is a set of subroutine definitions, protocols, and tools for building application software. In general terms, it is a set of clearly defined methods of communication between various software components. Within ECFS, the API is allows automated programs to submit or search for comments in an automated fashion.

⁴ Response Time vs. Latency - Response time is the total time it takes from when a user makes a request until they receive a response. Response time can be affected by changes to the processing time of your system and by changes in latency, which occur due to changes in hardware resources or utilization. In this case, a change in the utilization of system resources as a result of the number of API calls increased latency and increased user response time.

⁵ (b) (7)(E) is the cloud provider that hosts ECFS.

⁶ (b) (7)(E) is an FCC contractor that provides cloud computing services including services to prevent DDoS attacks.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

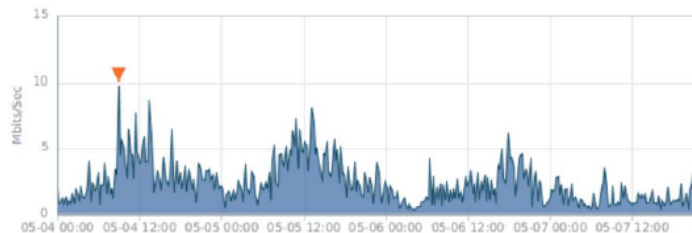
From: (b) (6)
Sent: 6/9/2017 9:17:44 AM -0400
To: "Tony Summerlin (CTR)" <Tony.Summerlin@fcc.gov>
CC: (b) (6)
Subject: ECFS API starts before May 7th

Tony,

Following graph shows hits/sec for ecfs api from May 4th to the 13th. The numbers before May 7th 11:30 PM are not visible because of the scale. There were 5 hits/sec vs 150 hits/sec starting 11:30 PM on May 7th.



Following graph shows hits/sec for ecf sapi from May 4th to May 7th . Steady load at 5 hits/sec



Thanks

(b) (6)

(b) (6) confirmed that (b) (6) sent this email and that the information in the email message is accurate. (b) (7)(C) provided an email message dated June 9, 2017 at 1026 hrs. EDT from David BRAY, Chief Information Officer (CIO), to SUMMERLIN (contractor) and Mark STEPHENS, Managing Director, with the Subject Line "Re: Re: ECFS API starts before May 7th" (email is attached). This email message is as follows:

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS

MEMORANDUM OF INTERVIEW (continuation sheet)

From: David Bray <David.Bray@fcc.gov>
Sent: 6/9/2017 10:26:30 AM -0400
To: "Tony Summerlin (CTR)" <Tony.Summerlin@fcc.gov>; Mark Stephens <Mark.Stephens@fcc.gov>
Subject: Re: Re: ECFS API starts before May 7th

Many thanks Tony -- there was a different chart that made it look like the hits started before 1130pm (possibly before 11pm) which if so is interesting because that means they started before the John Oliver clip perhaps in anticipation of it?

Also can we get clarity from (b) what they mean by hits. Hits = establishing a session once or multiple sessions?

Thank you.

(b) (7)(C) asked if there is a "different chart that made it look like the hits started before 1130pm (possibly before 11pm)." (b) (7)(C) is not aware of any such chart.

(b) (7)(C) provided (b) (6) a copy of the Commission's response to Question #1 in its letter to Senator Wyden, dated June 15th and asked if the response accurately reflects (b) (6) perspective on the alleged DDoS attacks and the Commission's understanding of the events. (b) (6) involvement was limited to "the level of activity only" (i.e., that section of the response identifying the level of API activity) and not to the conclusions reached about the cause for that level of activity. (b) (6) reiterated that (b) (6) is not aware of any subsequent log analysis to confirm the conclusions reached in the response to Senator Wyden.

(b) (6) indicated that the [https://www.fcc.gov/ecfs/search/proceedings?q=name:\(\(17-108\)\)](https://www.fcc.gov/ecfs/search/proceedings?q=name:((17-108))) URL would make an API call (i.e., request for information or resources) and that it would generate "numerous" API calls. (b) (7) indicated that (b) (6) has estimated the number of API calls generated by the URL to be (b) (7)(E) API calls but (b) (6) was not able to confirm that number. [NOTE: OIG will contact ITC to obtain this information.]

(b) (6) indicated the level of API activity on the FCC side would be dependent on the level of (b) (7)(C) caching. (b) (7)(E)
(b) (7)(E)
(b) (7)(E)

(b) (7) asked where user-generated API traffic would be identified in the logs that were provided. (b) (6) indicated that this information would be located in the (b) (7)(E) (b) (7) asked about the format of the (b) (7) logs and the location of foreign IP addresses in the logs. (b) (6) indicated that (b) (7) adds its own IP address to the (b) (7) and that we will need make sure that selected IP addresses are not (b) (7) IP (b) (7)(F) addresses.

The interview ended at approximately 2:00 p.m.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS
-------------------------------	--------------------------

OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE INFORMATION
FCC Office of Inspector General
Page 5 of 5



Federal Communications Commission
Office of Inspector General

Memorandum of Interview

Type of Activity: ☐ Personal Interview ☒ Telephone Interview ☐ Other	Interview Date and Time: February 8, 2018 9:00 AM
Interview of: Special Agent (SA) (b) (6) Federal Bureau of Investigation (b) (6)	Location of Interview: Telephone Interview
Report Date: February 8, 2018	Conducted By: (b) (7)(C), FCC OIG (b) (7)(C), FCC OIG

Subject Matter/Remarks

On February 8, 2018, Federal Communications Commission (FCC) Office of Inspector General (OIG) (b) (7)(C) conducted a telephone interview of FBI SA (b) (6) as part of an investigation into alleged false statements made in conjunction with a claimed distributed denial of service (DDoS) attack that allegedly occurred at the FCC on May 7-8, 2017.

Background

(b) (6) is currently a Special Agent with the FBI in the (b) (6). At the time of the events relevant to this investigation, (b) (6) was a special agent at the FBI Washington Field Office working on a squad focusing on criminal cyber matters.

(b) (6) first found out about the alleged DDoS attack on May 9th or 10th, when (b) (6) supervisors at FBI headquarters requested (b) (6) contact the FCC in response to information they obtained from media reports that a DDoS attack occurred at the FCC.

(b) (6) was involved with the Washington Field Office Cyber Task Force, an FBI group that includes OIG agents from numerous agencies. From (b) (6) experience working with this group, (b) (6) understood that OIGs routinely are called upon by their agencies to investigate potentially criminal cyber matters. In some of these cases, the task force would often be called upon to assist as a "force multiplier," effectively conducting a cooperative investigation with the OIG. (b) (6) assumed the FCC OIG would investigate the alleged DDoS attack in a manner similar to other agencies. Thus, (b) (6) called Jay Keithley (Keithley), FCC AIGI, to offer FBI assistance in the event the OIG needed it. Keithley said he would refer the matter to (b) (7)(C), who was out of the

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS Attack

MEMORANDUM OF INTERVIEW (continuation sheet)

office on training for the remainder of the week. Keithley also suggested (b) (6) contact Leo Wong (Wong), FCC Chief Information Security Officer.

False Statements

Investigators referred (b) (6) to an email FCC OIG previously sent to (b) (6) for (b) (6) review. The email is correspondence from Wong to his superiors at the FCC recalling a conversation Wong had with (b) (6) on May 10, 2017, to discuss the DDoS attack. (b) (6) generally confirmed the accuracy of the parts of the email that referred to the conversation. (b) (6) repeated to investigators that (b) (6) indicated to Wong that (b) (6) understood (b) (7) would be taking the lead in looking into the matter, but that (b) (6) and the FBI could provide assistance to Wong if he needed it. Referring to contemporaneous notes taken during the telephone call with Wong, (b) (6) recalled Wong stating he had not yet “done a deep dive,” into the logs. He did note there were many comments from IP addresses emanating from an (b) (7)(E) server that slowed down the system.¹ According to (b) (6), these comments from (b) (7)(E) server could either have been simple benign mass comments or a criminal bot. Based on the conversation with Wong, it was clear the FCC did not at that time know what had happened. Wong had no idea whether the comments were benign or potentially criminal. Wong kept making the distinction that the system never went down, it just slowed. When asked to confirm the attack, Wong repeated that the FCC had not done a deep dive. Wong said the FCC did not report the attack because it was not major.

In assessing a DDoS attack, (b) (6) does not care if a system slowed down or crashed. An attack can exist in the absence of either, especially in the absence of a complete crash. Because Wong kept referring to slow downs, and because he had not considered the log data, (b) (6) concluded the FCC could not have known with any certainty it was attacked.

(b) (7) referred (b) (6) to a letter dated June 15, 2017, from the FCC to Senators Schatz and Wyden, responding to questions concerning the DDoS attack. Investigators referred (b) (6) to the following language from the letter:

The FCC consulted with the FBI following the 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 that the May 7-8 disruption was not a system “hack” or intrusion and at no point was the Commission’s network cybersecurity breached.

(b) (6) did not confirm the accuracy of the quote. The only conversation (b) (6) had with Wong, or with anyone outside of the OIG at the FCC, was the May 10th phone call, described above. To (b) (6) knowledge there were no other FBI contacts with the FCC in this regard. “From a criminal standpoint,” (b) (6) does not consider cyber matters in terms of “major” or not. This distinction is meaningless and (b) (6) would not have agreed to anything in these terms.

¹ Investigator note: “System” refers to the FCC’s Electronic Comment Filing System (ECFS).

