AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

EXAMINING PRESERVATION OF STATE DEPARTMENT FEDERAL RECORDS

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 13 AND SEPTEMBER 22, 2016

Serial No. 114–161

Printed for the use of the Committee on Oversight and Government Reform



Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

26–120 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

JENNIFER HEMINGWAY, *Staff Director*
ANDREW DOCKHAM, *General Counsel*
TRISTAN LEAVITT, *Senior Counsel*
LIAM MCKENNA, *Senior Counsel*
SHARON CASEY, *Deputy Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

Page

Hearing held on September 13, 2016 1

WITNESSES

Mr. Bryan Pagliano, reflected in the record as not present
Mr. Justin Cooper
Oral Statement 10
Mr. Bill Thornton, Platte River Networks
Oral Statement 10
Mr. Paul Combetta, Platte River Networks
Oral Statement 10
Hearing Continuation held on September 22, 2016 53

APPENDIX

Letter of September 21, 2016, from Mr. MacDougall representing Mr. Pagliano submitted by Mr. Cummings 55

EXAMINING PRESERVATION OF STATE DEPARTMENT FEDERAL RECORDS

Tuesday, September 13, 2016

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The committee met, pursuant to call, at 10:01 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Mica, Turner, Duncan, Jordan, Walberg, Amash, Gosar, Gowdy, Farenthold, Lummis, Massie, Meadows, DeSantis, Mulvaney, Buck, Walker, Blum, Hice, Russell, Carter, Grothman, Hurd, Palmer, Cummings, Maloney, Norton, Lynch, Cooper, Kelly, Lieu, DeSaulnier, Welch, and Lujan Grisham.

Also Present: Representative Smith of Texas.

Chairman CHAFFETZ. The Committee on Oversight and Government Reform will come to order and without objection the chair is authorized to declare a recess at any time.

This is a very important hearing that we are having, examining the preservation of State Department Federal records. As we know now, Hillary Clinton, as Secretary of State for nearly 4 years, or roughly 4 years, helped create one of what is reported to be one of the biggest security breaches in the history of the State Department. It is an absolute mess. We have witnesses here that are vital to our understanding of the problem, how we got into this mess and how we are potentially going to clean it up.

Joining us will be Mr. Justin Cooper, a former employee of President Bill Clinton and the Clinton Foundation. Mr. Cooper purchased the first server used by Secretary Clinton and had it installed in the basement of her private residence in Chappaqua, New York. He also registered the email domain, clintonemail.com in 2009 on the same day that Secretary Clinton's confirmation hearings began in the United States Senate.

Mr. Cooper has described his role in managing Secretary Clinton's private server as the quote, "customer service face," end quote. He explained to the FBI he helped Secretary Clinton set up her mobile devices, and when she finished with them, he would break them in half or destroy them with a hammer.

Interesting, Mr. Cooper was never employed by the State Department while he managed the server she used to conduct the business of the government.

When Mr. Cooper needed upgrading to the server for a better service. He turned to Mr. Bryan Pagliano. Mr. Pagliano had

worked for Secretary Clinton's 2008 Presidential campaign and was in the process of closing out the campaign's IT assets when Mr. Cooper called to discuss a new server for the Secretary. To put that new server together, Mr. Pagliano used one from her campaign. Anything else he needed was evidently bought off-the-shelf. And then in March of 2009, Mr. Pagliano and Mr. Cooper met in the Clinton's home in Chappaqua, New York, and installed the new server, reportedly in the basement. Unlike Mr. Cooper, Mr. Pagliano then went on to become a State Department employee.

Just a few months after installing the server, Mr. Pagliano was hired at the State Department as a GS–15 Schedule C. Public reports suggest Mr. Pagliano received a State Department check, and he was paid by the Clintons, none of which he reported on his public disclosure forms as required. In a recent Office of Inspector General report, Mr. Pagliano's supervisors at the State Department, quote, "questioned whether he could support a private client during work hours given his capacity as a full-time government employee," end quote. Mr. Pagliano left the State Department in February of 2013, just as Hillary Clinton, Secretary Clinton left.

When responsibility for the server is turned over—when left—when the responsibility for the server is turned over to our next two witnesses, things started to get a little bit more complicated. Mr. Bill Thornton and Mr. Paul Combetta both worked for Platte River Networks. Platte River was hired by Secretary Clinton in early 2013 to host the email server after Mr. Pagliano had been working on it. PRN, or Platte River Networks, migrated Secretary Clinton's emails on the Pagliano-managed server to its own server, which was located at a data center in Secaucus, New Jersey. Things with Platte River Networks get complicated in March of 2015 according to the FBI report.

In early March 2015, The New York Times revealed Secretary Clinton used a private email account while at the State Department. The House Select Committee on Benghazi sends both a preservation request and a subpoena following the news. According to the FBI report, that preservation request is forwarded to PRN or Platte River Networks by Cheryl Mills, the former Secretary Clinton's chief of staff and current attorney.

In his first interview with the FBI, evidently, Mr. Combetta had no memory of that request. In a subsequent interview, he not only remembered the request, but stated he understood it meant not to delete any of Secretary Clinton's emails. Then around the end of March, a number of things happened. There's a conference call between Platte River Networks, Cheryl Mills and David Kendall, another one of Secretary Clinton's private attorneys. Then once again, Mr. Combetta's story changes.

In his first FBI interview, he says he deleted no emails of Secretary Clinton around that time, but later on, he states he not only deleted the archive of Secretary Clinton's email on the server, but also used a product called BleachBit to delete her PST files on the server. At the same time, a number of manual deletions were made on the backups of that Platte River Networks server.

We appreciate the witnesses that are here today and we hope they can illuminate the situation, allow us to better understand it. Because, as I said before, this is one of the biggest breaches of se-

curity in the history of the State Department. We have a duty and an obligation to investigate it. I now recognize the ranking member, Mr. Cummings, for his opening statement.

Mr. CUMMINGS. Thank you very much, Mr. Chairman. Today is our third, third emergency hearing about Secretary Clinton's emails in 4 business days; third in 4 days. Emergency. I believe this committee is abusing taxpayer dollars and the authority of Congress in an astonishing onslaught of political attacks to damage Secretary Clinton's campaign for President of the United States of America.

This is the first time in my 20 years in Congress that I personally witnessed the oversight power of this committee abuse in such a transparently political manner to directly influence a Presidential campaign.

The point of today's hearing is to investigate baseless Republican accusations that Secretary Clinton or her aides ordered the destruction of emails to conceal them from investigators. The most important fact for today's hearing is that the FBI already investigated these accusations and thoroughly debunked them. They interviewed witnesses, examined forensic evidence and concluded that these accusations have no merit. FBI Director Comey stated, and I quote, "We found no evidence that any of the additional work-related emails were intentionally deleted in an effort to conceal them," end of quote.

He went on to say that, quote, "We did not find any evidence of evil intent," and intent to—"or intent to obstruct justice."

Now, that's the FBI Director, the man who had been a lifelong Republican, a man who was applauded by the Republicans as one of the most honorable public servants that ever existed. So he went on and he emphasized in a memo to staff just last week, and I quote, "The case itself was not a cliffhanger," end of quote. Of course, the Republicans did not like the answers that the FBI Director gave. So they simply manufactured today's hearing out of thin air. This entire hearing is a contrived campaign photo op.

Here is the playbook the Republicans are using. Step one, publicly accuse the witnesses of criminal activity no matter how ludicrous, and then refer them to U.S. Attorneys' Office for criminal investigation. That's step one.

Step two, the next day, invite these same witnesses to an emergency hearing on those criminal accusations and then rush to issue a flurry of unilateral subpoenas demanding that they testify. No debate, no vote.

Step three, express false outrage when these witnesses—this is the playbook—express false outrage when these witnesses who you just accused of criminal activity take advice from their counsel to assert their Fifth Amendment right not to testify. There you have it. Presto, instant photo op.

That is what happened to Mr. Combetta and Mr. Thornton despite the fact that a team of career law enforcement agents at the FBI just unanimously recommended against bringing any criminal charges in this case.

Keep in mind that Director Comey said that this was an all-star group of FBI agents, an all-star group of FBI agents said unanimously that these gentlemen should not be charged.

Then there's Bryan Pagliano, the IT specialist who worked on Secretary Clinton's email system. Mr. Pagliano has already been interviewed by the FBI and the FBI provided us with the results of his interview. But the Republicans disagree with the FBI's conclusions. So here we are. Mr. Pagliano has already asserted his Fifth Amendment rights before this Congress. He did this when Chairman Gowdy issued his own unilateral subpoena to force him to appear before the Benghazi Committee on the same issue. Of course, I sat as the ranking member on that select committee.

Obviously, Mr. Pagliano was concerned about the criminal accusations that Republicans are making—were making, so his attorney advised him to assert the Fifth Amendment. There's no legitimate reason for Republicans to force Mr. Pagliano to appear yet again before Congress just to assert his Fifth Amendment rights one more time. How many times will Republicans do this? Will they force him to take the Fifth in front of the Science Committee next? How about the Homeland Security or Intelligence Committee? Should we have them go to those committees too? This is an absolute abuse of authority.

Now, Chairman Gowdy and I disagree about many things, but I give him full credit for one thing that he did. At least when he subpoenaed Mr. Pagliano, he did it in a private session. He did not force Mr. Pagliano to assert the Fifth and probably just to humiliate him, and I respect Mr. Gowdy for that.

Let me say this as plainly as I can. If this committee's goal were just to get Mr. Pagliano or other witnesses on the record asserting their Fifth Amendment rights, we could do that easily in a private session just like Mr. Gowdy did with Mr. Pagliano a year ago. There's no legitimate reason to force Mr. Pagliano or the other witnesses who were subpoenaed for this hearing to assert the Fifth in open session. There's only an illegitimate reason, to get a photo op that Republicans think could harm Secretary Clinton's Presidential campaign.

Finally, some may argue that Mr. Pagliano, or Mr. Combetta should testify before us because they received limited use of immunity for their statements to the FBI. But no lawyers worth their salt are going to let their clients testify before a congressional committee whose chairman just sent another referral for criminal prosecution, no matter how frivolous accusations are. They are just not going to do it. Pursuing these kinds of blatantly political attacks undermines the integrity of our committee, the congressional process, and the constitutional rights that are supposed to protect our citizens against unsubstantiated accusations just like these.

And so with that, Mr. Chairman, I yield back and I thank you.

Chairman CHAFFETZ. We will hold the record open for 5 legislative days for any members who would like to submit a written statement. I would also ask unanimous consent to allow Lamar Smith, the chairman of Science, Space, and Technology Committee, to join our committee and would be happy to also entertain a request for a UC from the Democratic side if they would like to join us as well.

Without objection, so ordered to allow Mr. Smith to join us today.

We would now like to recognize our witnesses. I do note the absence of Mr. Pagliano. Let me address that.

Let the record reflect that Mr. Pagliano is not present at the witness table. The committee invited Mr. Pagliano to testify at the hearing in a letter dated September 7, 2016. Mr. Pagliano informed the committee through his attorneys that he might assert his Fifth Amendment privilege. And I authorized a subpoena for Mr. Pagliano's testimony. On September 8, 2016, the committee transmitted a subpoena to Mr. Pagliano's attorney and the subpoena required his presence here today.

Mr. Pagliano is uniquely qualified to provide testimony that will help the committee better understand Secretary Clinton's use of a private email server during her tenure as Secretary at the State Department among other things. The committee invited him to appear with the expectation that his testimony will advance the committee's investigation, which seeks further information about the setup and management of Secretary Clinton's account and other technical aspects of the account.

I take my responsibility as the committee chairman seriously, especially the decision to issue a subpoena. It is a serious matter and Mr. Pagliano has chosen to evade a subpoena duly issued by a committee of the United States House of Representatives. I will consult with counsel and my colleagues on the committee to consider a full range of options available to address Mr. Pagliano's failure to appear. It is vital to hear from us, because it is our understanding that while Mr. Pagliano worked in the IT department at the State Department for nearly 4 years, virtually every single email that Mr. Pagliano had has suddenly disappeared. There's something like less than 20 emails—this is the guy who worked in the IT department at the State Department. #thingsthatmakeyougohmm. Really? All of his emails have suddenly disappeared.

Mr. Pagliano is also important because he was receiving a paycheck from the Clintons, but failed to disclose that on his financial forms. We would like to give him an opportunity to answer that question.

We also believe that he entered into an immunity agreement. You'd think somebody would sing like a songbird if you got immunity from the FBI. What are you afraid of? We wanted to hear from him. That's why we issued a subpoena. There are a number of things we would like to ask him and he should be here. When you are served a subpoena from the United States Congress, it is not optional. That is not an optional activity, and he is not here today.

Mr. CUMMINGS. Mr. Chairman.

Chairman CHAFFETZ. Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Mr. Chairman. Last night—well, let's make sure that we have a complete picture here. Last night the chairman sent another letter to Mr. Pagliano saying that our committee might go into executive session to accept his Fifth Amendment assertion.

Chairman CHAFFETZ. No, I did not say that.

Mr. CUMMINGS. Well, what did you say?

Chairman CHAFFETZ. I want this committee to be open and transparent. We do things as everything we can possibly do out in the open. That is the American way. That's the way this committee is going to be run.

Mr. CUMMINGS. Will the chairman yield?

Chairman CHAFFETZ. Yes, sir.