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attack
-------------------------------	---------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

(b) (7) then referred (b) (6) to a letter dated July 21, 2017, from the FCC to the House of Representatives (July 21st letter). Investigators referred (b) (6) specifically to the following language from the letter:

The FCC consulted with the FBI following the 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 that the May 7-8 disruption was not a system “hack” or intrusion and at no point was the Commission’s network cybersecurity breached.

(b) (6) did not confirm the accuracy of the quote. (b) (6) again reiterated that “all that matters is was a crime committed or not.” (b) (6) does not consider cyber incidents in terms of “significant” or not. Regardless, (b) (6) did not have enough information to reach any conclusion, especially since (b) (6) did not have any information regarding what was in the logs, and thus would not have opined on criminality. (b) (6) never discussed Presidential Policy Directive-41 at any time with Wong, and until OIG investigators forwarded (b) (6) the July 21st letter, (b) (6) was not familiar with Presidential Policy Directive-41.

Related Information

(b) (7) referred (b) (6) to a red-line draft of the July 21st letter OIG obtained in the course of its investigation. (b) (6) was referred to the following specific language in response to the question of what analysis did the FCC and FBI conduct to determine whether this was a “major incident.”

The impacted agency is ultimately responsible for determining if an incident should be designated as major and may consult with US-CERT to make this determination. The CISO in consultation with the FBI determined these criteria were not achieved.

Commented [Leo Wong1]: Sounds like the decision was made jointly which really wasn’t the case. Can we say “Decision was confirmed later with FBI that the threshold for major incident was indeed not met and no US-CERT incident was necessary.”

(b) (6) maintains both the language in the draft statement and the suggested language in Wong’s comment would have been inaccurate. In (b) (6) only conversation with Wong on May 10th, (b) (6) did not discuss criteria, and certainly did not agreed that they were not met. Neither did (b) (6) confirm that a threshold for a major incident was not met, confirming again that quantifying an incident is not a relevant determination.

Conclusion

In order for (b) (6) to have reached a determination of whether or not the DDoS attack occurred, or even to have opined on it, much work would have had to have been completed first, including a thorough analysis of the logs.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attack
-------------------------------	---------------------------------



Federal Communications Commission
Office of Inspector General

Memorandum of Interview

Type of Activity: ☒ Personal Interview ☐ Telephone Interview ☐ Other	Interview Date and Time: February 05, 2018 10:58 am - 12:07 pm
Interview of: (b) (6) Office of Managing Director (OMD), Information Technology Center (ITC)	Location of Interview: FCC Headquarters 445 12 th Street, S.W. Washington, DC (b) (7)(C)
Report Date: February 15, 2018	Conducted By: (b) (7)(C) (b) (7)(C) (b) (7)(C)

Subject Matter/Remarks

On February 05, 2018, Federal Communications Commission (FCC) Office of Inspector General (OIG) Agents (b) (7)(C) interviewed (b) (6) in furtherance of an investigation into alleged false statements made in conjunction with a claimed distributed denial of service (DDoS) attack that allegedly occurred at the FCC on May 7-8, 2017.

Agents (b) (7)(C) are the authors of this report.

(b) (7)(C) presented credentials to (b) (6) at the beginning of the interview. (b) (7)(C) started the interview by explaining that the focus of the investigation was initially centered on the allegations of multiple DDoS attacks alleged by FCC Chief Information Officer (CIO) David Bray in a May 8th FCC press release, but has now shifted into an investigation of false statements made by Bray, Tony Summerlin, and Leo Wong in responses to congressional inquiries. (b) (7)(C) explained that the matter was formally referred to DOJ in December and that, although DOJ has not made a decision about opening a case, DOJ is advising OIG as it proceeds with conducting interviews into the matter. (b) (7)(C) explained the Kalkines warning and provided a copy of the Kalkines warning form to (b) (6). (b) (7)(C) requested that (b) (7)(C) read through and sign the form acknowledging that the warning had

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

been provided and explained to (b) (6). (b) (6) had no questions and signed the form after reviewing it. A signed copy of the Kalkines warning is attached to this MOI as Exhibit F.

BACKGROUND OF (b) (6)

In response to questioning, (b) (6) voluntarily provided the following information:

(b) (6) personal and contact information is:

(b) (6)

(b) (6) title is (b) (6). (b) (6) has been a full time employee of the FCC since (b) (6). Previously, (b) (6) had worked as (b) (6). His current supervisor, since about December 2017, is (b) (6). Prior to this, (b) (6) reported to Christine Calvosa, the FCC's Deputy CIO for Technology and Resiliency.

INFORMATION PROVIDED BY (b) (6)

In response to questioning, (b) (6) voluntarily provided the following information:

(b) (6) stated that (b) (6) role regarding the Electronic Comment Filing System (ECFS) management was that of a subject matter expert (SME). Prior to the opening of the net neutrality proceeding, (b) (6) office reviewed the events that occurred during the previous net neutrality proceeding in 2014 and attempted to scale and optimize ECFS accordingly. (b) (6) further explained that, although these discussions took place long before the incident on May 7 and 8, 2017 that disrupted ECFS's performance (the "May 7th Incident"), ECFS is a "finicky beast" and that any system improvement will likely expose further issues.

When asked whether (b) (6) office had any prior knowledge of the segment in the HBO series Last Week With John Oliver (JO) centered on net neutrality, scheduled to air on May 7, 2017, specifically after producers from the show reached out to both the Office of Media Relations (OMR) and the Chairman's office, (b) (6) replied that neither (b) (6) nor anyone from (b) (6) team knew.

(b) (7)(E)

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS Attacks

MEMORANDUM OF INTERVIEW (continuation sheet)

(b) (7)(E)

Directly after the airing of the JO segment, (b) (6) was responsible for identifying the cause of performance issues within ECFS and optimizing the system so that it remained functional. While (b) (6) team didn't look at the source of requests, and they could not isolate web traffic from JO's redirect website GOFCCYOURSELF.COM, it seemed obvious from the timing that large-scale web traffic from GOFCCYOURSELF.COM was likely the source of ECFS's performance issues.¹

(b) (6) explained that ECFS (b) (7)(E) While (b) (6) team remedied this issue, they later noted similar issues on May 17th, 2017 involving traffic from a site called ComcAstroturf.com, that conducted a name search on ECFS (b) (7)(E).²

When asked whether (b) (6) believed that Bray viewed the May 7th Incident as an occurrence not related to the JO segment, (b) (6) stated (b) (6) had no idea what Bray believed. When asked about Bray's analysis and conclusion that ECFS had been the target of multiple distributed denial-of-service (DDoS) attacks from malicious users with mal-formed queries, (b) (6) explained that (b) (6) team provided Bray with statistics regarding ECFS on May 7, but did not conduct log analysis or any other form of analysis (See Exhibit D). When presented with a discussion between Bray and Summerlin regarding the appropriate definition of a DDoS attack that would apply to the May 7th incident (See Exhibit J), (b) (6) did not agree with Bray's understanding of the definition of a DDoS attack. (b) (6) did not view the ratio of comments to overall web traffic as very problematic (see Exhibit C) and stated that (b) (6) would not come to the same conclusions as Bray so easily. (b) (6) added that ECFS's internal system was the source of mal-formed queries, which were very inefficient, and that an outside user would need specific knowledge of ECFS to know about its internal issues.

Agent (b) (7)(C) asked (b) (6) about (b) (6) involvement in the response following the May 7th Incident – specifically the press release from Bray, and the letters to both the Senate and House of Representatives – and whether the event should have been reported to the United

¹ GOFCCYOURSELF.COM is a website that John Oliver's show created and later promoted during his net neutrality segment. The website is a redirect that links visitors to the ECFS net neutrality proceeding in order to simplify the comment filing process. John Oliver also registered another website, justtellmeifimrelatedtoanazi.com, that also redirects to the ECFS net neutrality proceeding.

² ComCastroturf is a website that describes its purpose as helping individuals find out whether their identities were stolen to post anti-net neutrality comments to the FCC. It provides a form that runs on a search on the FCC's ECFS system. The website was created on May 15, 2017.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

Stated Computer Emergency Readiness Team³ (US-CERT). (b) (6) stated (b) was not involved in the press release, (b) was involved in finding answers to specific questions for the congressional responses, and (b) was only involved in discussions after the fact regarding US-CERT.

Agent (b) (7)(C) referenced specific language from FCC Chairman Ajit Pai's June 2017, letters responding to questions from two U.S. Senators: "Specifically, the disrupters targeted the comment filing system application programming interface (API), which is distinct from the website." Exhibit F at Bates No. 025.

(b) (6) stated that (b) had never seen this language before and (b) would hesitate to make such a statement without evidence. When asked about Bray's claim of analysis supporting the malicious usage of bots, (b) (6) replied that, while bots were one possible explanation, there was no analysis, that (b) was aware of, conducted to support those conclusions. (b) (6) thought Bray may have been referencing the statistics (b) (6) team provided, but there was no log analysis conducted. (b) (6) office would have handled any requests for the logs and any analysis. Therefore, (b) would have been aware of any analysis conducted.

(b) (6) did not believe a crime was committed, as (b) did not see any malicious intent from users. (b) (6) added that, although ECFS was hit by bots on a daily basis, any resulting performance issues in connection with the May 7th Incident were due more to ECFS's design than the bots.

When presented with emails between Bray, Tony Summerlin, and a (b) (7)(E) contractor discussing possible DDoS definitions that would fit the description of the May 7th Incident (See Exhibits H, I, and J), (b) (6) explained Bray's broad interpretation of a DDoS was that heavy web traffic was equivalent to a DDoS attack. (b) did not believe Bray initially understood the ECFS architecture. During several informal conversations after the May 7th Incident, (b) (6) explained the architecture, as well as technical details and issues of ECFS, to Bray.

Agent (b) (7)(C) directed (b) (6) attention to the June 2017 response to Congress, specifically to the response to question #1 (see Exhibit F at Bates Nos. 025-26) and asked whether Bray understood those issues when the response was drafted. (b) (6) believes Bray understood ECFS's architecture and issues by the time Bray added text to the response to Congress in June, even though that text did not accurately reflect such an understanding.

³ US-CERT is an office within the Department of Homeland Security (DHS) responsible for (1) providing cybersecurity protection to Federal civilian executive branch agencies through intrusion detection and prevention capabilities; (2) developing timely and actionable information for distribution to federal departments and agencies; state, local, tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations; (3) responding to incidents and analyzing data about emerging cyber threats; and (4) collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

Agent (b) (7)(C) asked (b) (6) to explain Bray's claim that the event occurred at 11 pm on May 7th, not 11:30 pm, and that Bray's staff found markers of malicious intent. (b) (6) stated that (b) (6) team saw a spike in web traffic starting at 11:30 pm, not at 11 pm. In addition, (b) (6) group did not identify any markers of malicious intent, rather (b) (6) group was busy enough keeping systems online throughout the event and did not have time to assess the intent of any users visiting the site. (b) (6) reiterated that (b) (6) was unaware of any additional or external analysis conducted in support of Bray's claims. Agent (b) (7)(C) provided an email chain that included a message from Tony Summerlin on July 24th in which Summerlin requested support for the "swarm bot attack" and that "something" occurred around 11 pm (Exhibit N). (b) (6) explained that the email messages sent in response to Tony Summerlin inquiry on July 24th (Exhibits N, O) were not really "analysis," but rather simply a compilation of system statistics (e.g., number of API requests, list of top foreign IP addresses, web vs API traffic) collected around the time of the event. In fact, (b) (6), the individual on (b) (6) team who forwarded the "analysis" reflected in Exhibit O, states in the message that "It's thin, and could 'barely' be called proper analysis at this point" in (b) (6) response. (b) (6) also states that "going through these without a real log analysis toolkit sucks, just for future reference and in case anyone was wondering" and discusses the difficulties obtaining and uploading the logs providing further evidence that no log analysis was conducted prior to the FCC's June 15th response to Senators Schatz and Wyden.

When questioned about (b) (6) involvement or knowledge of contact with the FBI, (b) (6) stated (b) (6) was aware of the discussions but did not know how they came up.

The interview concluded with (b) (7)(C) describing the differences in opinion (b) (6) had with Bray. (b) (6) viewed himself in a much more technical role, viewing things as either functioning or not functioning, and you fix them and move on if they are broken. In contrast, Bray never considered anything to be a failure and everything was always to be considered an opportunity for improvement.

TABLE OF EXHIBITS:

Exhibit No.:	Document Type(s):	Subject / Description:	Date:	Bates Range:
(b) (7)(E)				
B	Email Chain	IT Team Discussion post event	5/8/2017	008-015
C	Email	DB gives stats to 8 th Floor	5/8/2017	016-017
D	Email	(b) (6) gives TS (b) (7) stats	6/9/2017	018-020
E	Document	Kalkines Warning	2/5/2018	021-022
F	Senate Letter	Chairman Pai Letters to Senators	6/15/2017	023-033
G	Email Chain	TS explains why LE was not informed of the event	7/12/2017	034-036
H	Email	TS reaches out to (b) (7)(E)	5/10/2017	037-038

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

I	Email Chain	TS and DB discuss consulting outside source on DDoS definition	5/10/2017	039-042
J	Email Chain	TS and DB discuss DDoS definitions	5/10/2017	043-047
K	Email Chain	LW provides TB answers to timing questions	12/7/2017	048-055
L	Email	(b) provides TS with (b) (7) graphs	6/9/2017	056-058
M	Email	TS provides DB with (b) (7) graphs	6/9/2017	059-062
N	Email Chain	TS asks (b) to find evidence to support DB claims	7/25/2017	063-065
O	Email Chain	(b) and team provide analysis	7/25/2017	066-070
P	Email Chain	TS discusses response to (b) questions with Cyber Ninjas contractor	11/12/2017	071-075

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS Attacks



Federal Communications Commission
Office of Inspector General

Memorandum of Interview

Type of Activity: ☒ Personal Interview ☐ Telephone Interview ☐ Other	Interview Date and Time: March 8, 2018 8:59 am - 9:38 am
Interview of: Leo Wong, Associate Chief Information Officer (CIO) for Information Resiliency / Chief Information Security Officer (CISO), Office of Managing Director (OMD)	Location of Interview: FCC Headquarters 445 12 th Street, S.W. Washington, DC Room 2-C-323 (OIG Conference Room)
Report Date: March 19, 2018	Conducted By: (b) (7)(C) [REDACTED] [REDACTED] [REDACTED] [REDACTED]

Subject Matter/Remarks

On March 8, 2018, Federal Communications Commission (FCC) Office of Inspector General (OIG) Agents (b) (7)(C) [REDACTED] interviewed Leo WONG.

Agent (b) (7)(C) [REDACTED] is the author of this report.

(b) (7)(C) [REDACTED] presented credentials to WONG at the beginning of the interview. (b) (7)(C) [REDACTED] started the interview by explaining that the focus of the investigation was initially centered on the allegations of the multiple distributed denial-of-service (DDoS) attacks alleged by FCC Chief Information Officer (CIO) David BRAY in the May 8th press release but has now shifted to an investigation of false statements made in responses to congressional inquiries. (b) (7)(C) [REDACTED] explained that the matter was formally referred to DOJ in December, and that although DOJ has not made a decision about opening a case, DOJ is advising OIG during the continued pendency of the investigation. (b) (7)(C) [REDACTED] explained the Kalkines warning and provided a copy of the written Kalkines warning form to WONG. (b) (7)(C) [REDACTED] requested that WONG read through and sign the form acknowledging that the warning had been provided and explained. WONG had no

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

questions and signed the form after reviewing it. A signed copy of the Kalkines warning is attached to this MOI as Exhibit H.

BACKGROUND OF LEO WONG

In response to questioning, WONG voluntarily provided the following information:

Leo Wong's personal and contact information is:

(b) (6)

A large black rectangular redaction box covers the personal and contact information of Leo Wong.

WONG's title is Associate Chief Information Officer for Information Resiliency and Chief Information Security Officer. WONG has been a full time employee of the FCC since 2015. His current supervisor is Mark Savi, Assistant CIO for Enterprise IT Operations. Prior to this, he reported to Christine Calvosa, the FCC's Deputy CIO for Technology and Resiliency and currently Acting CIO.

INFORMATION PROVIDED BY LEO WONG

In response to questioning, WONG voluntarily provided the following information:

WONG stated he had no role in responding to the event on May 7 and 8, 2017 that disrupted the Electronic Comment Filing System's (ECFS) performance (the "May 7th Incident"), and that he only became involved when the ECFS helpdesk received a call from the FBI.

(b) (7)(C) provided an email chain started on May 9, 2017, in which Matthew BERRY (FCC Chief of Staff) asks BRAY about contacting federal law enforcement (Exhibit A). In this email chain, WONG advises BRAY that "I would say we are within Federal regulations to not report this incident of high traffic to US-CERT due the the traffic to ECFS not being a major incident."

(b) (7)(C) asked why the May 7th incident was not classified as a security incident, and why the United States Computer Emergency Readiness Team (US-CERT) was never contacted regarding the incident. WONG replied that his team never reviewed any logs, and therefore had no evidence that a security incident had occurred. US-CERT would have requested logs if he had contacted them, and that, since his team did not have any logs, they did not report the May 7th incident as a security incident. Wong added that his team was still building its processes regarding the use of (b) (7)(E) the platform on which ECFS is hosted.

[NOTE: This response directly contradicts the reasons for not notifying US-CERT provided to BERRY (through BRAY) and numerous statements to OIG throughout the course of the investigation].

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

(b) (7)(C) asked WONG to describe his involvement in the press release made by BRAY, as well as the responses that the FCC prepared to the letters from the Senate and House of Representatives seeking information regarding the purported DDoS attack. WONG claimed to have had no involvement in the press release. (b) (7)(C) asked WONG if he agreed with the conclusion in BRAY's press release that the FCC was "subject to multiple distributed denial-of-service attacks (DDoS)." WONG indicated that he saw no evidence of a denial of service attack (DoS).

(b) (7)(C) provided an email message dated July 12, 2017 from Tony SUMMERLIN (contractor who serves as Senior Advisor to the CIO) to Leo WONG discussing the way in which the DDoS attack was reported and how the IT group should respond to OIG auditors conducting the FISMA¹ audit (Exhibit C). When asked to explain SUMMERLIN's draft response to the FISMA Auditors, WONG replied he was unsure, but SUMMERLIN may have been trying to explain that, though BRAY referred to the May 7th incident as a DDoS attack, WONG's team found no evidence to support the claim.