Mr. CUMMINGS. It's my understanding that Mr. Pagliano, his lawyers sent a letter saying that they felt that this was abusive process, and nothing but to embarrass him. And he said that if you wanted to go into executive session to give him immunity, he'd be happy to appear. I just want the committee to have the full rep of what happened here. He said would be happy to appear. And so is there—so I take it that the consultation that you are going to do is going to go into whether or not we are going to give him immunity, whether or not we are going to go into executive session, and when do we expect those decisions?

Chairman CHAFFETZ. Well, he made the decision not to be here and there are consequences for that. Okay. This is, again, the integrity of the House of Representatives. This is not an optional activity. You don't just get to say, hey, well, you know, I decided not to do that. So we will look at the full range of options, but if anybody is under any illusion that I'm going to let go of this and just let it sail off into the sunset, they are very ill-advised.

Mr. CUMMINGS. Will the chairman yield?

Chairman CHAFFETZ. Yes.

Mr. CUMMINGS. Looking at your letter dated September 12, 2016, to Mark J. MacDougall. You say here in the letter, and I quote, "The committee requires Mr. Pagliano's appearance because, among other reasons, the possibility that he will waive or choose not to assert the privilege as to some or all questions, the possibility that the committee will agree to hear his testimony in executive session and the possibility that the committee will immunize his testimony pursuant to 18 U.S.C. Section 6005."

That's what I was inquiring about, Mr. Chairman. That's your letter.

Chairman CHAFFETZ. And to clarify——

Mr. CUMMINGS. Yeah.

Chairman CHAFFETZ. —it requires his presence to have those types of discussions. So when he doesn't show up, that option is off the table. It's—you have to be here to have that discussion.

Mr. MICA. Mr. Chairman. Just a point of parliamentary inquiry. You said that it is not an option for the witness who's refused to testify. He was duly presented and served with a subpoena from this committee. Is that correct?

Chairman CHAFFETZ. Yes.

Mr. MICA. And one of the options would be possible contempt of Congress, among the options that we have available. And at what point would that be appropriate to consider the options, in a future hearing or a request to the chair?

Chairman CHAFFETZ. We will consider all options. I would like to continue on with this hearing, given the three witnesses that are here. They are here, and rather than unduly delay the rest of this hearing dealing with Mr. Pagliano, we will complete this hearing and then look at the options.

Mr. MICA. Thank you, Mr. Chairman.

Mr. CUMMINGS. Just one thing, Mr. Chairman. Are we going to do that after the hearing? What you just said you were going to do?

Chairman CHAFFETZ. We are going to consider the options given that Mr. Pagliano is not in attendance after he was issued a subpoena. We will deal with that after the conclusion.

Mr. CUMMINGS. And one of those things that we might consider is going into executive session since Mr. Pagliano said he would be happy to come in executive session. Would that be one of the things?

Chairman CHAFFETZ. I will entertain all of the potential requests. But I'm telling you, I have no intention of going into executive session when he thumbs his nose at the United States Congress, wastes this committee's time, U.S. marshals having to serve subpoenas and for him not to show. That is just not acceptable.

Mr. LYNCH. Mr. Chairman, on a point of order.

Chairman CHAFFETZ. Yes.

Mr. LYNCH. I just want to understand this as well as I can.

Did the chairman issue a criminal referral on Mr. Pagliano?

Chairman CHAFFETZ. We—when we heard that the FBI had not looked at anything that that Secretary Clinton had testified under oath before Congress, we did give a referral.

Mr. LYNCH. Okay. And that's outstanding? Right? I mean, we——

Chairman CHAFFETZ. We don't know. We don't know.

Mr. LYNCH. Well, you issued it.

Chairman CHAFFETZ. We issued it, but we don't know——

Mr. LYNCH. Here's my point. Here's my point. You issued a criminal referral for an individual, and then you ask him to come in here and testify before Congress. That is—that is——

Chairman CHAFFETZ. Let me clarify.

Mr. LYNCH. This would require him to surrender his Fifth Amendment rights, if he's—you're referring him and putting him under threat of criminal prosecution and then asking him to come in here. That's not fair. And the immunity doesn't cover him, because your referral for criminal prosecution came after the fact and beyond the limited purpose for which he was granted immunity, sir.

Chairman CHAFFETZ. There's no criminal referral on Mr. Pagliano. Did we refer the comments and the issues that Mr. Comey as the Director of the FBI brought up? Absolutely, we did.

Mr. LYNCH. Right. Which he said——

Chairman CHAFFETZ. He said he required—he required us to send that.

Mr. LYNCH. But it puts him at risk. What we have done as a committee and through you on this referral, is put him under threat of criminal prosecution because of the issue that you're investigating. I understand that. I understand that. But it puts him in jeopardy coming before this committee while that criminal referral is in existence. And I'm just saying, he's an American citizen. I know the Constitution gets in the way of this committee sometimes lately.

Chairman CHAFFETZ. If the gentleman will suspend. The gentleman will suspend.

Mr. LYNCH. The gentleman will yield.

Chairman CHAFFETZ. The—to clarify, the referral was to look at Secretary Clinton's testimony before Congress. That was the refer-

ral. Mr. Pagliano, his attendance is required here. There was interaction with Mr. Pagliano with another committee, but that's another committee. You have to bring that up with the other committee. I'm concerned about the integrity of this committee. I think we have done the right thing here. His attendance is required here today. He is not here and we will deal with that afterwards.

We do have Mr. Combetta here.

Mr. GOWDY. Mr. Chairman.

Chairman CHAFFETZ. We do have Mr. Thornton here and we do have Mr. Cooper here.

Mr. GOWDY. Mr. Chairman.

Chairman CHAFFETZ. The gentleman from South Carolina.

Mr. GOWDY. Could I engage with the chair in a colloquy?

Chairman CHAFFETZ. Yes.

Mr. GOWDY. I thought witness Pagliano was granted immunity.

Chairman CHAFFETZ. That's what I have read.

Mr. GOWDY. Well, Congress can't prosecute anyone. So the one entity who can has granted him immunity. I'm trying to figure out what his criminal liability is?

Mr. LYNCH. If the gentleman would yield?

Mr. GOWDY. Well, I was having a colloquy with the chair.

Mr. LYNCH. I understand that, but I have——

Mr. GOWDY. But if you can answer the question, I will be happy to hear from you.

Mr. LYNCH. The FBI granted him limited immunity for the purpose of——

Mr. GOWDY. The FBI didn't grant him immunity. The Department of Justice granted him immunity.

Mr. LYNCH. That's correct. That's correct, for that limited purpose.

Mr. GOWDY. How do you know it was limited use immunity? I haven't seen the immunity agreement.

Chairman CHAFFETZ. Let me also inject here.

Mr. GOWDY. No, I have great respect for Mr. Lynch. I have asked what kind of——

Mr. LYNCH. His attorney, his attorney, Mr. Pagliano's attorney, says in his letter that he was given limited immunity for that purpose.

Mr. GOWDY. Well, that raises another interesting question that I hope the gentleman from Massachusetts will help me figure out, which is, when you have reached an agreement with the government, oftentimes it includes cooperation with other entities within that same government. So I wonder whether the Department of Justice and their proffer or immunity agreement with Mr. Pagliano made it clear that he needed to cooperate with another branch of government? We can't prosecute anyone. Only the Department of Justice can. And they have made it, frankly, crystal clear, they are not prosecuting anyone in this fact pattern. So where's the criminal liability?

Mr. LYNCH. The gentleman has constitutional rights under the Fifth Amendment. Whether they are violated by the FBI, or violated here in Congress——

Mr. GOWDY. Well, but——

Mr. LYNCH. —they are still violated.

Mr. GOWDY. Well, as the gentleman from Massachusetts knows, the Fifth Amendment——

Mr. LYNCH. He cannot be required to be a witness against himself.

Mr. GOWDY. Right, but the Fifth Amendment doesn't protect you from non-incriminating answers.

Mr. LYNCH. Well, we have got a criminal referral here.

Mr. GOWDY. Not on him. He can say his name.

Mr. LYNCH. Sure it is. Sure it is.

Mr. GOWDY. He can say where he works. Every answer doesn't incriminate you.

Mr. LYNCH. It was issued after——

Chairman CHAFFETZ. The gentleman from Massachusetts will suspend. The gentleman from South Carolina, it is his time.

Mr. GOWDY. I was just inquiring of the chair. I thought there an immunity agreement in place between the Department of Justice and this witness. So if he has been immunized, and you can't prosecute anyone for anything, where is the criminal liability to him coming and answering questions, which further assumes that every question you ask is going to expose him to criminal liability? There is no Fifth Amendment privilege against answering non-incriminating questions.

Mr. LYNCH. Will the gentleman yield?

Mr. GOWDY. Sure.

Mr. LYNCH. But he can incriminate himself because we have issued, you know, a criminal referral here.

Mr. GOWDY. He has got immunity.

Mr. LYNCH. He doesn't have immunity. He doesn't have immunity. He doesn't have immunity.

Mr. GOWDY. You haven't seen the immunity agreement.

Mr. LYNCH. I'll answer this—look it, if you want to read it yourself, it's from the gentleman's attorney. He says he has got limited immunity.

Mr. GOWDY. Well, I'm going to need a more reliable source than a criminal defense attorney. I want to read the agreement itself. I want to read the agreement between the Department of Justice and this witness, and whether or not that agreement requires this witness to cooperate with other entities of government. That is commonplace. For them to say you can tell us the truth, but you can't tell Congress, makes no sense. That's all I want.

Chairman CHAFFETZ. Okay. The gentleman will suspend. The committee should also be aware that the committee did send a subpoena to Mr. Pagliano to produce this immunity agreement. That was due today at 10 a.m., and he did not produce that as well. So he was under subpoena to not only have his presence here, but so that everybody on this panel can see this immunity agreement, which he supposedly has in his possession. Those documents were also subpoenaed by the committee, and he did not comply with that as well.

It is the intention of the chair here, we are going to move on. There's a lot to address with Mr. Pagliano. Like I said, we are not letting go of this, but we need to continue with this hearing.

We have Mr. Combetta, Mr. Thornton, Mr. Cooper here, we do appreciate you being here. All witnesses are to be sworn before they testify. So if you will please rise and raise your right hand.

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth and nothing but the truth?

Thank you. You may be seated. Let the record reflect that all witnesses answered in the affirmative.

STATEMENTS OF JUSTIN COOPER; BILL THORNTON, PLATTE RIVER NETWORKS; AND PAUL COMBETTA, PLATTE RIVER NETWORKS

Chairman CHAFFETZ. We have not received any written testimony from today's witnesses. Mr. Combetta, do you intend to make an opening statement?

Mr. COMBETTA. On advice of counsel, I respectfully decline to answer, and I assert my Fifth Amendment privilege.

Chairman CHAFFETZ. Mr. Thornton, do you intend to make an opening statement?

Mr. THORNTON. On the advice of counsel, I respectfully decline to answer and assert my Fifth Amendment constitutional privilege.

Chairman CHAFFETZ. Mr. Cooper, do you intend to make an opening statement?

Mr. COOPER. I have no opening statement.

Chairman CHAFFETZ. Okay. Please, if you all can move the microphone a little tighter, a little closer, it is just hard to hear.

Mr. Combetta, we sent a subpoena to you for your—supposed, we had read that there was an immunity agreement. Mr. Combetta, did you produce your immunity agreement this morning as required under the subpoena?

Mr. COMBETTA. On advice of counsel, I respectfully decline to answer and assert my Fifth Amendment privilege.

Chairman CHAFFETZ. Mr. Combetta, a couple of questions. Senator Johnson last year released a portion of an August 19, 2015 internal communication between two Platte River Networks employees. Here's how it read. Quote, "Wondering how we can sneak an email in now after the fact asking them," meaning them, we read to be the Clinton Executive Services Corporation, "when they told us to cut the backups and have them confirm it for our records. Starting to think this whole thing is really covering up some shady"— and there is an expletive there. "I just think if we have it in writing that they told us to cut the backups then we can go public with our statements saying we've had the backups since day one. Then we were told to trim to 30 days would make us look a whole lot better."

As I understand it, you were one of the two employees assigned at PRN in the Clinton account. Did you send or receive this email?

Mr. COOPER. On advice of counsel, I respectfully decline to answer and assert my Fifth Amendment privilege.

Chairman CHAFFETZ. Mr. Combetta, 2 days after that last email, you wrote on August 21, 2015, to an employee of a third party backup firm called Datto, this is what it said. Quote, "We are trying to tighten down every possible security angle on this customer. It occurs to us that anyone at PRN with access to the data partner

portal, i.e., everyone here, could potentially access, this device via remote web feature. Can we set up either two factor authentication or move this device to a separate partner account or some other method to allow only who we permit on our end to access this device via the Internet," end quote.

If I understand the email correctly, every single employee at PRN could have accessed some of the most highly classified national security information that has ever been breached at the State Department. Can you prove that no other individuals accessed this data or even passed it on to someone else?

Mr. COMBETTA. On advice of counsel, I respectfully refuse to answer and assert my Fifth Amendment privilege.

Chairman CHAFFETZ. One last one here, Mr. Combetta. You are an IT guy who is paid by the Clintons. Generally, IT guys don't erase their client's emails unless they are told to do so. So who told you to delete the emails?

Mr. COMBETTA. On advice of counsel, I respectfully decline to answer and assert my Fifth Amendment privilege.

Chairman CHAFFETZ. Mr. Cummings, do you have any questions?

Mr. CUMMINGS. Yeah. Do you all plan to continue to assert your—Mr. Combetta, Mr. Thornton, do you plan to continue to assert your Fifth Amendment rights? Is that your plan? Is that your plan?