WONG said that the draft congressional responses were circulated to IT leadership. He was consulted regarding his discussion with the FBI (Exhibit E, page 3). (b) (7)(C) asked WONG whether any log analysis was conducted, as referenced in the congressional response (Exhibit E, page 2), to which WONG replied that his team didn't conduct any analysis and that "I think the only 'analysis,' was from (b) (7) given to (b) (6) team."² WONG's team did not have access to the logs for analysis but (b) (6) team did.

(b) (7)(C) asked WONG whether he could have requested logs for analysis, to which WONG replied "That was all of (b) (6) team, they were so busy, David Bray said the priority wasn't investigating what happened but to keep the system up." When asked whether BRAY directed that any log analysis be conducted, WONG explained that BRAY asked him to contract with an organization named Cyber Ninjas to conduct the analysis, but that by the time Cyber Ninjas was ready to conduct the analysis, BRAY had left the commission and log analysis was no longer a priority. **[NOTE:** The statement of work for the Cyber Ninjas project was not created until August 2017.]

WONG was presented with responses to both the Senate (Exhibit E, page 3) and House (Exhibit F, page 2) characterizing contact with the FBI regarding the May 7th incident. WONG stated that both summaries were accurate. WONG also acknowledged the accuracy of his summary of the discussion with FBI Special Agent (b) (6) (Exhibit E, page 3 and Exhibit F, page 2). (b) (7)(C) provided a copy of an email message dated May 10, 2017, from WONG to BRAY, the

¹ FISMA is the Federal Information Security Modernization Act of 2014.

² WONG is referring to the statistics provided by (b) (7)(E) to (b) (6) team within ITC on May 8, 2017. (b) (7) provides the content delivery service on which tECFS is hosted under contract to the FCC.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

(b) (6) email group³, and (b) (6) summarizing the results of his conversation with the FBI (Exhibit B). (b) (7)(C) asked WONG if he could explain why the summary he provided to the ITleadership group on May 10th that was written shortly after his conversation with the FBI didn't include several significant comments that were included in the Senate and House response such as the "conclusion" that was reached with the FBI regarding the severity of the incident or whether or not the matter should be reported to US-CERT. WONG simply replied "no."

(b) (7)(C) provided an email message dated July 5, 2017, from WONG to SUMMERLIN that included a draft response to Congress and included a comment from WONG regarding his conversation with the FBI. When asked to explain his comments⁴ on the circulated congressional response (Exhibit D), WONG explained that he and SA (b) (6) agreed to contact each other if either found any additional evidence regarding the May 7th incident that met the threshold of a major incident which would require further reporting, and that, since neither contacted each other, WONG assumed there was no evidence that a major incident had occurred. However, when Agent (b) (7)(C) replied asking WONG if he had contacted the FBI again, WONG said he believed he spoke to SA (b) (6) again.⁵ [NOTE: The comment in the draft report clearly references an event that has already taken place – "decision was reached later" – and not some future contact. In addition, WONG knew from his conversation with SA (b) (6) that the FBI did not intend to do any additional work related to this incident.]

(b) (7)(C) presented WONG with the MOI of SA (b) (6) disputing WONG's characterization of their conversation (Exhibit G). (b) (7)(C) noted the following discrepancies between WONG and SA (b) (6) statements:

- SA (b) (6) disputed the characterization of (b) (6) discussion with you that was included in the responses to the Senate and House.
- SA (b) (6) stated (b) (6) does not consider cyber matter in terms of "major" or not and that (b) (6) would not have agreed to anything in these terms.
- SA (b) (6) stated (b) (6) only interest in this matter is whether or not there was evidence of criminal activity.
- SA (b) (6) stated (b) (6) did not have enough information to reach any conclusion about criminality (especially since (b) (6) did not have any information on what was in the system logs).

³ On May 10, 2017, the (b) (6) email group was comprised of Christine Calvosa, (b) (6) Leo Wong, and Tony Summerlin (CTR).

⁴ In his comments to the draft report on July 5, 2017, WONG provided the following comment on the FCC's characterization of his discussion with SA (b) (6) "Sounds like the decision was made jointly which really wasn't the case. Can we say. "Decision was confirmed later with FBI that the threshold for major incident was indeed not met and no US-CERT incident was necessary."

⁵ This response contradicts his previous statement that he had not spoken to the FBI or SA (b) (6) after their initial conversation. It should also be noted that SA (b) (6) stated that (b) (6) did not speak with WONG after their first conversation and that (b) (6) is not aware of any additional contact between WONG and the FBI.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

- SA (b) (6) stated PPD-41 was not mentioned in the discussion and that (b) has no knowledge regarding PPD-41.

In response to each of these discrepancies, WONG replied simply with “Okay.” WONG later stated there may have been a misunderstanding between himself and SA (b) (6), and that WONG was only making the point that he did not have any evidence to characterize the May 7th incident as a major incident that would require a US-CERT response. When Agent (b) (7)(C) asked whether WONG informed SA (b) (6) that WONG’s team did not have access to the logs, WONG replied he did not inform him because SA (b) (6) hadn’t asked. WONG acknowledged, when questioned by Agent (b) (7)(C), that (b) did not distinguish between evidence against and a lack of evidence. This distinction may not have been clear on his part.

Although WONG stated he was the original point of contact between OIG and IT leadership, he believed (b) (6), the current point of contact, has better access.⁶

TABLE OF EXHIBITS:

Exhibit No.:	Document Type(s):	Subject / Description:	Date:	Bates Range:
A	Email Chain	BRAY and BERRY discuss reporting incident to law enforcement	5/9/2017	001-016
B	Email	WONG summary of conversation with FBI	5/10/2017	017-019
C	Email Chain	SUMMERLIN gives WONG a response for OIG Auditors	7/12/2017	020-022
D	Email Chain	WONG edits to draft response to House letter	7/5/2017	023-026
E	Letter	FCC Response to Senator Wyden	6/15/2017	027-032
F	Letter	FCC Response Representative Doyle	7/21/2017	033-036
G	MOI	MOI for SA (b) (6)	2/8/2018	037-051
H	Kalkines	Signed Kalkines Warning from WONG	3/8/2018	052-053

⁶ WONG was originally identified as the central point of contact for Agent (b) (7)(C) to discuss the May 7th incident with IT leadership. Christine Calvosa, Acting CIO, later identified (b) (6) as a more appropriate point of contact to discuss the technical aspects of the ECFS and IT response to the May 7th incident.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------



Federal Communications Commission
Office of Inspector General

Memorandum of Interview

Type of Activity: ☒ Personal Interview ☐ Telephone Interview ☐ Other	Interview Date and Time: March 29, 2018 2:00pm - 2:30pm
Interview of: Matthew Berry, Chief of Staff, Office of Chairman Pai	Location of Interview: FCC Headquarters 445 12 th Street, S.W. Washington, DC (b) (6)
Report Date: March 30, 2018	Conducted By: Jay KEITHLEY, Assistant Inspector General for Investigations (b) (7)(C)

Subject Matter/Remarks

On March 28, 2018, Federal Communications Commission (FCC) Office of Inspector General (OIG) Agent (b) (7)(C) and Assistant Inspector General for Investigations (AIGI) Jay Keithley (KEITHLEY) interviewed Matthew BERRY.

(b) (7)(C) conducted the interview and KEITHLEY took notes during the interview. KEITHLEY is the author of this report.

(b) (7)(C) presented credentials to BERRY at the beginning of the interview. (b) (7)(C) started the interview by acknowledging that BERRY had been briefed on this investigation and was aware of the investigation including the referral of the matter to the Fraud and Public Corruption section of the United States Attorney's Office for the District of Columbia in December. (b) (7)(C) indicated that, although DOJ has not made a decision about opening a case, DOJ is advising OIG during the continued pendency of the investigation. (b) (7)(C) explained to BERRY that he is being interviewed as a witness in this matter and that no agent warning is necessary. However, (b) (7)(C) did explain to BERRY that he is obligated to tell the truth and it was a crime for him not to do so.

Case Number:
OIG-I-17-0011

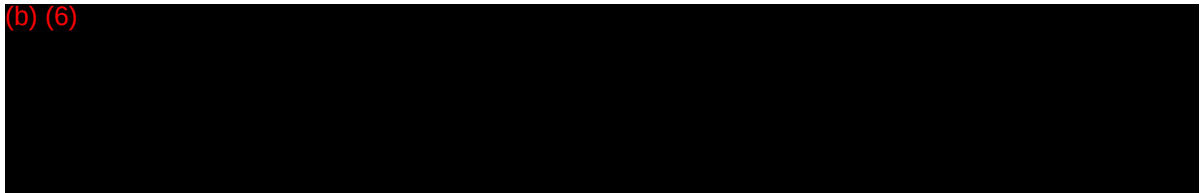
Case Title:
ECFS DDoS Attacks

MEMORANDUM OF INTERVIEW (continuation sheet)

BACKGROUND OF MATTHEW BERRY

Matthew Berry's personal and contact information is:

(b) (6)

A large black rectangular redaction box covers the personal and contact information of Matthew Berry.

BERRY's title is Chief of Staff (COS). BERRY has been COS since Ajit Pai became the FCC Chairman in January 2017. BERRY was the COS in May 2017 when the multiple distributed denial-of-service attacks alleged by Dr. David Bray (BRAY), the Commission's Chief Information Officer, took place and when the congressional responses, referenced below, were provided to the Senate and House in June and July 2017, respectively. BERRY reports to Chairman Pai.

INFORMATION PROVIDED BY MATTHEW BERRY

In response to questioning, BERRY voluntarily provided the following information:

(b) (7)(C) explained that the purpose of the interview was to determine BERRY's involvement in the development and release of three documents associated with a purported Distribute Denial of Service (DDoS) attack on the Commission's Electronic Comment Filing System (ECFS). The alleged attack took place over the night of May 7th and the early morning of May 8th. Copies of the documents – a FCC Statement (press release) issued May 8, 2017, a letter dated June 15, 2017 to Senator Ron Wyden responding to questions regarding the purported DDoS attack, and a letter dated July 21, 2017 to several Congressional Democrats responding to questions similar to those propounded by Senator Wyden. Copies of the documents are attached as Exhibits A, D and E, respectively (collectively "EXHIBITS").

BERRY was COS on May 7th and was, as explained more fully below, involved in the development of the EXHIBITS. He is not an expert in computer or network technology or operations and relied on technical staff in the Commission's IT group, particularly BRAY, in developing the EXHIBITS. BRAY was BERRY's primary contact/source of information in this matter.

BERRY was aware John Oliver (OLIVER) was doing a segment on the FCC's Internet Freedom/Net Neutrality rule making proceeding on Sunday May 7th. He sent questions to the Commission's Office of Media Relations regarding how to handle communications/comments flowing from the OLIVER segment. He may have made IT aware of the OLIVER segment, but is not sure. BERRY vaguely recalls discussions involving ITC related to preparing for the Net Neutrality proceeding and ensuring systems were ready for comments.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE INFORMATION
FCC Office of Inspector General
Page 2 of 4

MEMORANDUM OF INTERVIEW (continuation sheet)

BERRY watched the Oliver segment and shortly after the show, learned from Twitter that the Commission's electronic comment filing system (ECFS) was having problems (slowed or overwhelmed). He then began receiving media inquiries. The next morning, Monday, May 8th, BERRY worked with Commission IT and Media Relations staffs to determine how to respond to the situation and the media inquiries. BERRY had no first-hand knowledge of the situation, and the first draft of FCC Press Release came from BRAY. (b) (7)(C) provided a copy of the Press Release (Exhibit A) and asked BERRY who would have been responsible for the language regarding "deliberate attempts by external actors to bombard the FCC's comment system with a high amount of traffic to our commercial cloud host. These actors were not attempting to file comments themselves; rather they made it difficult for legitimate commenters to access and file with the FCC." BERRY indicated this language came from BRAY. BERRY also recalls that (b) (6) may have been involved in the discussion.

BERRY assumed the Oliver segment was the cause of the increased traffic on ECFS, but BRAY told him that wasn't so. In calls, meetings and email exchanges BRAY and his staff told BERRY that the "path used" (BERRY's words) to send traffic to ECFS would not come from the "gofccyourself.com" URL that the OLIVER program referenced during the episode and tweeted. Tony Summerlin (SUMMERLIN), an IT contractor who worked for BRAY, was very involved in these discussions. (b) (7)(C) provided a email chain from May 8, 2017 (Exhibit B) in which BERRY asked BRAY if he was "confident that it wasn't a bunch of John Oliver viewers attempting to comment at the same time that did this but rather some external folks deliberately trying to tie-up the server" and BRAY responded "Yes, we're 99.9% confident this was external folks deliberately trying to tie-up the server to prevent others from commenting and/or create a spectacle." BERRY acknowledged that this was the email chain in which he questioned BRAY about the possibility that the event was caused by the result of the "gofccyourself" URL the OLIVER program had established and that he relied on BRAY's response that the event was not the result of that URL.

During these discussions, BERRY asked if law enforcement, the Department of Homeland Security (DHS) or the FBI should be contacted. When he first learned that the FBI had contacted the Commission (OIG), BERRY wanted to confirm that the contact was bona fide – was in fact from an FBI agent. Later that morning, the IT Department told BERRY that they had spoken with both DHS and the FBI and both concurred with IT's handling of the situation. (b) (7)(C) provided a email chain from May 9, 2017 (Exhibit C) in which BERRY asks BRAY about contacting federal law enforcement and, in a followup message, asking if there are "any govt's [sic] organizations we could at least consult with." BERRY acknowledged this was the email chain in which he questioned BRAY about federal law enforcement and another federal agency.

(b) (7)(C) provided a copy of the letter sent to Senator Wyden on June 15, 2017, in response to questions regarding the event (Exhibit D). (b) (7)(C) asked BERRY to describe his involvement in the preparation of the letter. BERRY indicated that (b) (6), a staffer in the FCC's Office of Legislative Affairs (OLA), worked with BRAY and ITC to prepare the first draft of the response to Senator Wyden's questions. When he received the resulting draft letter,

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

BERRY felt it needed work. BERRY edited the response based on what he was told orally and in email from IT, primarily BRAY. The language in Question 1 of the response to Wyden, Exhibit D, mentioning (1) reliance on analyses of the logs and (2) contacts with and statements of the FBI, came from BRAY. BERRY found it difficult to pull information together to develop the response, and Chairman Pai was upset with the process.

(b) (7)(C) provided a copy of the letter sent to Congressman Doyle on July 21, 2017, in response to questions regarding the event (Exhibit E). (b) (7)(C) asked BERRY to describe his involvement in the preparation of the letter. BERRY's recollection of the development of the response to questions from the House Democrats is not as good as in the development of the response to Senator Wyden; however, his role was similar. BERRY recalls this letter was easier to prepare because OLA was able to use the June 15, 2017 letter as a model.

Since the purported DDoS attack, Berry has "stayed on" IT to make sure preventative measures – more resources, scaling up and ways to "shut off" the system when confronted with unusually high volumes of comments – are being pursued. He believes system monitoring and processing have improved since the "attack."

TABLE OF EXHIBITS:

Exhibit No.:	Document Type(s):	Subject / Description:	Date:	Bates Range:
A	Press Release	Press Release by Dr. Bray on May 8, 2017	5/8/2017	001-002
B	Email Chain	MB question about John Oliver episode and DB response.	5/8/2017	003-005
C	Email Chain	Email chain regarding the notification of federal law enforcement or another federal agency.	5/9/2017	006-011
D	Letter	FCC Response to Senator Wyden	6/15/2017	012-017
E	Letter	FCC Response to Congressman Doyle	7/21/2017	018-021

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS Attacks



Federal Communications Commission
Office of Inspector General

Memorandum of Interview

Type of Activity: ☒ Personal Interview ☐ Telephone Interview ☐ Other	Interview Date and Time: April 20, 2018 08:58 am - 10:36 am
Interview of: Tony Summerlin, Senior Strategic Advisor, Censeo Consulting Group, Inc.	Location of Interview: FCC Headquarters 445 12 th Street, S.W. Washington, DC (b) (7)(C)
Report Date: April 27, 2018	Conducted By: (b) (7)(C)

Subject Matter/Remarks

On April 20, 2018, Federal Communications Commission (FCC) Office of Inspector General (OIG) Agents (b) (7)(C) interviewed Tony SUMMERLIN.

Agent (b) (7)(C) is the author of this report.

(b) (7)(C) presented credentials to SUMMERLIN at the beginning of the interview.

In response to questioning, Tony SUMMERLIN voluntarily provided the following information:

BACKGROUND OF TONY SUMMERLIN

Tony SUMMERLIN's personal and contact information is:

(b) (6)

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS Attacks

MEMORANDUM OF INTERVIEW (continuation sheet)

SUMMERLIN's title is Special Advisor to the CIO. SUMMERLIN was a federal employee at the FCC from January 2015 to the end of that year. Since then, he has served as a subcontractor with Censeo Consulting Group, Inc., providing consulting services to the CIO. His Contracting Officer Representative is Christine CALVOSA, Acting CIO.

INFORMATION PROVIDED BY TONY SUMMERLIN

SUMMERLIN began the interview by providing a brief overview of his career and professional qualifications. SUMMERLIN attended college at UNC Chapel Hill and originally worked as a banker and later financial auditor. SUMMERLIN spent the majority of his career in the software and information technology sector; he described several software companies that he created and later sold. For the last twenty or so years, SUMMERLIN has worked in various roles and capacities involving government information technology leadership. SUMMERLIN specifically mentioned his previous work at the White House, Director of National Intelligence (DNI), his current work with the Joint Special Operations Command / Special Operations Command (in a volunteer capacity), his involvement in the development of Microsoft SharePoint, as well as his friendship with Vint Cerf. SUMMERLIN had previously worked with former FCC CIO David BRAY while they were both at DNI; when BRAY became the CIO at FCC, he asked SUMMERLIN to come on as an advisor/consultant.

SUMMERLIN claimed that he was responsible for the current version and configuration of the electronic comment filing system (ECFS); he explained that former FCC Chairman Tom Wheeler asked him to fix the system after the 2014 net neutrality filing period. SUMMERLIN lamented that the Commission was neither willing to spend the money to change their public comment procedures. He further explained that (b) (7)(E)¹, the underlying system for ECFS, would likely never fail or crash, it could easily become stretched so thin that the system would appear non-responsive to users.

Specifically regarding the May 7th event, SUMMERLIN was notified by another contractor, (b) (6), at 6:00 am on May 8th, 2017. SUMMERLIN asked (b) (6) whether any of the traffic appeared to be malicious. (b) (6) replied that (b) (6) did not see any indication of malicious traffic, only that (b) (6) saw bot traffic, to which SUMMERLIN replied "get out the credit card" indicating that the Commission would incur additional costs responding to the incident. SUMMERLIN explained that bot traffic was likely the source of the spike since he did not think human-generated traffic could have generated such a spike.