Mr. COMBETTA. On advice of counsel, I respectfully refuse to answer and assert my Fifth Amendment privilege.

Mr. CUMMINGS. And you, Mr. Thornton?

Mr. THORNTON. On the advice of counsel, I respectfully decline to answer and assert my Fifth Amendment constitutional privilege.

Mr. CUMMINGS. I'm not going to have any other questions since it's clear that you are going to—you are taking the Fifth on this. But, and I can understand why you are doing what you are doing. We have had a case here before where answering a question or two we then ended up being in all kinds of litigation as to whether or not you had waived your Fifth Amendment privileges, and so I have nothing further. And I do know that D.C. ethics—there's D.C. ethics opinion that addresses the abuse of witnesses trying to take their Fifth Amendment privileges, and as a lawyer, I'm not going to be a part of that process.

Chairman CHAFFETZ. Mr. Combetta, given that you have indicated that you do not intend to answer any questions, out of respect for your constitutional rights, we will now excuse you from the table. Okay.

Mr. Thornton, yesterday, Chairman Lamar Smith of the House Science, Space, and Technology Committee released an August 13, 2015 letter from Datto to PRN's attorney which said this, and I quote, "We have been following the news reports concerning various investigations related to Secretary Clinton's emails, including Platte River's provision of IT-related services to her. We have some concerns relative to data security. Platte has not enabled encryption at the local device. Given the sensitive high-profile nature of the data which is alleged in press reports to potentially reside on the Datto device, it may be the target of cyber attack from a multitude of highly sophisticated and capable entities or individuals. We believe such an event could place the encrypted"—"the

unencrypted data itself at risk as well as expose both Datto, and Platte River systems to collateral damage. In its current state"—and it goes on, "the device and the data that is stored thereon," and it goes on, "is more vulnerable to"—"is more vulnerable to cyber attack than Datto believes is prudent under the circumstances."

Mr. Thornton, given the vulnerabilities identified by Datto, are you aware of any hacks of PRN's systems?

Mr. THORNTON. On the advice of counsel, I respectfully decline to answer and assert my Fifth Amendment constitutional privilege.

Chairman CHAFFETZ. I would like to just ask you one other question that I can't imagine has any implications on any criminal culpability or anything else. It's just a simple question, yes or no. And we will—if you will answer this one, we will cut you loose here.

Were you interviewed by the FBI?

Mr. THORNTON. On the advice of counsel, I respectfully decline to answer and assert my Fifth Amendment constitutional privilege.

Chairman CHAFFETZ. You can't answer the question about whether or not you were interviewed by the FBI?

Mr. THORNTON. On the advice of counsel, I respectfully decline.

Chairman CHAFFETZ. Mr. Cummings.

Mr. CUMMINGS. Again, and as a member of the bar for 40 years, I'm not going to participate in this. You know, I just think that when we bring witnesses here and we parade them when we could do it in executive session, or whatever, again, I think it would be unethical for me to do that. So I have nothing.

Chairman CHAFFETZ. Given that the witness has indicated he does not intend to answer any questions out of respect for his constitutional rights, we will now excuse Mr. Thornton from the table.

We will recess for 2 minutes while the clerk is able to reset the table. The committee stands in recess.

[Recess.]

Chairman CHAFFETZ. The committee will come to order. As we last left it, there are some serious questions based on the emails about the—here you have some of the most vulnerable secrets in all of the State Department, all of the United States, people put their lives on the line for this country and this data, evidently, is unencrypted, without dual authentication and it begs a lot of questions.

Mr. Cooper, you told the FBI, evidently, that you helped set up Hillary Clinton's—Secretary Clinton's New York and D.C. residences with an iMac, correct?

Mr. COOPER. That is correct.

Chairman CHAFFETZ. So did you set them up or did you set them up with somebody else?

Mr. COOPER. Those were out-of-the-box solutions that were set up prior to her——

Chairman CHAFFETZ. I'm sorry. You've got to move it a little closer. It's just, we're having a hard time.

Mr. COOPER. Those were out-of-the-box solutions that were set up prior to her becoming Secretary of State.

Chairman CHAFFETZ. And where did you set them up?

Mr. COOPER. They were set up in the offices that she used in each of her homes.

Chairman CHAFFETZ. Did that include the SCIF?

Mr. COOPER. At the time they were set up, those rooms were not used as SCIFs.

Chairman CHAFFETZ. Did you ever have to service any of those computers or work on any of those computers?

Mr. COOPER. Over periods of time I did service, some work on those computers.

Chairman CHAFFETZ. You did or did not?

Mr. COOPER. Did work on those computers.

Chairman CHAFFETZ. Including the one in the SCIF?

Mr. COOPER. I don't recall any specific time that I worked on it once they were in the SCIFs.

Chairman CHAFFETZ. So—well, how many did you set up at her home?

Mr. COOPER. There was a computer in her office in each of her homes. I worked in their homes for a period of 15 years and, and certainly, when they were originally set up, they were set up primarily for the use of staff in her homes. And I would use those computers from time to time to print documents. Once they became SCIFs, I don't recall specifically using those computers.

Chairman CHAFFETZ. Or servicing of those?

Mr. COOPER. No.

Chairman CHAFFETZ. Did you have a security clearance at that time?

Mr. COOPER. No, I did not have a security clearance.

Chairman CHAFFETZ. After you left the White House early in—when did you leave the White House?

Mr. COOPER. 2001.

Chairman CHAFFETZ. 2001, did you ever have a security clearance at any level after that?

Mr. COOPER. No, I did not have a security clearance.

Chairman CHAFFETZ. And you had full access to the whole server the entire time that you were working for the Clintons?

Mr. COOPER. Yes, I had access to the server.

Chairman CHAFFETZ. And you have no security clearance?

Mr. COOPER. I have no security clearance.

Chairman CHAFFETZ. You told the FBI that Huma Abedin recommended in the fall of 2008 that you contact Bryan Pagliano to build the new server system. Is that correct?

Mr. COOPER. I spoke with Mr. Pagliano at Ms. Abedin's request in fall 2008. We had an existing server system for President Clinton's staff located in the Clinton's residence. I spoke to Mr. Pagliano as that system had its limitations and we were thinking about expanding it. He had some opportunities using surplus equipment from the Clinton campaign that we could use for President Clinton's office to set up.

Chairman CHAFFETZ. Sir, we got to still move that microphone.

Mr. COOPER. Sorry.

Chairman CHAFFETZ. Just straighten it out and put it right up under there. There you go, a little closer.

Did you—what conversations did you have with Huma Abedin about the setting up of the server?

Mr. COOPER. I don't recall any specific conversations with her about the setting up of the server.

Chairman CHAFFETZ. What about setting up emails?

Mr. COOPER. At some point, I had a conversation with her about setting up an email for Secretary Clinton on the servers.

Chairman CHAFFETZ. What about setting up an email for Huma Abedin on those servers?

Mr. COOPER. As well, I had a conversation about setting up an email address for Huma Abedin.

Chairman CHAFFETZ. And did you set up an email for Huma Abedin?

Mr. COOPER. Yes.

Chairman CHAFFETZ. And did she use that email?

Mr. COOPER. As far I knew, yes.

Chairman CHAFFETZ. What other staff used the Clinton email?

Mr. COOPER. The other staff were all staff members for President Clinton's office.

Chairman CHAFFETZ. So——

Mr. COOPER. Not on the Clinton email domain; on the Clinton——

Chairman CHAFFETZ. Clintonemail.com, to be specific.

Mr. COOPER. There were no other staff that I recall using that domain.

Chairman CHAFFETZ. Just—so who had an email address at Clintonemail.com?

Mr. COOPER. The additional person who had an email address, there was Chelsea Clinton.

Chairman CHAFFETZ. So did you have one?

Mr. COOPER. No.

Chairman CHAFFETZ. So you, Huma Abedin and Secretary Clinton had email addresses there.

Mr. COOPER. I did not have an email address on Clinton email.

Chairman CHAFFETZ. I'm sorry. Okay, so—sorry. Hillary Clinton, Huma Abedin and Chelsea Clinton each had email addresses at that address?

Mr. COOPER. Correct.

Chairman CHAFFETZ. What other computers did you set up in their residence? How many computers did you set up?

Mr. COOPER. The only computers I set in the residence were the two iMacs which you have previously mentioned, and the initial Apple server which came in with support from Apple to set up that server in their household.

Chairman CHAFFETZ. And did you set up anything in Washington, D.C. at her residence there?

Mr. COOPER. As mentioned, one of the two iMacs which you referred to was in Washington, D.C.

Chairman CHAFFETZ. So the other one was in Chappaqua, New York.

Mr. COOPER. Correct.

Chairman CHAFFETZ. Okay. So there's a total of two computers, one in Chappaqua. Why did you set up Clintonemail.com?

Mr. COOPER. Secretary Clinton was transitioning from the Presidential campaign and her Senate role and had been using primarily a BlackBerry for email correspondence. There were limitations to her ability to use that BlackBerry as well as a desire to change her email address because a number of people had received her email address over the course of those activities. So we created,

with a discussion, I believe, with Huma Abedin at the time, what domains might be of interest. We obtained a domain and we added it to the original server used by President Clinton's office for her to use with her BlackBerry at the time. And we set that up in a way where the messages simply came into that server and bounced right to her BlackBerry and were not retained on that Apple server.

Chairman CHAFFETZ. Who paid for these computers?

Mr. COOPER. All of them were paid personally by the Clintons.

Chairman CHAFFETZ. Personally?

Mr. COOPER. Personally.

Chairman CHAFFETZ. And who were you being compensated by?

Mr. COOPER. I was being compensated by the Clintons.

Chairman CHAFFETZ. Just personally, or the Clinton Executive Services, Clinton Foundation? What was it?

Mr. COOPER. At that time I was an employee of both the Clinton family personally and the Clinton Foundation.

Chairman CHAFFETZ. Okay. All right, my time has expired. I will now recognize the ranking member, Mr. Cummings.

Mr. CUMMINGS. Mr. Cooper, the FBI's investigative summary states that the Apple server you helped install in the home of President and Secretary Clinton in 2008 was originally purchased for the purpose of hosting email services for President Clinton's staff. To the best of your knowledge, is that accurate?

Mr. COOPER. Yes, that's accurate.

Mr. CUMMINGS. According to the FBI's summary, the decision was made to keep that server in the Clinton residence. The reason was, and I quote, "Due to concern over ensuring email reliability and a desire to segregate email for President Clinton's various post-Presidency endeavor," end of quote. According to the FBI, the decision was made in January 2009 to switch from the Apple server to a new server. Yet, the FBI investigative summary states that in 2009, quote, "According to Cooper, in or around January of 2009, the decision was made to move to another server because the Apple server was antiquated and users were experiencing problems with email delivery on their BlackBerry devices," end of quote.

Is that accurate?

Mr. COOPER. I would say that there is not a date certain that there was a decision made to switch from one server to the other. In my conversations with Mr. Pagliano, I was aware that the Apple server which we were using was not fully meeting our needs and was not expandable to meet potential future needs of other staff in President Clinton's office joining the server. It also did not have a robust solution to support BlackBerry usage. It is very hard for me to even remember what the technology around BlackBerry was then and how they functioned.

There were more progressive ways to use a BlackBerry. Mr. Pagliano had the expertise to set up a server that had a proper BlackBerry interface with it and that was something that was desired by President Clinton's team. And so over a period of time, as Bryan decommissioned those servers from the campaign, we were able to purchase them from the campaign. He then took time to set them up on his time, either in the campaign offices or his home—I'm not sure of the location—and then delivered them to

Chappaqua, I believe, in around March of 2009, when I physically helped him move them into the space where they were going to reside.

Mr. CUMMINGS. So Secretary Clinton began using that new server for email around March 2009. Is that accurate?

Mr. COOPER. Her connection to that server, I believe, was in March 2009.

Mr. CUMMINGS. The Republicans have a conspiracy theory that Secretary Clinton used the server in her home for email in order to avoid complying with records laws. Representative DeSantis asked Director Comey directly about that theory. He asked, and I quote, "Was the reason she set up her own private server, in your judgment, because she wanted to shield communications with Congress and from the public?"

Now, Mr. Cooper, here is what Director Comey said, and I quote, "I can't say that. Our best information is that she set it up as a matter of convenience. It was an already existing system that her husband had and she decided to have a domain on that system."

Now, do you have any evidence to dispute what the FBI Director Mr. Comey said?

Mr. COOPER. No, I don't have any evidence to dispute that. I believe that Secretary Clinton had a personal email on her BlackBerry and was looking for a new solution to be able to use personal email.

Mr. CUMMINGS. Now, were you ever told that Secretary Clinton used a server in her home to avoid the Federal Records Act.

Mr. COOPER. No, I was never told that.

Mr. CUMMINGS. Were you ever told that Secretary Clinton used the server in her home to avoid the Freedom of Information Act?

Mr. COOPER. No, I was never told that.

Mr. CUMMINGS. Now, Mr. Cooper, I think it would be helpful to walk through exactly what your role was and was not with regard to the production of Secretary Clinton's emails to the State Department and the FBI.

Did you cooperate with the FBI investigation, to the best of your ability?

Mr. COOPER. Yes, I did.

Mr. CUMMINGS. Did you turn over to the FBI any relevant records that were in your possession?

Mr. COOPER. Yes, I turned over records to the FBI.

Mr. CUMMINGS. In mid- to late 2014, Secretary Clinton's attorneys attempted to collect all of Secretary Clinton's work-related files from her tenure at the State Department and turn them over to the State Department.