SUMMERLIN was presented with an email chain between members of the Information Technology Center (ITC) discussing the May 7th event (Exhibit A). (b) (7)(C) pointed out that (b) (6), ECFS Subject Matter Expert, consistently indicated that the incident was the

¹ (b) (7)(E). It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE INFORMATION
FCC Office of Inspector General
Page 2 of 5

MEMORANDUM OF INTERVIEW (continuation sheet)

result of the John Oliver episode. (b) (7)(C) also indicated that Matthew BERRY, FCC Chief of Staff, believed the event was a result of the John Oliver episode and that he asked BRAY directly whether this was the case. BRAY responded that he was “99.9% sure” that the incident was not the result of the John Oliver episode. SUMMERLIN was not aware of BRAY’s statement to BERRY. SUMMERLIN stated BRAY was furious that he had not been informed about the John Oliver episode. He also confirmed that BRAY did, in fact, believe the John Oliver episode was to blame for the May 7th event. BRAY regularly complained about the John Oliver episode for the remainder of his time as the FCC CIO; BRAY had even mentioned over the phone one week ago (mid-April 2018) how he felt the situation regarding the John Oliver episode was unfair.

SUMMERLIN did not participate in drafting the May 8th press release. In fact, SUMMERLIN has not read the press release. (b) (7)(C) read the following section from the press release and asked SUMMERLIN for his reaction:

“Beginning on Sunday night at midnight, **our analysis reveals** that the FCC was subject to **multiple distributed denial-of-service attacks** (DDoS). These were **deliberate attempts by external actors** to bombard the FCC’s comment system with a high amount of traffic to our commercial cloud host. **These actors were not attempting to file comments themselves**; rather they made it difficult for legitimate commenters to access and file with the FCC. While the comment system remained up and running the entire time, these DDoS events tied up the servers and prevented them from responding to people attempting to submit comments. We have worked with our commercial partners to address this situation and will continue to monitor developments going forward.”

SUMMERLIN disagreed with BRAY’s characterization of the May 7th event in the press release. SUMMERLIN was unsure where BRAY got some of his information regarding the intent of comment filers or potentially malicious intent of bots. He also disagreed with BRAY’s characterization of summary counts of API activity as analysis. SUMMERLIN and BRAY had argued extensively on BRAY’s definition of “analysis.” SUMMERLIN characterized the summary counts of API activity as an “observation” as opposed to analysis. SUMMERLIN did agree with BRAY’s technical description of the May 7th event (Exhibit B). SUMMERLIN stated the heavy API traffic was to blame for ECFS’ performance issues, and that, while he wasn’t sure whether the redirect provided John Oliver during his net neutrality episode (gofccyourself.com) could have been a factor in the heavy traffic, he did mention the FCC was unable to verify any incoming comments or traffic because of policy limitations.

At the time of the May 7th event, SUMMERLIN was unaware of the John Oliver episode. John Oliver was never considered during the immediate aftermath of the event. Rather, he and technical experts such as (b) (6) were concerned solely with keeping the system online.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE INFORMATION
FCC Office of Inspector General
Page 3 of 5

MEMORANDUM OF INTERVIEW (continuation sheet)

SUMMERLIN contacted (b) (6)² to inquire whether they would be interested in supporting the FCC regarding the May 7th event (Exhibit C). The FCC did not ultimately establish a contract with (b) (7)(E) but (b) (6) would not have reached a conclusion about the cause of the event without performing a thorough analysis. SUMMERLIN explained he ultimately works for BRAY, and he was trying to support BRAY's decision that there had been a DDoS. SUMMERLIN told BRAY that, while he did not agree there had been a DDoS, if BRAY insisted there had been a DDoS, he needed to qualify the term.

When presented with an email chain in which SUMMERLIN explains that the "language that Dr. Bray chose led people to think that it was meant to cause harm" and explains why the incident was not reported to US-CERT (Exhibit D), SUMMERLIN stated that members of ITC leadership, specifically Leo WONG, saw the event as a resource capacity issue, and not a malicious or DDoS issue. He believed WONG likely opted not to report the issue to US-CERT as he saw no malicious activity to report in the first place. Members of ITC leadership were in agreement that the May 7th event was a resource issue, and that they only were supporting BRAY, their boss, when they considered the possibility that the event was a DDoS. At one point SUMMERLIN pleaded with BRAY not to make any claims that the event was a DDoS.

SUMMERLIN, when presented with the one-page description of the May 7th event that was given to Congress, stated that, while he does agree that the description of the event was vague, it was technically true. SUMMERLIN was involved in the development of the Congressional responses; he advised multiple ITC members (e.g., WONG, (b) (6)) on their portions of the response. SUMMERLIN had far too little information in the way of event logs to make any thorough determination or analysis of the event. His lack of data was the reason he stated the event occurred at 11pm instead of 11:30 pm. He implied BRAY kept stating the event occurred at 11 and not 11:30, so he attempted to find evidence to back up that claim, but was unable to gather any evidence period, due to the limited log availability. While he found WONG's statements about his interaction with the FBI odd, because WONG was the CISO and he is only a contractor, SUMMERLIN deferred to WONG's statement. SUMMERLIN agreed that the FBI would not reach a conclusion on the severity of the event based on a phone call without any subsequent analysis.

The interview concluded with SUMMERLIN explaining that, until CGB was willing to change their comment collection policies, he believed the FCC would continue to encounter similar issues in the future. SUMMERLIN, as a side note, also mentioned that members of the 8th floor had asked for special exceptions to the API submission limit, claiming he was told "We have these folks that want to"³

² (b) (6) and a (b) (6).
(b) (6) provides a variety of IT services including Incident Response.

³ SUMMERLIN trailed off during his response but it was clear to the investigators that "members of the 8th floor" (a term used to describe the Office of the Chairman and Commissioners) were aware of comment campaigns that were intending to use the Public API to file bulk comments.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

TABLE OF EXHIBITS:

Exhibit No.:	Document Type(s):	Subject / Description:	Date:	Bates Range:
A	Email Chain	ITC Email chain just after the May 7 th event	May 8, 2017	001 - 008
B	Email	Bray provides an explanation of May 7 th event to CoS	May 8, 2017	009 - 010
C	Email Chain	Summerlin contacts (b) (7)(E) for professional opinion	May 10, 2017	011 - 014
D	Email Chain	Summerlin explains why May 7 th event was not reported	July 12, 2017	015 - 017

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS Attacks



Federal Communications Commission
Office of Inspector General

Memorandum of Interview

Type of Activity: ☒ Personal Interview ☐ Telephone Interview ☐ Other	Interview Date and Time: May 3, 2018 1:00 pm - 2:45 pm
Interview of: Christine Calvosa, Acting Chief Information Officer (CIO) and Deputy CIO for Technology and Resiliency (T&R), Information Technology Center (ITC) within the Office of Managing Director (OMD)	Location of Interview: FCC Headquarters 445 12 th Street, S.W. Washington, DC (b) (7)(C)
Report Date: May 4, 2018	Conducted By: (b) (7)(C)

Subject Matter/Remarks

On May 3, 2018, Federal Communications Commission (FCC) Office of Inspector General (OIG) Agents (b) (7)(C) interviewed Christine CALVOSA.

Agent (b) (7)(C) is the author of this report.

(b) (7)(C) presented credentials to CALVOSA at the beginning of the interview. (b) (7)(C) started the interview by explaining that the focus of the investigation was initially centered on the allegations of the multiple distributed denial-of-service (DDoS) attacks alleged by FCC Chief Information Officer (CIO) David BRAY in the May 8th press release but has now shifted to an investigation of false statements made in responses to congressional inquiries. (b) (7)(C) explained that the matter was formally referred to DOJ in December, and that although DOJ has not made a decision about opening a case, DOJ is advising OIG during the continued pendency of the investigation. (b) (7)(C) explained the Kalkines warning and provided a copy of the written Kalkines warning form to CALVOSA. (b) (7)(C) explained that if false statements are made during the interview we are obligated to refer those false statements to DOJ. (b) (7)(C) requested that CALVOSA read through and sign the form acknowledging that the warning had

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

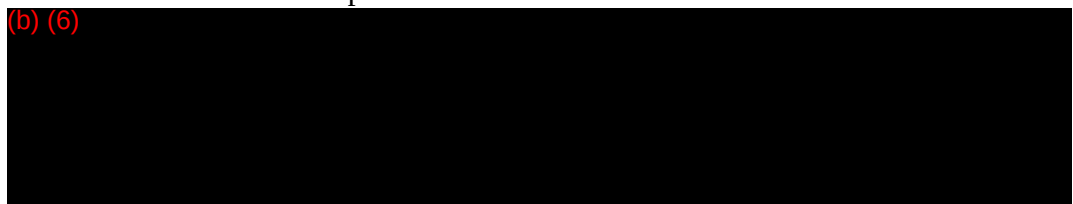
been provided and explained. CALVOSA had no questions and signed the form after reviewing it. (b) (7)(C) asked CALVOSA if she would like a copy of the signed Kalkines form and CALVOSA indicated that she would like a copy (a copy of the signed form was scanned and sent to CALVOSA via email on May 4, 2018). A signed copy of the Kalkines warning is attached to this MOI as Exhibit A.

BACKGROUND OF CHRISTINE CALVOSA

In response to questioning, Christine CALVOSA voluntarily provided the following information:

Christine CALVOSA's personal and contact information is:

(b) (6)

A large black rectangular redaction box covering several lines of text.

CALVOSA's title is Acting Chief Information Officer (CIO). CALVOSA has been acting CIO since Dr. David BRAY left the FCC in October 2017. CALVOSA is also the Deputy CIO (DCIO) for Technology and Resiliency. CALVOSA is a GS-2210-15. The CIO position is a Senior Executive Service (SES) position. CALVOSA's duty station is FCC Headquarters located at 445 12th Street, S.W., Washington, DC 20554. CALVOSA's regular duty hours are 8:00am to 5:30pm or 6:00pm.

CALVOSA's duties and responsibilities as DCIO for Technology and Resiliency (T&R) are to oversee and provide guidance on any technology or security involvements in support of the Commission as a whole and stake holders. T&R includes Cloud Integration and Catalog, Enterprise IT Operations, Information Resiliency, and Tailored Platform and Data. She is responsible for the IT operations ops team, service center, daily operation of Commission systems, IT engineering and cloud solutions. She is also responsible for new technology efforts (e.g., Windows 10, VDI, Skype vs Jabber, etc.).

CALVOSA's duties and responsibilities as Acting CIO include overseeing all of IT including IT Management and Lifecycle (M&L). (b) (6) is the DCIO for M&L. M&L includes FCC Intrapreneurs, IT Planning and Performance, IT Budget and Acquisition, and Data and IT Policy. IT Budget and Acquisition is currently managed by (b) (6). Data and IT Policy (currently without a team lead) also includes privacy office (lead by Leslie Smithh) and 503 compliance.

CALVOSA started at the FCC in December 2014. Prior to working at the FCC, CALVOSA served as the Chief Technology Officer (CTO) with the United States Department of Agriculture (USDA) Natural Resources Conservation Service (NRCS). As Acting CIO, CALVOSA reports

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

to Mark Stephens, the FCC Managing Director. As the DCIO for Technology and Resiliency, CALVOSA reported directly to Dr. BRAY.

CALVOSA graduated from Penn State University in 2001 where she earned a Bachelor of Science in Management Information Systems and a Minor in International Studies. CALVOSA worked for an IT consulting firm (PEC Solutions) for 3 to 4 years before moving to Booz Allen Hamilton for almost 5 years. After Booz Allen Hamilton, CALVOSA started her federal career at USDA-NRCS.

CALVOSA described her relationship with Dr. BRAY as strictly professional for a long period. CALVOSA developed a more personal relationship with Dr. BRAY after he adopted a child and has stayed in touch with Dr. BRAY since he left the FCC in October 2017.

(b) (7)(C) asked about BRAY's management style. BRAY looked to his deputies, CALVOSA and (b) (6), for guidance and as resources when decisions were made. Ultimately, BRAY was the decision maker. BRAY was not a micromanager. When things went down, there were lots of people screaming at him. He was very involved made sure "we could get things operational in a timely manner." BRAY focused on getting services restored fast for the FCC user base.

INFORMATION PROVIDED BY CHRISTINE CALVOSA

CALVOSA had no role in responding to the event on May 7th. CALVOSA was away from the office on personal travel from Saturday, May 6th until Wednesday, May 10th. CALVOSA did not return to the FCC until Thursday, May 11th. CALVOSA did not check her email while she was away from the office and she was not contacted by anyone from the FCC during this period. CALVOSA was not aware of the incident and did not become involved in responding to the incident until May 11th.

(b) (6) provided a copy of press release issued by BRAY on May 8th in which BRAY alleges that "our analysis reveals that the FCC was subject to multiple distributed denial-of-service attacks" and that these were "deliberate attempts by external actors to bombard the FCC's comment system with a high amount of traffic" (attached to this MOI as Exhibit B).

CALVOSA stated that this was the first time she had read the press release. CALVOSA "wasn't in the nitty gritty of when this happened" and no one called her when she was on vacation. The "IT team probably gave David the information based on what he was asking, but I don't know."

(b) (7)(C) provided a copy of the email message BRAY sent on May 8, 2017, at 1316 hours with the subject line "***Internal information only.***" (attached to this MOI as Exhibit C).

(b) (7)(C) stated this email message has been provided by BRAY as the "analysis" that BRAY references in the press release. (b) (7)(C) explained that OIG analysis indicates the incident was a viral event that was direct result of the John Oliver episode and that the URL redirect from

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

John Oliver generated a significant amount of API activity that, combined with the fact that the Electronic Comment Filing System (ECFS) (b) (7)(E) overloaded the API and reduced system availability. By the time (b) (6) (an FCC contractor involved in managing the IT infrastructure hosting ECFS) got into the office on Monday, May 8th, there were numerous alerts from (b) (7)(E) (b) (6) told OIG that the focus was on fixing ECFS and the Agency dealt with the issue of handling the load capacity by (b) (7)(E).

(b) (7)(C) asked what was behind the responses that went to the Senate and House responding to inquiries and describing the event. (b) (7)(C) explained that OIG knows there was some discussion about having (b) (7)(E) coming in under contract to determine what caused the event, but that these efforts were not completed. CALVOSA stated she has “not done any in depth analysis” and that “when I got in on Thursday, my inbox was flooded.” “My focus was getting the system up and stable. Getting it back up. I applauded (b) (6) and then on getting it back up.”

(b) (7)(C) asked if there was ever an effort made to find out what actually happened? CALVOSA stated that there was “not on my end.” (b) (7)(C) asked if BRAY made any effort to find out what actually happened. CALVOSA stated “that’s a good question to ask him [BRAY].” (b) (7)(C) asked how BRAY reached his conclusions? CALVOSA replied “You’d have to ask Dr. Bray how he reached his conclusions. (b) (7)(C) indicated SUMMERLIN (Tony SUMMERLIN, FCC IT contractor) told OIG that Exhibit C was not an analysis and that SUMMERLIN argued with BRAY about this matter for a month. CALVOSA indicated she would not describe it as an analysis but would say that it’s an observation.

CALVOSA had not been aware John Oliver was doing an episode on Net Neutrality on May 7th. CALVOSA was also not aware of the John Oliver episode in 2014 that also resulted in ECFS system availability issues.

(b) (7)(C) provided an email chain between Matthew BERRY (FCC Chief of Staff) and BRAY from May 8, 2017 at 1035 hours in which BERRY asks BRAY if he is “confident that it wasn’t bunch of John Oliver viewers attempting to comment at the same time that did this but rather some external folks deliberately trying to tie-up the server” and BRAY’s response that “we’re 99.9% confident this was external folks deliberately trying to tie-up the server to prevent others from commenting and/or create a spectacle” (attached to this MOI as Exhibit D). CALVOSA was not familiar with this email exchange. [NOTE: The ITleadership Outlook email group was copied on this email exchange and CALVOSA was a member of that email group at the time of this message.]

(b) (7)(C) provided an email message sent from SUMMERLIN to Leo WONG on July 12, 2017 at 1638 hours in which SUMMERLIN discusses how BRAY’s press release was misinterpreted (attached to this MOI as Exhibit E). This message was drafted by SUMMERLIN

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

to respond to an email message from (b) (6) (FCC OIG Auditor conducting the FISMA audit) but was never sent to FCC OIG. (b) (7)(C) asked CALVOSA for her impression of the email. Was it a view held in ITC that this was a misunderstanding? Was BRAY describing a crime in the press release? CALVOSA agreed with what SUMMERLIN stated in the email message “that it was likely misinterpreted.” CALVOSA went on to say the following:

“Me personally, I wasn’t here. I’m just going to tell you, as the DCIO of R&T, if asked my opinion, I would have changed how this was represented [in the press release]. I would have looked at the observation set and described what we saw, not necessarily saying [reaching a conclusion] since we hadn’t done a thorough analysis. This is the first agency I’ve been at where this is very public facing, that wants to get information out fast. I would make sure that I vocalize what we were seeing in terms of activity, what we’re observing. I would have left it that there’s more to come, and that we’re moving to get the system back up as fast as possible.

(b) (7)(C) asked why the event wasn’t recognized internally as a security event or FISMA event? CALVOSA provided the following response:

“I don’t know, because I wasn’t here. Typically when we see an incident, our incident response procedures have us follow up our process very soon after the event, for improvement, to act on something. I would have taken a different approach.”

(b) (7)(C) asked why US-CERT wasn’t notified. CALVOSA provided the following response:

“Leo [WONG] as IT security lead has the responsibility to make a recommendation on what we should do. He worked directly with David on it. I know there was a conversation about that, but I don’t recall what was stated.”

(b) (7)(C) asked CALVOSA to describe her involvement in preparing the House and Senate responses. CALVOSA provided the following response:

“I was involved in seeing the letters that came through, and I was involved in making my recommendations to what was drafted, and handing it over to David [BRAY], and OCH [Office of the Chairman] made the final decision on what was there. David [BRAY] in ITC was the final decision maker for IT’s response. The IT leadership team – David [BRAY], Tony [SUMMERLIN], (b) (6), Leo [WONG], and maybe (b) (6) or someone else – we all reviewed it.

(b) (7)(C) asked CALVOSA who drafted the first versions. CALVOSA provided the following response:

“I don’t know. Typically it was a combo of Tony [SUMMERLIN] and David [BRAY], but I don’t know in this case.”