Mr. Cooper, were you involved in that 2014 document production process?

Mr. COOPER. No, I was not.

Mr. CUMMINGS. Now, did the FBI determine that none of Secretary Clinton's work-related emails were intentionally deleted in an effort to conceal them from investigators.

Do you have any reason to dispute that finding?

Mr. COOPER. I do not have any reason to dispute that finding.

Mr. CUMMINGS. Thank you very much.

Chairman CHAFFETZ. I now recognize the gentleman from Florida, Mr. Mica, for 5 minutes.

Mr. MICA. So Mr. Cooper, you started, again, the whole setup of the first server in 2007, '08, right? And you gave the Clinton domain email address, set that up. Is that correct? That was at the very beginning as she was leaving the campaign, coming into office.

Mr. COOPER. I'm sorry. From my recollection, there was a President Clinton domain set up prior to that point, and the Clinton email domain was set up in January of 2009.

Mr. MICA. In 2009. Okay. At some point when she left, I guess, the private capacity, came into the public, I have some information that at least two of her old mobile devices were destroyed and you took part in that. Is that correct?

Mr. COOPER. I believe you are referring to the FBI report that mentions the two——

Mr. MICA. Yes.

Mr. COOPER. I can't——

Mr. MICA. And did you take part in destroying some of her old mobile devices?

Mr. COOPER. Yes. At some point in time when she was transitioning from one mobile device to the next, we would take the information that was on the old device, back it up, transfer it to the new device——

Mr. MICA. Had you worked with Mr. Pagliano?

Mr. COOPER. I would interface with Mr. Pagliano on this.

Mr. MICA. Did you ever discuss with him how you could destroy a device? Did he participate in destruction of any devices?

Mr. COOPER. I don't recall any conversations of that type.

Mr. MICA. Okay. Are you aware of what happened to his emails? You actually were the one servicing the server for most of the period while she was Secretary of State. Is that correct?

Mr. COOPER. I would categorize it differently. Bryan Pagliano serviced the server.

Mr. MICA. You set it up and he conferred—you conferred with him. You——

Mr. COOPER. Mr. Pagliano set it up. He engineered it and I was the interface between the users, and——

Mr. MICA. Would he have had any emails on those servers, to your knowledge?

Mr. COOPER. No.

Mr. MICA. He wouldn't? And you have no idea what happened to all of his emails?

Mr. COOPER. I certainly do not.

Mr. MICA. You also were made aware on two—or made aware on two occasions to Secret Service, I think January 2011, that someone was trying to hack the system. Is that correct?

Mr. COOPER. I used that word colloquially to describe what was a series of false logins on the server.

Mr. MICA. And not once, but twice, and then you closed down the system briefly to deal with the situation?

Mr. COOPER. Correct.

Mr. MICA. When were you first contacted by the FBI?

Mr. COOPER. I believe it was August of last summer.

Mr. MICA. And was that the first time you sat down with them, or was that later?

Mr. COOPER. Yes.

Mr. MICA. That was your first interview?

Mr. COOPER. Yes.

Mr. MICA. How many times were you interviewed?

Mr. COOPER. Three times.

Mr. MICA. And could you give us the approximate dates? Last summer was the first, and then subsequent——

Mr. COOPER. Last summer, subsequently in the fall, and this spring, I believe.

Mr. MICA. Were you ever offered any type of immunity agreement by the Department of Justice?

Mr. COOPER. I was not.

Mr. MICA. How long have you been represented by your current counsel?

Mr. COOPER. Since the beginning of—since I was first contacted by the FBI.

Mr. MICA. And, again, you have explained that it was the Clintons who paid for your counsel up to that time and the organization that was set up by the Clintons?

Mr. COOPER. I'm the only person who's paid for my counsel.

Mr. MICA. You paid for your own expenses? They have not paid for any?

Mr. COOPER. Correct.

Mr. MICA. Have you had any kind of a joint defense agreement with any other individual involved in the FBI's investigation?

Mr. COOPER. I have no such agreement.

Mr. MICA. No such agreement.

Finally, you stepped back from the day-to-day activities with the Clintons about the time of the transition. Is that correct, as she left office?

Mr. COOPER. Yes.

Mr. MICA. And Pagliano took over?

Mr. COOPER. Yes.

Mr. MICA. And you were also responsible for the transfer—helping with the transfer. In fact, you walked her aide, Hanley, over the phone through taking the information that they had in emails and archiving it. Is that correct?

Mr. COOPER. At one point, I assisted Monica Hanley in setting up a laptop computer so that she could create an offline archive of the emails that were on the server.

Mr. MICA. And to your knowledge, was everything——

Mr. COOPER. I do not know the outcome of that.

Mr. MICA. You don't know if they were. And do you know, finally, was there any deletion, or attempts for—to delete any information that had been stored that was going to be transferred and archived?

Mr. COOPER. I have no knowledge of that.

Mr. MICA. I thank you.

Chairman CHAFFETZ. I now recognize the gentlewoman from the District of Columbia, Ms. Norton, for 5 minutes.

Ms. NORTON. Thank you, Mr. Chairman. The FBI report for the average American put the matter involving Ms. Clinton's emails to

rest for the average person. The FBI was a tough report, and yet, you could take kernels, and that's what happened here, and I want to ask you, Mr. Kernel—Mr. Cooper, about one of those kernels. One of the most venal of the conspiracy theories to come forward out of that report follows on from some testimony you gave. The report quotes you, and I take it you were under oath before the FBI?

Mr. COOPER. I'm sorry, I was not under oath.

Ms. NORTON. Well, it says you advised that you sometimes assisted users, including Clinton. I'm now quoting report—"when they obtained a new mobile device by helping them back up the data from the old device before transferring it to the new device and syncing the new device with"— Clinton—"with the Clinton server."

Mr. COOPER. That's correct.

Ms. NORTON. That quote is correct. Then the summary describes two instances—and here is where the conspiracy theories have been acted out both in this House, and in Presidential campaign—that you recall two instances where you destroyed old mobile devices with a hammer. And Mr. Trump claimed that who would do that if they didn't have anything to hide. And Representative DeSantis picked up than rhetoric and said, it obviously shows intent to hide something.

Mr. Cooper, I'd like to directly ask you about the destruction of those BlackBerrys.

Was your purpose in destroying the old BlackBerry device ever to hide Secretary Clinton's emails from being saved or disclosed from Federal Records Laws?

Mr. COOPER. Congresswoman, no, it is not in any way to destroy or hide any information at all. I couldn't speak to whether there were records on there that needed to be or should be considered Federal records. In fact, the opposite would be the case, in that I was going out of my way to preserve all of the information that was on those devices, transfer them to the new devices and make sure the server loaded on them.

Ms. NORTON. Well, that was going to be my question. Before you destroyed them, from one BlackBerry to another, did you transition the very same emails from the old BlackBerry to the new one?

Mr. COOPER. It is a combination of the backup procedure and the procedure of activating the new device. All of the information from the previous device would have ended up on the new device before we went and deleted using the BlackBerry tools to wipe the old device.

Ms. NORTON. So that would mean, would it not, or did it mean that you copied the content, total content——

Mr. COOPER. It means that——

Ms. NORTON. —of the Secretary's device, saved it and loaded it onto a new device so you had the exact same thing onto the new device?

Mr. COOPER. That is correct.

Ms. NORTON. During the course of the FBI's investigation, did you realize that you still had retained the extra copy of the content of those old BlackBerry devices on your own machine, and did you provide that information to the FBI?

Mr. COOPER. In preparing to meet with the FBI and examining my files related to the server, I did describe some files that may have contained content related to this.

I turned that content over to my attorneys who have worked with the FBI and Department of Justice on capturing that material for their possession.

Ms. NORTON. So I take it that that was to make the case that you do not intend to destroy the BlackBerrys to hide anything.

Mr. COOPER. That is correct.

Ms. NORTON. And now the FBI has the information that was on every single BlackBerry, including that last BlackBerry.

Mr. COOPER. Certainly, they have the information for the ones that I had backup files on.

Ms. NORTON. And, in any case, it's from one BlackBerry to another BlackBerry with nothing lost in between.

Mr. COOPER. Correct.

Ms. NORTON. Thank you very much, Mr. Chairman.

Chairman CHAFFETZ. I now recognize the gentleman from Tennessee, Mr. Duncan, for 5 minutes.

Mr. DUNCAN. Thank you very much, Mr. Chairman.

Mr. Cooper, do you have an IT background or do you consider yourself to be an expert in the IT field?

Mr. COOPER. No, I do not consider myself to be an expert.

Mr. DUNCAN. Do you think the State Department should have had someone more qualified than you to oversee and protect Secretary Clinton's server from hackers?

Mr. COOPER. I was not working for the State Department. And I believe the server to be—again, it was primarily used by President Clinton's office. Secretary Clinton had what I believe was a personal account on that server. I'm not in a position to talk about what the role of the government is in protecting that sort of information.

Mr. DUNCAN. On Sunday, January 9, 2011, at 2:57 a.m., 2:57 in the morning, you sent an email to Secretary Clinton's top aide, Huma Abedin, explaining that you had to shut down Secretary Clinton's server due to someone trying to hack it.

How many times did you personally have to shut down the server to prevent it from being hacked?

Mr. COOPER. Again, it's the server that contained both Secretary Clinton's and also President Clinton's office on there. This was an attempt—a series of failed log-on attempts, which were brought to my attention by an alert we had on the system.

One of the ways to stop that in the early operations of the server was to shut down the server for a period of time so that the attacks would cease. We would then over time develop more sophisticated ways, at the direction of Mr. Pagliano, to help to filter those sorts of failed log-in attempts.

Mr. DUNCAN. Do you know whether powering down a server is the typical way in the IT community to protect against hacks?

Mr. COOPER. I can't speak to that.

Mr. DUNCAN. Do you know what a brute-force attack is?

Mr. COOPER. Yes. A brute-force attack, from my understanding, is a series of high-frequency failed log-in or attempted log-ins using a variety of usernames and passwords.

Mr. DUNCAN. How many brute-force attacks did you observe on the Clintons' server?

Mr. COOPER. I can't say with any specificity how many had happened. They happened with some limited frequency over the period of, I'd say, the last 2–1/2 years while she was in office, but we had developed systems to tamper these down.

Mr. DUNCAN. They occurred with frequency?

Mr. COOPER. Some frequency.

Mr. DUNCAN. All right. I yield my remaining time back to the chairman.

Chairman CHAFFETZ. Mr. Cooper, how many people had access to this server?

Mr. COOPER. In terms of its administrators?

Chairman CHAFFETZ. I want the whole universe—administrators, users, the whole gamut.

Mr. COOPER. There were two people who had some administrative rights, which was myself and Mr. Pagliano. I can't off the top of my head tell you exactly how many users there were over the lifetime of the server, but it was less than 20 people.

Chairman CHAFFETZ. Was there remote access log-in available?

Mr. COOPER. The only remote access log-in to the server was for myself and Mr. Pagliano.

Chairman CHAFFETZ. Was it encrypted?

Mr. COOPER. I can't speak to that. I can't recall.

Chairman CHAFFETZ. So you're running it; you don't even know if it was encrypted?

Mr. COOPER. Mr. Pagliano was running it. I was using it.

Chairman CHAFFETZ. Did it have dual authentication?

Mr. COOPER. I don't recall dual authentication.

Chairman CHAFFETZ. So there's no dual authentication. We're not sure it has encryption. It does have remote access. You have some 20-odd people that can do it. It's intermingled with the Clinton Foundation.

Clinton Executive Services, did it also have access to that?

Mr. COOPER. I can't say it's intermingled with the Clinton Foundation. Clinton Executive Services——

Chairman CHAFFETZ. You're being paid by them, right? There were people being paid by the Clinton Foundation that were accessing and using the system, right?

Mr. COOPER. In part. There were individuals who had multiple job responsibilities for multiple entities within the Clinton world, and some people did do work for the Clinton Foundation, yes.

Chairman CHAFFETZ. So did the State Department ever contact you or complain or issue any sort of concern?

Mr. COOPER. No, I did not have any concern or——

Mr. DUNCAN. Mr. Chairman, I have one more question.

Chairman CHAFFETZ. Yes, Mr. Duncan.

Mr. DUNCAN. Mr. Cooper, I understand that in order to make Secretary Clinton's private insecure email server connect with the State Department's much more secure server, the State Department had to lower its own security settings, at least temporarily, to match Secretary Clinton's more insecure security server.

Do you know anything about that, the fact that she had this insecure server?

Mr. COOPER. That is not something I specifically know about. I've read accounts of that in the media, but I have no direct knowledge of that.

Mr. DUNCAN. All right. Thank you very much.

Chairman CHAFFETZ. Thank you.

We'll now recognize the gentleman from Massachusetts, Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman.

Thank you, Mr. Cooper, for being here and your willingness to testify. Appreciate that.

Mr. Cooper, the FBI conducted a yearlong investigation that concluded that—and I'll use Director Comey's own statement here. He said, "We did not find clear evidence that Secretary Clinton or her colleagues intended to violate laws governing the handling of classified information."

And he went on to say that "I do not see evidence that is sufficient to establish that Secretary Clinton or those with whom she corresponded both talked about classified information on email or knew when they did it that they were doing something that was against the law."

Now, I know you're not a computer expert, and that's probably a more appropriate line of questioning for Mr. Pagliano. But in its yearlong investigation, the FBI did have a number of technical computer experts on their team, and they took about a year.

And I want to, again, recite their conclusion. And this is Director Comey again in his testimony before this committee. He said, quote, "With respect to potential computer intrusion by hostile actors, we did not find direct evidence that Secretary Clinton's personal email domain, in its various configurations since 2009, was successfully hacked."

And the FBI investigation summary similarly stated, "The FBI investigation and forensic analysis did not find evidence confirming that Clinton's email server systems were compromised by cyber means."

Do you have any information today, Mr. Cooper, that contradicts the FBI's finding?

Mr. COOPER. I do not have any information that would contradict that finding.

Mr. LYNCH. Okay.

The FBI also interviewed Bryan Pagliano, the IT expert on the server. The FBI's investigative summary describes in some detail what he explained. And it states, quote, "When asked about the maintenance and security of the server system he administered, Pagliano stated there were no security breaches, but he was aware that there were many failed log-in attempts, which he referred to as brute-force attacks," what the gentleman was referring to earlier in his line of questioning.

Mr. Cooper, is that statement that I just read, that quote from Mr. Pagliano in his conversation with the FBI, is that consistent with your recollection?

Mr. COOPER. That is consistent with my recollection.

Mr. LYNCH. Okay.

Did you take any steps to protect the server when there were these failed brute-force, so-called, log-in attempts?

Mr. COOPER. Over time, Mr. Pagliano developed a few different solutions that allowed us to manage them in a variety of ways, from blocking the IP addresses manually and ultimately automatically, as I recall.

Mr. LYNCH. Okay. The FBI summary explains some additional steps that were described. I'm not sure if it was—I think it was Mr. Pagliano who took those steps to improve the security of the server, including establishing secure socket-layer certification for encrypted log-in on March 29th and Internet protocol filtering to block access from would-be hackers.

Is that consistent with your recollection?

Mr. COOPER. That is consistent with my recollection.

Mr. LYNCH. Thank you.

That's all I have, Mr. Chairman. I yield back.

Chairman CHAFFETZ. The gentleman yields back.

We'll now recognize the gentleman from Ohio, Mr. Jordan, for 5 minutes.

Mr. JORDAN. Thank you, Mr. Chairman. I actually had questions for the guys who aren't here, so I want to just walk the committee through a few things.

If we can put up the slide, that would be good.

And this is where the chairman was earlier when Mr. Thornton and Mr. Combetta were here. This is an email we think either from one of those guys—one of those guys sent it and/or received it. And I just want to read this.

Look at the date first, August 2015. A lot of things happened before that date. But, "Wondering how we can sneak an email in now after the fact asking them when they told us to cut the backups and have them confirm it for our records. We're starting to think this whole thing is really covering up a lot of bad stuff."

They wanted something in writing because they knew they were going to get thrown under the bus later on.

And we know that they changed the backup structure, because look at the FBI report, page 18. Cheryl Mills instructed someone—name is redacted—at Platte River Network to modify the email retention policy on Clinton's ClintonMail.com email account. She wanted to get rid of anything after 60 days.

So we know they were instructed to do it; they just wanted something in writing.

Let's just walk through some history here.

From the FBI report, July 2014: At the request of Cheryl Mills, Platte River Network remotely transfers all Hillary Clinton emails to Cheryl Mills' and Heather Samuelson's laptops. These laptops later have BleachBit applied to them, and stuff is deleted.

What happened right before that? What happened right before July 2014? Again, go to the report. Page 15 of the report: During the summer of 2014, Cheryl Mills is given a heads-up by the State Department that there would be a letter coming, requesting all Hillary Rodham Clinton's emails.

Jump forward to December. Cheryl Mills requests Platte River Network change the email retention policy on her account, what I just read.

What happened right before that? What prompted this change? December 2nd, Chairman of the Benghazi Committee Trey Gowdy

sends a letter to David Kendall, says, hey, we just found out about this other account—we didn't know at the time it was the only account—this other account that Hillary Clinton has. We'd like the information, any emails relating to the Benghazi situation from that account. And, of course, right after that, they changed the policy, and Platte River Network is instructed to delete anything after 60 days.

And now we move forward to the amazing month, the one the chairman cited in his opening comments, March 2015.

March 2nd, New York Times reports she's got just this one email account, this private server situation.

March 3rd, Mr. Gowdy sends a preservation letter telling them to preserve everything that might be relevant to our investigation.

March 4th, there's a subpoena.

March 9th, Platte River Network is put on notice about the preservation order.

March 10th, she does her press conference.

And, of course, the important dates, March 25th and March 31st. Those two dates, there are conference calls with Clinton lawyers—Bill Clinton's lawyers and Hillary Clinton's lawyers and Platte River Network's.

And, of course, on the 31st of that month is when they take BleachBit to the whole darn thing and they get rid of everything—they get rid of everything.

So now we have two guys—three guys, one on the front end, Mr. Pagliano, who helped Mr. Cooper set it up, take the Fifth and get immunity, and now we have two guys on the tail end—right?—Mr. Combetta and Mr. Thornton, didn't work for the government, they take the Fifth, and Mr. Combetta, at least, gets immunity.

Go back to the date again, August 2015. These guys are starting to wonder, wow, we don't have anything in writing. We've been given all these instructions—verbally, phone calls, conference calls—all these instructions to change the backup, delete things, erase things, BleachBit things, take hammers to things, all these instructions. We don't have anything in writing. We might be in trouble. And guess what? They are.

That's the story. And that's why it's appropriate, Mr. Cummings, for the chairman to invite them in here today and see if they would finally answer somebody's question.

Mr. Gowdy's just right; he is exactly right. They'll talk to the people who can put them in jail, but they won't talk to Congress. They'll talk to the Justice Department—Mr. Pagliano, Mr. Combetta will talk to the Justice Department, but they won't talk to us. We can't put them in jail. We just want to get answers for the American people, and they won't talk to us.

I've never seen anything like this, Mr. Chairman, where you get—as we talked about yesterday. No regular American can get away with the kind of behavior Secretary Clinton gets away with. Two standards now in the country. And this is what is so wrong, and this is why the hearings you're having and the investigation we're doing is entirely appropriate.

And, with that, I yield back.

Chairman CHAFFETZ. The gentleman yields back.

We'll now recognize the gentleman from Texas, Mr. Farenthold, for 5 minutes.

Mr. FARENTHOLD. Thank you, Mr. Chairman.

Mr. Cooper, thank you for being here and having the courage to testify before us and getting to the truth.

I want to just take a big step back. I'm pretty geeky, and I'm going to ask some geek questions you may or may not be able to answer.

But the server the Clintons had, this wasn't, like, just a personal computer that everybody has that they pick up their email. I've had people go, "Oh, I've got a server in my house. That's how I get email." They think their personal computer is a server.

This is a computer running business-class software that delivered and forwarded and stored email for dozens of people. Is that correct?

Mr. COOPER. Yes, that's correct.

Mr. FARENTHOLD. And are you familiar with many people who have this type of equipment in their home? It's typically something that's in an office. Is that correct?

Mr. COOPER. That's correct.

Mr. FARENTHOLD. Do you know anybody who has a server at their home, besides maybe me?

Mr. COOPER. I'm certainly aware of some people who have servers——

Mr. FARENTHOLD. But it's pretty rare.

Now, are you familiar with what email software was running on the server?

Mr. COOPER. I do not recall specifically what the software was running on either server.

Mr. FARENTHOLD. All right. And you told the chairman that what it was set up to do was an email came and it forwarded it to Mrs. Clinton's BlackBerry. And did it delete it from that server, or did it keep it on that server?

Mr. COOPER. My recollection—and just to be clear, there are two servers that we're speaking about. There was an Apple server in use from approximately June 2008 until——

Mr. FARENTHOLD. Right.

Mr. COOPER. —March 2009. That server, which was originally, again, set up for President Clinton's office staff, had some software on it. I'm sorry, I don't recall the name of what the software packet is on there that administered that ware.

One was a mail client, and one was a tool that was supposed to interface with BlackBerry, but it wasn't BlackBerry's own product.

Mr. FARENTHOLD. So was it secure? Or did it just, like, forward using SMTP——

Mr. COOPER. I can't——

Mr. FARENTHOLD. —like the Verizon-BlackBerry gateway?

Mr. COOPER. I can't speak to the security of what that software was. But I believe, in the case of Secretary Clinton, because she wasn't going to be accessing that email in any other fashion and the focus was transitioning her email address over so people would start to use her new email address, we were simply receiving messages in, not retaining them on that server, and having them automatically forward to her——

Mr. FARENTHOLD. Right. And on the later server, did it do the same thing?

Mr. COOPER. On the later server, it functioned more like what you are probably used to in your day-to-day activity, where there was a mailbox on that server that could be accessed——

Mr. FARENTHOLD. Right. And was it opened up to where you could get your email through that server through POP3 or IMAP or a Web client?

Mr. COOPER. While I don't specifically recall, I believe, depending on the user, we would customize—Bryan would help to customize what ports were open——

Mr. FARENTHOLD. Right.

Mr. COOPER. —based on how that user was accessing——

Mr. FARENTHOLD. And did you require that users picking up their mail remotely use a secure client? Or did they just come in cleartext over the standard SMTP ports——

Mr. COOPER. I can't——

Mr. FARENTHOLD. —the POP reports?

Mr. COOPER. I don't recall what the protocols were.

Mr. FARENTHOLD. All right. So you don't know if there was a requirement to log in with an SSL. So it could potentially have been in cleartext.

All right. Did you turn over the logs and notifications that you received to the FBI, the email—of the brute-force attacks?

Mr. COOPER. I did not turn those over to the FBI. There was an instance where we shared some logs with the United States Secret Service when we were first experiencing failed log-in attempts.

Mr. FARENTHOLD. All right. And so you got a notice when there was a failed log-in attempt, but if somebody doing this brute-force attack, where they just enter a username and throw random passwords at it, if they'd gotten it right, you wouldn't have been notified, would you? You'd have thought maybe it was Mrs.—you would have probably thought it was Mrs. Clinton or some legitimate user actually getting in.

Mr. COOPER. I don't want to suppose, but——

Mr. FARENTHOLD. You only get notices of failed log-in attempts.

Mr. COOPER. Correct.

Mr. FARENTHOLD. You weren't notified every time somebody actually logged in, though there may actually have been a log kept.

Mr. COOPER. Correct.

Mr. FARENTHOLD. So somebody could have gotten in, and you just wouldn't have known it.

And I'm sorry, I don't remember if I asked this, so I'm going to ask again. Was there a firewall between the Internet and this server, a piece of hardware between the server and the Internet?

Mr. COOPER. I believe there was a firewall associated with the Pagliano server, yes.

Mr. FARENTHOLD. All right. And was there one with the Apple server?

Mr. COOPER. I don't recall.

Mr. FARENTHOLD. All right.

And then we talked a little bit about Mrs. Clinton going through a variety of BlackBerrys. Were they all the same version of BlackBerrys, or did she migrate up between—you know, when the new

BlackBerry came out, did she want the latest and greatest BlackBerry?

Mr. COOPER. Again, it's a little bit difficult, I think, for me, at least, to go in a time warp and know the sequences. But BlackBerry was releasing models quite frequently then with very different user interfaces, from trackballs to trackwheels to trackpads.

Mr. FARENTHOLD. I know. I went through that nightmare myself.

Mr. COOPER. And I think over time, you know, she would move to a newer device usually when her older device may have been, you know, a little bit older, a little bit failing.

Mr. FARENTHOLD. And do you know if the security patches were regularly put on all of these servers?

Mr. COOPER. I feel fairly confident that the security patches were updated by Mr. Pagliano.

Mr. FARENTHOLD. I'll tell you, having kept a server in my house for a while, I gave it up and now moved over to an online hosting, because it's next to impossible to keep up with the pace of the security fixes that are coming out.

I see I'm out of time. That happens when I geek out. I yield back.

Chairman CHAFFETZ. Thank you.

We'll now recognize the gentlewoman from Wyoming, Mrs. Lummis, for 5 minutes.

Mrs. LUMMIS. Well, I'm glad that we had a geek-out because I can't do that. I'm a rancher. I'm not as familiar with these technologies.

But I do know this, just as an average American, when it comes to technology: We do know that the Chinese Government hires people to hack by day and that those same hackers hack for hire at night. So there are people who are spending every single day in China, probably Russia, other countries, trying to hack into the computers of U.S. Government officials.

So security's a constant problem in this country, especially for high elected officials or appointed officials. And I do know this: that encryption can be used to help prevent that, that dual-authentication processes can be used to help prevent that kind of hacking.

So, Mr. Cooper, are you telling me that there was no dual authentication, no encryption, and the Secretary of State had no protection of our secrets, when we all know that efforts are being made to hack people just like her in government?

Mr. COOPER. I unfortunately cannot provide you with the details of what the specific security functions were on the server. I know that there were security functions on the server and they evolved over time, essentially as technology evolved over time, and there were different things that were available and considered at different junctures.

I would certainly agree with you that this is something that we should all be concerned with. And I saw this, again, as this was—there's a need to, yes, protect the privacy of individuals in their personal lives using their email.

Mrs. LUMMIS. We also know that—as Members of Congress, we just know that if we travel to a foreign country and we have a device with us, especially to Russia, they tell you to wrap our devices in aluminum foil so there's no transmission. And I've seen televised

examples of Secretary of State Clinton using her electronic devices to communicate while she's running all over the world.

And now that we know that these servers and devices were scattered around in her home and that there was some sort of management of documents in Colorado, how can people like me assure the American people that the information that was on those emails—and that some of which has been destroyed and is not available to us—is not being sifted through even as we speak by Chinese hackers and Russian hackers?