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

(b) (7)(C) explained that, after OIG understood (from talking to (b) (6)) the API activity associated with the URL redirect provided by the John Oliver program, OIG started to look at the incident from a different perspective and that (b) (6) told OIG it was common knowledge that all ECFS traffic went through an API. CALVOSA provided the following response:

“I understand that. I wasn’t here for the legacy ECFS system or 2014 incident. I knew that 14-08 [2014 Net Neutrality proceeding] was one of the biggest dockets. We worked to take lessons learned from that, and do the modernization of ECFS including an API for bulk commenting. System is made to be an open system for the public to provide comments on dockets.”

(b) (7)(C) provided copies of the Senate response from June 15, 2017 (attached to this MOI as Exhibit F) and the House response from July 21, 2017 (attached to this MOI as Exhibit G). (b) (7)(C) indicated all of the evidence we have been able to obtain (e.g., email correspondence, (b) (7)(C) alerts, etc.) shows that the event started at 11:30pm. (b) (7)(C) asked CALVOSA if she was aware of any evidence showing that the event started at 11pm as indicated in the Senate and House responses. CALVOSA stated that “I don’t have any.” (b) (7)(C) asked CALVOSA why she believes the Senate and House responses indicated the event started at 11pm, when there is no evidence that this is when the event started. CALVOSA provided the following response:

“When I got back to the office, and was catching up, I was only seeing the email about what the team was seeing in the system to get it back up. I didn’t get into the nitty gritty of what happened during the event. I was still trying to get a full understanding of what happened. I have not done any analysis of what happened. No one else has to my knowledge. My understanding was that were under a bot swarm, and there was no one actually put comments in to the system. That’s what was told to me when I got back from vacation.”

(b) (7)(C) indicated the statement in the Senate response where the Commission states “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.” (b) (7)(C) asked CALVOSA if she was aware of any log analysis. CALVOSA responded “no.”

(b) (7)(C) asked CALVOSA to analyze the logs from her perspective. CALVOSA provided the following response:

“We are now taking a deep dive on understanding what happened maybe 4 hours before the event, what happened during the event, what triggered it, all facets of what were seeing, to a couple days afterward to see if we’re still seeing things come up. Taking time to do an in-depth analysis. What logs it touches, etc. Preparing a report, understand how the application flows, etc, saying this is what we found, how we assessed it, how we did the analysis, to give a good understanding of the level of work done to understand how the system works (entry

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

points, exit points) for someone non-IT savvy to understand how the analysis was done. Probably have to talk to David [BRAY] about what he meant by analysis of logs.”

(b) (7)(C) directed CALVOSA to a statement in the Senate response in which the Commission states that “In addition to the basic findings above, our IT staff found other markers of potential malicious intent.” (b) (7)(C) asked CALVOSA what IT staff found these markers and to describe the markers that were found. CALVOSA responded “No, I’d have to go through my emails to find out.” (b) (7)(C) asked CALVOSA if she was aware of this analysis. CALVOSA responded that “I’d have to go back.”

(b) (7)(C) directed CALVOSA to a statement in the Senate response in which the Commission states that “Later analysis showed the perpetrators requested multiple keys associated with individual IP addresses.” (b) (7)(C) asked CALVOSA to describe the process followed to identify individuals who requested multiple keys. CALVOSA provided the following response:

“As part of the initial observation. I don’t recall if we went back, now that we know how this is happening to us, to know how we needed to scale up. I can’t recall if this was one of the things that we observed.

(b) (7)(C) asked CALVOSA if an effort was made to obtain logs from data.gov (a website run by GSA through which API keys are obtained to provide bulk comments to ECFS using the public API). CALVOSA stated “I don’t.”

(b) (7)(C) directed CALVOSA to the sections of the Senate and House responses addressing FCC discussions with the FBI. (b) (7)(C) asked CALVOSA who at the Commission spoke with the FBI. CALVOSA provided the following response:

“Leo [WONG]. I recall Leo followed up with the FBI, I don’t know if the FBI gave him further guidance. Leo was asked to follow up with FBI. Leo said he talked to the FBI. I asked Leo if we have any action items with the FBI, and he said no.”

(b) (7)(C) asked CALVOSA if it was her understanding that WONG reached a conclusion with the FBI regarding the severity of the event. CALVOSA responded “That’s what I understand. I asked Leo if they were going to write anything down, he said no.”

(b) (7)(C) explained to CALVOSA that OIG has spoken with FBI SA (b) (6) on several occasions related to this matter and that SA (b) (6) indicated to OIG that the FBI wouldn’t reach a conclusion about the severity of the event without looking at the data. (b) (7)(C) explained that he read the section from the Commission’s response to the Senate describing Commission interaction with the FBI and that SA (b) (6) responded “that’s insane” in response to the characterization. (b) (7)(C) explained that SA (b) (6) indicated (b) (6) has no idea about presidential policy directive 41, that it is not the FBI’s role to assess the severity of the event, and that the FBI is only interested in the possibility of criminal activity.

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

(b) (7)(C) provided a copy of the email message sent from WONG to SUMMERLIN on July 5, 2017 at 1358 hours that includes a draft response to the House with the following comment from WONG (attached to this MOI as Exhibit H):

“Sounds like the decision was made jointly which really wasn’t the case. Can we say
“Decision was confirmed later with FBI that the threshold for major incident was indeed not met and no US-CERT incident was necessary.”

(b) (7)(C) indicates that WONG does not appear to agree with the way the conclusion with the FBI is characterized in the draft response (which is largely the way that it is presented in the final response). (b) (7)(C) asked CALVOSA to explain why WONG provided this comment. CALVOSA responded “I don’t know. Did you ask Leo?” (b) (7)(C) stated that we did ask WONG and that WONG “didn’t say much.” (b) (7)(C) explained that WONG “said there was some agreement with FBI about PPD41” and that OIG explained to WONG that the FBI disagreed.

(b) (7)(C) provided an email chain beginning on November 8, 2017, at 0740 hours in which OIG was attempting to obtain information on the amount of API activity generated by the URL redirect created by the John Oliver program (attached to this MOI as Exhibit I). (b) (7)(C) explained that, after OIG spoke with (b) (6), OIG wanted to determine how much API activity generated by the URL redirect and that OIG initially estimated (b) (7)(E) for each URL redirect. (b) (7)(C) explained that OIG now knows there were API calls, but that OIG was working to get an exact number from ITC. OIG was told that in order to obtain the accurate data, the system would have to be restored to May 7th and that restoring the system would be burdensome. (b) (7)(C) showed CALVOSA that, at the same time OIG was advised that system restoration would be burdensome, (b) (6) was working with (b) (6), a contractor with FCC IT, to perform the testing and that the testing results were obtained on the same day OIG advised FCC IT not to perform the restoration. (b) (7)(C) showed CALVOSA the email message from November 13th in which CALVOSA, after being provided the testing results, stated that “(b) (7)(C) has not requested a follow up for this item, therefore, we will not follow up.” (b) (7)(C) asked CALVOSA why the test results were not provided. CALVOSA provided the following response:

“I dissected (b) (7) email, and make sure we answered them. When I got back in the office, I made it clear to the team that we’re going to answer all of your questions. We had multiple threads going on, I wanted to keep the answers specific to the questions from particular threads. I wanted to make sure we were answering your questions. When I got involved, I took all your emails that the team was answering your question, if we didn’t follow up on this, I thought we might have followed up on a question in another thread.”

Case Number: OIG-I-17-0011	Case Title: ECFS DDoS Attacks
-------------------------------	----------------------------------

MEMORANDUM OF INTERVIEW (continuation sheet)

(b) (7)(C) asked CALVOSA to describe the ECFS development process, efforts to modernize ECFS, and her understanding of ECFS operation. CALVOSA provided the following response:

“I didn’t know the intricacies of how ECFS was built. Both people who built ECFS are no longer here. I don’t have a deep dive. I know the data flow of how people come in [comments come into ECFS] and how we make it [comments] available. The initial developer was someone who went off to school and the other developer transitioned to the NCI development team [CALVOSA was unable to recall the names of the developers]. The development process and ECFS modernization effort involved many bureaus OCH, CGB, etc.. At that point I was not involved in the requirements for the system. I never had that level of detail.”

(b) (7)(C) asked CALVOSA to discuss ECFS resiliency, lessons learned from the May 7th incident, and why she didn’t look further into the cause of the May 7th incident. CALVOSA provided the following response:

“This incident helped us how to scale, how to enhance availability. We’ve made leaps and strides in making the system available, and being prepared for another RIF. Make the system more resilient.”

Interview ended around 2:45pm.

TABLE OF EXHIBITS:

Exhibit No.:	Document Type(s):	Subject / Description:	Date:	Bates Range:
A	Kalkines	Signed Kalkines Warning from CALVOSA	5/3/2018	001 - 002
B	Press Release	Press Release from May 8, 2017	5/8/2017	003 - 004
C	Email	Bray provides an explanation of May 7 th event to BERRY	5/8/2017	005 - 006
D	Email Chain	BERRY asks BRAY about John Oliver program	5/8/2017	007 - 009
E	Email	SUMMERLIN comments on misunderstanding	7/12/2017	010 - 011
F	Letter	Response to Senate inquiry	6/15/2017	012 - 017
G	Letter	Response to House inquiry	7/21/2017	018 - 021
H	Email	WONG and SUMMERLIN edit Congressional Response	7/5/2017	022 - 025
I	Email Chain	(b) (7)(C) asks (b) (6) about ECFS API	11/8/2017	026 - 050

Case Number:
OIG-I-17-0011

Case Title:
ECFS DDoS Attacks