And what security does our country have by virtue of what looks to me like some pretty lackadaisical attitudes towards sensitive data, Top Secret data, Secret data, confidential data?

Mr. COOPER. First, Mrs. Lummis, I'm not an expert in computer security. I understand some of the concerns you've expressed from things I've read in the newspaper, but I have no expertise in that area.

Second, I have no knowledge of the content and cannot verify what the content was on this equipment.

And, third, I also have no specific knowledge in which countries Secretary Clinton chose or did not choose to use her devices.

Mrs. LUMMIS. Mr. Chairman, I yield back.

Chairman CHAFFETZ. And before you yield back, if you'd yield to me for a second.

Mrs. LUMMIS. I yield to the chairman.

Chairman CHAFFETZ. So, Mr. Cooper, A, you get huge brownie points from the committee for showing up and having the guts to actually answer questions. We're very grateful for that. I'm also very grateful for your candid nature in expressing the idea that you don't have the expertise to even answer those questions as thoroughly as possible.

The problem I have—again, I believe you're doing the best you can, at least based on the testimony I've heard thus far. Here's the problem: It's you, Mr. Cooper, with no experience, no dual authentication, no encryption, up against the Chinese and the Russians. Who do you think's going to win that one?

That's what scares the living daylights out of us, is because of the cavalier nature in which this was set up, and some of the Nation's most sensitive and secure information. That's the concern.

We're now going to recognize the gentleman from——

Mr. CUMMINGS. You're not going to let him answer the question?

Chairman CHAFFETZ. It wasn't a question.

We're now going to recognize the gentleman from Vermont, Mr. Welch, for 5 minutes.

Mr. WELCH. Thank you very much. I'll have a few questions and a bit of a statement.

Mr. Chairman, you're a good chairman, doing a great job, but I disagree with you about the excessive, in my view, focus on Hillary Clinton.

I want to give a little perspective here. Legitimate investigation. But we had the FBI, we had Mr. Comey, who has an unimpeachable record of vigilance as a prosecutor, who calls them as he sees them. He went through every single thing, every single email. And he came to the conclusion that there was no criminal conduct,

there was no evidence that, in fact, the Secretary's email had been hacked, and he says it's not even a close call.

So, whether that email should have been set up, the private server—the Secretary's acknowledged that that was a mistake—there's a legitimate basis to inquire as to what happened. But we've done it. And the FBI's done it. And I have a feeling that a little bit of this has to do with something other than the emails, and it may have to do with something that's looming in November.

Now, one of the issues that I have as I listen to many of the questions of my colleagues is that they're essentially asking the witnesses to try to disprove a negative. For instance, my friend from Wyoming was asking about the Russians and the Chinese trying to get into that email. They probably are. They're trying to get into every department we have, probably trying to get into the White House, trying to get into the Department of Defense and the Joint Chiefs of Staff. So that apprehension is well-founded. But there's no way any of us can disprove or prove that they have or haven't gotten into the email of the Secretary of Defense or the Secretary of State or the White House or any of the House accounts.

So the repetition of the question that raises the apprehension that the Chinese or the Russians are making this determined effort to hack into accounts and focusing it all on Hillary Clinton acts as though that intentionality of the Russians and the Chinese doesn't apply across the board to anybody and everybody that's in government or may have access to some information that they'd want.

So talking about Mr. Cooper having the guts to come in here, thank you, Mr. Cooper, but you can't prove or disprove, any more than anyone else can, whether the Russians have successfully penetrated anyone's email account, let alone Secretary Clinton's.

So the whole issue here is a repetition of an initial assertion that somehow, some way, not only did Secretary Clinton make a mistake by having a private server, but that the insinuation is that she actually jeopardized secrets.

And there's a memory gap here, because this committee is the one that had Mr. Comey in here, and he sat here for I don't know how many hours, but he answered every single question that every single member had. And that exhaustive investigation that Mr. Comey and the FBI did demonstrated that there was no evidence of either criminal violation and he found no evidence that the emails had been penetrated.

So that's really the basis upon which a lot of us believe that this committee—and it's a great committee; all of us are proud to serve on it—is playing a role that's beyond oversight and investigation, is kind of advocacy in creating a sense of alarm among the American people as to whether something that is valuable information has been taken.

Do you have any indication, Mr. Cooper, that any secret information has been taken by the Russians, the Chinese, or any other actor?

Mr. COOPER. I have no indication. I'd simply refer you to the FBI report and their findings.

Mr. WELCH. All right. And in all your discussions with your colleagues, has anybody else indicated that they had a shred of evi-

dence that any national security information of the United States was penetrated as a result of the Clinton emails?

Mr. COOPER. I don't even think I've had any conversations to that effect.

Mr. WELCH. All right.

And is it a big deal for people to change their devices—iPads, iPhones, BlackBerrys? Is that somehow a big deal?

Mr. COOPER. I think it's rather commonplace these days.

Mr. WELCH. All right. I thank you, and I yield back.

Thank you, Mr. Chairman.

Chairman CHAFFETZ. Before the gentleman yields back, if I can—I appreciate the kind comments, but let's remember, we got multiple people pleading the Fifth, afraid of criminal wrongdoing. We also have an FBI Director—one of the questions was, did you look at what Secretary Clinton said under oath? There are other equities that we have than the destruction of documents. He said he didn't look at any of that. And so that was also part of his testimony. He didn't even look at that part of it. That's the imperative for us to do our jobs.

But I do appreciate the gentleman's—appreciate him yielding.

We'll now recognize the gentleman from North Carolina, Mr. Meadows, for 5 minutes.

Mr. MEADOWS. Thank you, Mr. Chairman.

Mr. Cooper, thank you for your answers as we look into this further.

You set up a server for the sole reason, as it relates to Ms. Clinton, so that she could use a domain name and have those private emails at her domain name served on that server. Is that correct?

Mr. COOPER. Again, I set up two servers, both with the primary purpose of servicing President Clinton's personal office.

Mr. MEADOWS. Right. But, in servicing Ms. Clinton, you put her domain name to service emails on those servers. Is that——

Mr. COOPER. Correct.

Mr. MEADOWS. Why did you not use another server like 1&1 or any of the other servers that are out there? Why would you not use those?

You know, I have a device that has a domain name that I own that I get emails at, and it's much cheaper for me just to have a server that does that. Why would you not have done that?

Mr. COOPER. First, we had the solution in place, so it was certainly an option. And, considering other options, I think that there were some appeals to this, in that the data was contained in one place. We knew where it was contained. It was physically in a secure location. And I think that some of the tools that you or I may employ today even with a personalized domain were not available at that time.

Mr. MEADOWS. Well, in 2009 they were, because I was using them. And so they were available then.

And so what you're saying is the reason to not have another—you're getting advice from your counsel.

Will you hold the clock for a second?

I guess you all are wanting to talk about——

Mr. SHAPIRO. I'm sorry. Just to turn off the mike so there's no interference.

Mr. MEADOWS. So the other aspect of this, Mr. Cooper, is you made a conscious decision to put her email address on this server to keep it from being viewed by other people that might have a server like 1&1 or anybody else? Is that your testimony?

Mr. COOPER. I'm not sure that I was the decisionmaker. I was someone——

Mr. MEADOWS. Who was? Was it Hillary Clinton?

Mr. COOPER. I was in discussions primarily with Huma Abedin. I don't know if she was the decisionmaker——

Mr. MEADOWS. So your testimony here today is that Huma Abedin said that she would prefer to have Ms. Clinton's email on a private server versus a server that was actually managed by someone else. That's your testimony.

Mr. COOPER. My testimony is that that was communicated to me.

Mr. MEADOWS. Okay. Well, that's illuminating, because if that's the case, what would be the potential reason for having it where you can see it and someone else couldn't see it?

Mr. COOPER. This was, again, a server that was already in existence for the use of President Clinton's office. And I think it provided a convenient and what was intended to be a reliable solution for her personal email.

Mr. MEADOWS. All right.

So how many email addresses did she have?

Mr. COOPER. She primarily used one email address at a time as far——

Mr. MEADOWS. Yeah. How many did she have? Because I notice, in her emails, they have numbers behind it and everything else. So how many different email——

Mr. COOPER. I believe if you count her AT&T email address as one, and then two others on the Clinton domain that I'm aware of.

Mr. MEADOWS. Okay.

And so, as you were managing this, I guess the other concern that I would have is, did you have a BlackBerry exchange server on your server?

Mr. COOPER. Yes, there was.

Mr. MEADOWS. So you had actually the push technology actually on your server.

Mr. COOPER. Correct.

Mr. MEADOWS. So when the discussion between Platte River and the attorneys and all of that happened in March, were you part of that discussion to clean and erase some of those emails from servers?

Mr. COOPER. I was not at all part of those discussions.

Mr. MEADOWS. All right. Is it commonplace when you have a discussion about erasing emails and archived emails to have an attorney on a discussion with a client? Is that common? I mean, I was in a business a long time; it never happened with me.

Mr. COOPER. That's not something that I have the ability to comment on.

Mr. MEADOWS. Well, you have an ability to comment on it. You may choose not to.

Mr. COOPER. I have no opinion on that.

Mr. MEADOWS. Well, have you ever been part of a conversation to erase emails where there's been an attorney there to advise you on the advisability of that? Have you personally?

Mr. COOPER. I have——

Mr. MEADOWS. Yes or no?

Mr. COOPER. I personally have had no experience in that situation.

Mr. MEADOWS. Okay. All right.

So let me finish. You said that you're paying for your attorney's fees here.

Mr. COOPER. Correct.

Mr. MEADOWS. Have you ever been reimbursed or have you ever had any potential reimbursement for fees, for attorney's fees, from anyone other than your own personal accounts?

Mr. COOPER. No.

Mr. MEADOWS. Do you anticipate any reimbursement?

Mr. COOPER. No.

Mr. MEADOWS. All right.

I yield back.

Chairman CHAFFETZ. We'll now go to the gentleman from Georgia, Mr. Hice, for 5 minutes.

Mr. HICE. Thank you, Mr. Chairman.

I want to begin by saying what I think is the feeling of many in this committee today, just how shameful it is that so many of our witnesses are no longer here. And, frankly, the appearance is they could care less about our national security and are less concerned about defending our country than they are in either being absent or pleading the Fifth.

And, as was brought up earlier, they're willing to meet with and talk with others, those who had the potential of prosecuting them. Who knows what possible deals have been made in some of those discussions. But they refuse to meet with us. And it begs the question, what in the world are they hiding?

And so I want to thank you, Mr. Cooper, for your courage and your willingness to be here with us today and to provide some answers. It means a great deal to us.

Did Secretary Clinton at any time have more than one device?

Mr. COOPER. I don't recall specifically her having more than one email device, but I have come to learn that at some point she had some iPad devices that she may have used simultaneously with the BlackBerrys.

Mr. HICE. So there is a possibility she had more than one device at a time?

Mr. COOPER. It's possible.

Mr. HICE. You have referred to yourself many times as not being an IT expert. At any time did you consult cybersecurity experts when you were setting up her initial server?

Mr. COOPER. The initial server, we consulted with Apple and their business solutions program to set up that server. And, of course, later, we consulted with Mr. Pagliano for those purposes.

Mr. HICE. Okay. And from any department or agency in the government, did you consult with at all?

Mr. COOPER. No, no consultation of that type.

Mr. HICE. Okay.

When you referred earlier to some of the hacks that were taking place, the brute force and so forth, with some degree of regularity, did you report those hacks or potential hacks to the FBI or Secret Service or any other agency?

Mr. COOPER. As I mentioned earlier, when we first experienced some of the repeated failed log-in attempts, I reported them to the Secret Service.

Mr. HICE. Okay. Did any of the—do you know if anything was done when it was reported? Did they come to investigate or search anything out?

Mr. COOPER. The Secret Service reviewed some of the logs from the server and made some recommendations to Mr. Pagliano about the possible origins of those failed log-ins and some techniques he might use to mitigate that problem.

Mr. HICE. Did any of the, be it agencies or other cybersecurity experts express any concern over this being a private server or use of private emails?

Mr. COOPER. Not directly to me.

Mr. HICE. Okay. So even when they came and did some investigation and some research, that question was never brought up to you.

Mr. COOPER. Correct.

Mr. HICE. How does BleachBit work? Are you familiar with that?

Mr. COOPER. I'm not familiar with that.

Mr. HICE. Well, it seems to me, Mr. Chairman and Mr. Cooper and everyone in this room and everyone in the country, for that matter, I mean, we know how absolutely dangerous it is, the potential dangers of information getting in the hands of our adversaries, and you've related that that possibility exists dramatically. In fact, Director Comey was right when he said that—I thought he was being very polite when he said this is extremely careless, what has taken place.

And, unfortunately, Mr. Cooper, you're right in the middle of that. As the chairman brought up a while ago, we have nations coming after us, and here you are, standing up as a defense to try to keep security from being leaked out to professionals and countries.

And the words of Director Comey have to be directed to you as well. This has been extremely careless, what's taken place. And your handling, frankly, of the IT infrastructure, even in the midst of admittedly not being an expert in this field, to me, shows absolute disregard for our national security.

And, Mr. Chairman, I'm grateful for your continued commitment to pursue and to try to get to this. And those who refuse to answer our questions and plead the Fifth to protect their own hide as opposed to protecting our national security, again, it's shameful.

But I thank you for pursuing this, Mr. Chairman, and I yield back.

Chairman CHAFFETZ. The gentleman yields back.

We'll now recognize the gentleman from Texas, Mr. Hurd.

Mr. HURD. Thank you, Mr. Chairman.

Mr. Cooper, thank you for being here. I know you've said many times that you're not an expert in computer security, so I won't try to get too detailed.

My first question is, have you ever worked in the Federal Government before?

Mr. COOPER. Yes. I worked in the White House in 2000–2001.

Mr. HURD. Were you involved in handling classified information?

Mr. COOPER. No.

Mr. HURD. Did Mr. Pagliano work for you?

Mr. COOPER. I'm sorry, can you clarify what you mean, "work for me"?

Mr. HURD. So you were responsible for setting up these servers. Is that correct?

Mr. COOPER. I oversaw the setup of these servers.

Mr. HURD. So who was your boss when you were setting up the server?

Mr. COOPER. President Clinton was my boss.

Mr. HURD. And when you set up the servers, you reached out to the services of Mr. Pagliano at some point. Is that correct?

Mr. COOPER. Correct.

Mr. HURD. And so was he your consultant?

Mr. COOPER. Yes, he was a consultant.

Mr. HURD. Was he working at State Department at the time?

Mr. COOPER. At the initial setup, he was not working at the State Department.

Mr. HURD. While he was working at the State Department, was he involved in providing consultative services to your organization?

Mr. COOPER. Yes.

Mr. HURD. Is that normal?

Mr. COOPER. I have no basis to judge that.

Mr. HURD. So, as the person responsible for setting up these servers, did you ever engage a third party to do stuff like technical vulnerability assessments or penetration testing?

Mr. COOPER. I left that responsibility to Mr. Pagliano.

Mr. HURD. And Mr. Pagliano was responsible for these servers from the beginning of the creation of these servers?

Mr. COOPER. He was not responsible for the Apple server. He was responsible from the transition of the Apple server to what we called the Pagliano server and through the duration of the Pagliano server.

Mr. HURD. And so the Pagliano server was backed up to an external hard drive between May 2009 and June 2011. Is that correct?

Mr. COOPER. From my understanding.

Mr. HURD. And we have a report from the FBI that states that you would periodically delete these records maintained in the backup as disk space ran out. Is that correct?

Mr. COOPER. I have no knowledge of how that procedure operated.

Mr. HURD. So you weren't responsible for that part?

Mr. COOPER. Correct.

Mr. HURD. Who was?

Mr. COOPER. Mr. Pagliano.

Mr. HURD. So, when the decision was made to set up an independent server, were you involved in that conversation? I know you were talking about this briefly with my colleague from North Carolina.

Mr. COOPER. Yes.

Mr. HURD. And why was the decision made to not use a commercial service versus doing something yourself?

Mr. COOPER. Again, the initial setup of both servers was in consideration of a small group of users from President Clinton's office. This was a solution that we felt was an appropriate solution that we were trying. As you can tell by the fact that we transitioned pretty quickly from the Apple system to another system, we were moving to a more robust piece of equipment. That——

Mr. HURD. So you've said yourself—at some point, did you raise your hand and say, hey, guys, I don't have the technical expertise to do this, maybe we should have somebody else?

Mr. COOPER. I was never in the position to be the technical expert on either server.

Mr. HURD. So there's been a lot of conversation about whether or not this system has been hacked and brute force, you name it. Has the FBI, to your knowledge, investigated whether there was indeed—was there a forensic investigation on the servers to see whether there was evidence of an attack?

Mr. COOPER. I would refer you to the FBI for that.

Mr. HURD. Were you ever asked questions about this? Did you all do an exhaustive, you know, review of whether or not you had records of data leaving the network? Were you monitoring whether data was leaving the network?

Mr. COOPER. I would refer you to Mr. Pagliano or the FBI for that. I have no knowledge.

Mr. HURD. Were you ever told or did you ever suspect classified information was being emailed to and from the Secretary?

Mr. COOPER. No.

Mr. HURD. Nobody ever brought that up with you or expressed a concern?

Mr. COOPER. No.

Mr. HURD. Interesting.

Do you think that common practices for good cyber hygiene was being used in the development of these servers?

Mr. COOPER. I'm not wholly familiar with what common practices are, but I can say that I believe some common practices were likely used.

Mr. HURD. And who were you using for guidance on what was good——

Mr. COOPER. Mr. Pagliano.

Mr. HURD. —digital system hygiene? Mr. Pagliano?

Mr. COOPER. And Apple on the original device.

Mr. HURD. Now, you've said Apple a few times. Is this like you went into the help desk at the mall? Like——

Mr. COOPER. We had an agreement with Apple's business service program at the time that spec of the equipment that we were going to use, set up the system, and installed it.

Mr. HURD. Excellent.

Mr. Chairman, I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We're now going to go to the gentleman from Alabama, Mr. Palmer, for 5 minutes.

Mr. PALMER. Thank you, Mr. Chairman.

Ms. Abedin and Ms. Hanley indicated the whereabouts of Clinton devices would frequently become unknown once she transitioned to a new device. What about these other devices? Did you make any inquiry about any of the missing devices to make sure they were properly secured and the data properly recorded?

Mr. COOPER. I can say with some certainty, whenever there was a transfer from one device to the next, there was always the goal and the process to transfer all the data from the previous device to the new device.

You're specifically, I believe, asking about what happened to the devices that I know that I personally did not dispose of. I can't speak to that. I believe that, you know, I may have asked those who were in the process of doing that for Secretary Clinton to also properly dispose of them by rendering them unusable.

Mr. PALMER. So you were responsible for setting up the servers and these devices. Is that——

Mr. COOPER. Mr. Pagliano set up the Pagliano server. For someone to transfer to a new BlackBerry device, it simply requires someone to tell the server that there's a limited period of time for a user to log in with a one-time username and password——

Mr. PALMER. But when you transitioned from one device to another, did you have any responsibility in handling the device that was no longer being used? What did you do with that? I understand you did something with some devices.

Mr. COOPER. On occasion, I was the person who made the transfer. And when I was complete with backing up the information, ensuring that it was on the new device, wiping the old device, I rendered them unusable in other manners, yes.

Mr. PALMER. Are you aware that there's a missing laptop and external storage device?

Mr. COOPER. I'm aware of that, based on the reading of the FBI report.

Mr. PALMER. So you do know about it. Do you know that the report was that it was lost in the mail?

Mr. COOPER. That's as much as I know.

Mr. PALMER. That's as much as you know. You don't know—do you know who mailed it?

Mr. COOPER. I have no details about that.

Mr. PALMER. So, if you don't know who mailed it, you don't know who it was sent to.

You are, as Mr. Hice pointed out, aware that Director Comey described Mrs. Clinton's use of a personal server and her handling of classified material as extremely careless. You are aware that he said that? You read the FBI report?

Mr. COOPER. Yes, I'm aware of the report.

Mr. PALMER. In your handling of Mrs. Clinton's servers, did you have any concerns that her use of a personal server and the use of outdated technology on her cellphones might be a problem?

Mr. COOPER. I viewed her use as personal use of a BlackBerry and of the server and that we kept up to date over a period of time.

Mr. PALMER. You've been around the Clintons for a pretty good period of time, haven't you?

Mr. COOPER. Yes.

Mr. PALMER. And you're aware of the highly sensitive material that Mrs. Clinton, as Secretary of State, was handling, that would pass through her communications devices and her servers through her email. You certainly had to be aware that there was sensitive information.

Mr. COOPER. I was generally aware that Secretary Clinton encountered sensitive information, sure. How that was transmitted to her was not something that I was specifically aware of.

Mr. PALMER. But in your disposal of these devices—and you said you made sure they were wiped and you took other measures to dispose of them—did you receive any instructions or any training about making sure that the data on those systems were properly recorded? Did anyone talk to you about that?

Mr. COOPER. I had no specific instructions around that.

Mr. PALMER. Would you consider your handling of these devices as possibly careless?

And I ask you that—and I think you've been a good witness. I appreciate the fact that you stayed. But, in listening to Mrs. Lummis' questions and your lack of knowledge of some of the cyber technology, the cyber protection technology and things like that, my concern is that it's almost an atmosphere of indifference.

And I really hope that's not the case, because this is not—although some of our colleagues on the other side of the aisle have tried to make this about her candidacy, it's really about our national security and how we handle things going forward. And that's the great concern that I think—really, the prevailing concern that this committee has, is that we make sure that we don't put our national security at risk, we don't put or intelligence officers at risk.

And that's my big concern, and particularly with this missing laptop that apparently no one's made an effort to recover.

I thank you, Mr. Chairman. I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We'll now recognize the gentleman from North Carolina, Mr. Walker, for 5 minutes.

Mr. WALKER. Thank you, Mr. Chairman.

I'd like to start just by making a couple statements. A lot of times, we're hearing some back-and-forth of really who to believe. I found it interesting that I believe there's three different times today that our friends to my right have not been necessarily truthful in some of the accusations they have made.

Number one, I believe that one of the members talked about this as some kind of relentless pursuit of Republicans trying to damage Secretary Clinton's Presidential chances or hopes, and, at the same time, this is some kind of photo op.

Well, let me remind everybody, if we could just pause for a moment and remember what Director Comey said, he said this was an investigation not caused by Congress but, rather, the inspector general, from the intelligence they were able to gather. So let me just put that on the record, making sure this has not been Republican-driven, this was the inspector general of the FBI.

Another thing they've tried to make a case for is this is some kind of Republican witch hunt. I specifically asked Director Comey did he feel this way; he said, no, he not. In fact, he said it was not a witch hunt.

And then, today, we hear our Democrat friends say that there is no evidence that emails were hacked. Well, on January the 9th, 2011, Mr. Cooper, you became aware of an attempt to hack Hillary Clinton's private email server. Is that correct?

Mr. COOPER. I believe you're referring to an email that was in the FBI report. And as I—you may not have been here earlier in the hearing. I said that I was using the world "hacked" colloquially. So I thought people were understanding what this was was a series of failed log-in attempts. And one of the earliest occurrences of this—the way that we managed to put an end to them was to shut down the server for very brief periods of time.

Mr. WALKER. Yeah, I was here earlier and heard you share a little bit about that. Do you agree that there is no evidence that this server could have been hacked?

Mr. COOPER. I can, to the best of my knowledge, just refer you to the FBI report, who did the forensic analysis on this.

Mr. WALKER. But you don't have kind of a take on it, even though you were——

Mr. COOPER. I have no knowledge that there was a successful hack on the——

Mr. WALKER. Are aware of how many times the Russians and the Chinese try to attack us on a daily basis?

Mr. COOPER. I am not aware of that.

Mr. WALKER. Not aware of that?

And make sure, this was on her private server. Is that correct? Not a State Department or a government-protected server. Is that correct?

Mr. COOPER. Correct. This was a private server.

Mr. WALKER. Yeah.

It's just—it's interesting that if it wasn't to what you consider maybe a hack status—you emailed her twice that day. How often did you normally email Mrs. Clinton in a given day?

Mr. COOPER. I believe the email was to Ms. Abedin. Again, this was one of the first or second occurrences that something like this was happening. I was just making her aware more that the email services might be off line for a few moments——

Mr. WALKER. Sure.

Mr. COOPER. —rather than——

Mr. WALKER. In the weeks before, how many times did you send an email that was in the same reference?

Mr. COOPER. I don't recall ever sending a great line with those emails.

Mr. WALKER. So this was the first time that you'd ever sent something like that?

Mr. COOPER. I can't say specifically it was the first time, but——

Mr. WALKER. Pretty rare, though, you would think?

Mr. COOPER. Yes.

Mr. WALKER. Okay. Yet, at the same point, you're now describing it that "hack" was probably not the best description of it.

Mr. COOPER. Correct.

Mr. WALKER. But you were concerned?

Mr. COOPER. I was mostly, in the email, making her aware that I was shutting down the server for a brief period of time.

Mr. WALKER. Were there any other times or attacks that you're aware of that you felt like that put the server in a vulnerable position while Ms. Clinton was in possession of the server? Any other times?

Mr. COOPER. As there was an increase in the failed log-in attempts, we made the Secret Service aware. And they reviewed the logs and made some recommendations to——

Mr. WALKER. Have you got a number, about roughly how many times it might have happened, all these failed email attempts or log-in attempts?

Mr. COOPER. I can't give you a specific number.

Mr. WALKER. Less than a thousand? More than a thousand?

Mr. COOPER. Less than a thousand.

Mr. WALKER. Okay.

In just closing here, and I'll yield back the rest of my time here, you might have mentioned this earlier, as well, in having to do some questioning right outside here, but can you remind me again how you were compensated? Can you go into that, to tell me what direction—who compensated you for all this?

Mr. COOPER. I worked for the Clintons for 15 years and was compensated in a variety of ways over that period of time depending on what my activities were. I worked for President Clinton, helping him write his memoirs and two subsequent books.

Mr. WALKER. Yeah.

Mr. COOPER. I traveled the world with him. At points, I supported the foundation. So I had varying sorts of income over the——

Mr. WALKER. Okay. It's a little gray area there, if I may be so bold. When you say you were compensated in a variety of ways, did that include being paid with cash?

Mr. COOPER. No.

Mr. WALKER. Okay. So this was just like, hey, a personal check from Bill Clinton, here you go, or——

Mr. COOPER. Yes, the taxable—you know, I was a full employee of Bill Clinton.

Mr. WALKER. Well, what was the title on—how were you getting paid with that? Did it say Bill and Hillary? I mean, what—how was that?

Mr. COOPER. Yes. There were multiple payrolls. There was a Clinton household payroll. Later, there was a Clinton Executive Services Corporation payroll.

Mr. WALKER. But there were personal checks as well?

Mr. COOPER. They were, through an employer services company that managed the payroll, yes.

Mr. WALKER. Okay. All right. Thank you.

Mr. Chairman, I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We'll now recognize the gentleman from Oklahoma, Mr. Russell, for 5 minutes.

Mr. RUSSELL. Thank you, Mr. Chairman.

And thank you, Mr. Cooper, for your patience and also your answers that you've provided the panel today.

You alerted folks to possible breach attempts and were concerned, obviously, about the security, as we've heard in your testimony today.

In January 2013, according to the FBI reports, a tour user logged in to a staffer of President Clinton's account on the Pagliano server and browsed email and folders of that person's account.

Were you aware of that breach? That's a little different than what was just stated to Mr. Walker.

Mr. COOPER. I was not aware of that breach till I read it in the same account where you read it.

Mr. RUSSELL. Did it cause you concern?

Mr. COOPER. Once I read it?

Mr. RUSSELL. Sure.

Mr. COOPER. Sure.

Mr. RUSSELL. In the spring of 2013, which would've been proximate to this same thing, according to the FBI, Sidney Blumenthal's AOL account was hacked by Guccifer, and Mrs. Clinton's email exchange with Mr. Blumenthal was made public. Were you aware of that breach?

Mr. COOPER. I was aware of that.

Mr. RUSSELL. What was your response to these breaches?

Mr. COOPER. At that point in time, I was transitioning out of any role or responsibility with the server as the various teams were selecting—it was ultimately Platte River Network to take over the email services. And I don't know that I had any sort of direct response.

Mr. RUSSELL. Did you believe that there was sensitive information? Certainly, it would qualify as very private, being the position that Mrs. Clinton held.

Mr. COOPER. Certainly private information, concern that that—you know, you would have, naturally, concern that that information was properly backed up and secured.

Mr. RUSSELL. And the FBI reported finding email marked "Secret" on the PRN server. And you assisted with the transfer of data to the PRN server. Were you aware of Secret or sensitive emails on the servers you worked on?

Mr. COOPER. I did not actually assist in the transfer to the PRN servers, and nor was I——

Mr. RUSSELL. Even with the missing laptop, which you didn't lose but apparently it got lost after PRN received it?

Mr. COOPER. Yeah, I have no knowledge of that.

Mr. RUSSELL. But you did have knowledge of providing a laptop to the——

Mr. COOPER. Provided a laptop and instruction on how to download emails, yes.

Mr. RUSSELL. Now, Mr. Cooper, you conveyed to I believe it was Mr. Meadows—and we appreciate the insight you have given us—that Huma Abedin assisted in arrangements on the use of the private server when all of this was being set up. Is that correct?

Mr. COOPER. Yes.

Mr. RUSSELL. Did you create or did Huma Abedin or Cheryl Mills or Jacob Sullivan have a user account on the private server?

Mr. COOPER. Huma Abedin had an account.

Mr. RUSSELL. Huma Abedin did have an account.

And, Mr. Cooper, are you aware that in the FBI report it states on page 10 that Mrs. Clinton's immediate aides, to include Huma Abedin, Cheryl Mills, and Jacob Sullivan, told the FBI that they had no knowledge of the existence of a private server until after Mrs. Clinton's tenure at State? But that would've not been true, would it?

Mr. COOPER. I can't speculate on what their comments were.

Mr. RUSSELL. Well, I know you can't speculate on what their comments were. But you just stated that Ms. Abedin knew of the server, she had an account on the server. So how is it possible that she could not have known about a server while Mrs. Clinton was at State?

Mr. COOPER. I can't speak to her recollection of when she knew, but she was—I can tell you——

Mr. RUSSELL. But that would be contrary to the facts, wouldn't it?

Mr. COOPER. I can just tell you that I know that she had an account on the server and she was aware and using an account on the server.

Mr. RUSSELL. At the time that Mrs. Clinton was—okay. Thank you for establishing those facts for us. We appreciate that.

And BlackBerrys, we know that there was preferences on functions and systems and going back and forth, a lot of different devices. And we also know that there was one BlackBerry that was provided from State, but they sent it with a warning that, look, all of this could be Freedom of Information Act; therefore, you know, go in with this understanding. And so they elected to not use that BlackBerry.

There were other BlackBerrys used associated with the server, which we have determined. How were they obtained? Were they third-party-obtained? Obviously, it wasn't through State, because there was only one that we know about. Maybe there were more.

Mr. COOPER. I can't speak to them being obtained by the State Department. I have no——

Mr. RUSSELL. Okay. Were they obtained through a third party? Or how were they——

Mr. COOPER. Other BlackBerrys were typically, to the best of my recollection, just obtained from the service provider, AT&T, who we had an account with to service those phones.

Mr. RUSSELL. Okay. So they weren't obtained by a third party like eBay, Amazon, something of that nature?

Mr. COOPER. Not to my knowledge.

Mr. RUSSELL. Okay.

And, with that, my time has expired. Thank you, Mr. Chairman.

Mr. CUMMINGS. Mr. Chairman?

Chairman CHAFFETZ. Yes.

Mr. CUMMINGS. Just one question of the gentleman.

You said that there was—you said that there was an email marked "Secret," and we just wanted to know what that was, because we never saw that. We'd just like to see the document.

Chairman CHAFFETZ. I'll let you work that out with Mr. Russell. We'll now recognize——

Mr. CUMMINGS. I wanted the record to be clear if there's not one.

Chairman CHAFFETZ. I'll now recognize Mr. Grothman of Wisconsin.

Mr. GROTHMAN. Yeah. Thanks for coming over.

I want to nail down a little bit more, a followup on what Representative Walker said. You first became involved with then-President Clinton in 1999? That was your first involvement with the Clintons?

Mr. COOPER. Yes.

Mr. GROTHMAN. Okay. At the time you were an aide—so, at that time, you were paid by the United States Government?

Mr. COOPER. In '99, I was an intern still. In 2000, I became a U.S. Government employee.

Mr. GROTHMAN. Wow. What being an intern will lead to, Huh? Okay.

And then when President Clinton left office, from then until today, you say you worked for the Clintons. But was it, like, the Clintons' personal for 2 years, their foundation, or the Clinton Executive Services Corporation? Who was cutting the checks from time to time?

Mr. COOPER. The organizations evolved over a period of time, as I think was only natural as different parts of the operation grew and shrank. For a period of time, I was in the transition office from President Clinton for the first 6 months out of office. I then worked for him in support of his efforts to write his memoir for almost 4 years.

Mr. GROTHMAN. Okay. So then it was Bill personally?

Mr. COOPER. In combination with the book publisher. And then, following that, worked on what was the Clinton household payroll for a series of years.

Mr. GROTHMAN. Okay. Could you get us a list? Just because I want to kind of see, you know, where you were involved in the thing. I hope it's not too much bother. From when Bill Clinton left office until today, who were you working for? Do you see what I am saying? Like, when you get the W–2——

Mr. COOPER. Sure. And then until I left in 2013.

Mr. GROTHMAN. Right, right, right. Were you getting, like, W–2s or 1099s, or how were they doing it?

Mr. COOPER. Yeah, I can have my attorneys prepare something for you.

Mr. GROTHMAN. Yeah. I would like to have that.

Next question: When you interacted with the Clintons, did you usually hear from Bill directly? Hillary directly? Huma? Who was the person you usually heard from?

Mr. COOPER. I primarily worked for President Clinton and worked with him on a day-to-day basis.

Mr. GROTHMAN. Okay. Did you ever get emails from Huma or Hillary?

Mr. COOPER. Certainly.

Mr. GROTHMAN. Okay. Like, once a month? Once a week?

Mr. COOPER. I couldn't tell you what the frequency was. Often, it was coordination between the family to organize their schedules.

Mr. GROTHMAN. Okay. Did you have any coordination with the foundation, or did the foundation ever employ you?

Mr. COOPER. Yes.

Mr. GROTHMAN. Okay. When you heard about the foundation, who was your contacts there? I mean, who was your contact with the foundation? Bill again?

Mr. COOPER. Yeah, over time, many different people worked for the foundation. Primarily, my role with the foundation was supporting President Clinton's activities with the foundation.

Mr. GROTHMAN. Okay. Did you ever hear from Huma or Hillary about the foundation?

Mr. COOPER. At varying times, they participated in foundation-related events over the lifetime of the foundation from when we left the White House to——

Mr. GROTHMAN. Okay. When did the foundation kick in? I mean, I can't remember when that thing began.

Mr. COOPER. You know, officially, the foundation was launched as we were leaving the White House in support of the Presidential library and developed programs over time from that period.

Mr. GROTHMAN. Before it became the charitable institution it eventually became.

Mr. COOPER. Correct.

Mr. GROTHMAN. Okay.

Did you receive emails from Secretary Clinton or Huma connected to State Department business?

Mr. COOPER. Not that I recall. Secretary Clinton on occasion had forwarded me documents to print.

Mr. GROTHMAN. Okay. Usually, when they contacted you, her or Huma, it would be foundation business or personal business?

Mr. COOPER. I would say personal business.

Mr. GROTHMAN. Can you give me an example of personal business?

Mr. COOPER. Asking where President Clinton was, if he was available, something that may have been going on in their household.

Mr. GROTHMAN. Okay.

I'll tell you what I'll do. I'll leave the remainder of my time to the chair. But I would like—I would like to see, you know, a chronology of, you know, this is who I got the W–2s from in 2002, this in 2003, this in 2004.

I'll give you one more question. Was it usually just one person cutting the check each month? Were there months in which you got a check from Bill personally and the foundation?

Mr. COOPER. It varied over different periods of time.

Mr. GROTHMAN. Okay.

Chairman CHAFFETZ. I thank the gentleman.

Mr. Cooper, who are you employed by now?

Mr. COOPER. I have my own consulting firm and have a variety of clients that I work with to help them with their thought leadership, to identify——

Chairman CHAFFETZ. Does that include any of the array of Clinton entities?

Mr. COOPER. No, it does not involve any current Clinton entities.

Chairman CHAFFETZ. Or people or anything like that?

Mr. COOPER. People? If you could clarify. I'm sorry. It does not involve any of the Clintons, no.

Chairman CHAFFETZ. Okay. Thank you.

We'll now recognize the gentlewoman from New York, Mrs. Maloney.

Mrs. MALONEY. Thank you, Mr. Chairman.

I'd like to begin by quoting Bernie Sanders. He famously said in one of the debates, he said, "Enough. Enough of these emails." And I think that those of us that have sat through this hearing today can say the same.

We're seeing a predictable pattern from the Republican Party, where they come out and make all kinds of accusations that I believe are politically motivated. They make all kinds of accusations against Secretary Clinton. And they claim—they make really reckless ones that are criminal accusations, and then they call for an investigation. And then the investigation happens, and what comes out of the investigation does not support the accusations. And then they move on to the next email, quote, attack that they put forward.

And this happened, we saw it with the discredited Benghazi hearings and accusations and reports and reviews, where the FBI and other independent investigators found no evidence, none whatsoever, of a crime with the emails. And so what do we have again? Another accusation claiming email criminal activity.

Now, this latest one is that Secretary Clinton and her top aides ordered the destruction of emails to conceal these emails from investigators. For example, my good friend—and he really is a good friend—Representative Meadows, I heard him on national television, where he claimed that the emails were deleted as a result of, and I quote, "a directive from the Clinton campaign." There's no evidence to support this accusation.

Chairman Chaffetz made a similar claim in his criminal referral to the U.S. attorney on September 6th, claiming that Secretary Clinton's attorneys, Kendall and Mills, issued this order during a call with Platte River Networks in March 2015. But these claims were already investigated by the FBI, and guess what? There was not any evidence to support these claims.

And the FBI summary explains that after Secretary Clinton's attorneys finished producing her work-related emails to the State Department she no longer needed her remaining personal emails.

Well, the FBI is there for a reason. They are there to investigate, to make determinations, and to come forward with conclusions. And they've concluded that there's no evidence. So why are we here? Why are we trying to contradict what the FBI found?

And the bottom line is that the FBI, based on their reviews, based on the professionals that they have looking at this, they came forward and said—and Director Comey actually said it right before this committee. He testified, "We do not find any evidence of evil intent and intent to obstruct justice," end quote. This is the head of the FBI, relying on a complete investigation of his personnel on this issue. He also said, and I'm quoting him again, "We did not find evidence to indicate that they did anything to try to erase or conceal anything of any sort." So the FBI has already made their determination.

So my one question to you, Mr. Cooper: In all of your work and your understanding, your experience with all of this, did you see anything that contradicts the conclusion of the FBI professionals

and Director Comey, who testified before this Congress he saw no criminal activity, he saw no abuse of justice. Did you see anything to contradict his conclusion?

Mr. COOPER. The facts, to my knowledge, no.

Mrs. MALONEY. No. Okay.

So I just want to remind everyone that the FBI, we're here for 1 day, but they conducted a yearlong investigation and concluded that no charges were appropriate. And they had, I would say, an all-star team. We have very good investigators here on our committee, but I would say a yearlong investigation by the FBI with their all-star teams, that they are professionals, they're trained professionals, and they came forward and said after that there was no charges, no charges were appropriate.

So I just want to join Bernie Sanders in saying enough is enough. And we've had investigations after investigation, accusation after accusation. And now we have another accusation after the investigation was completed by the FBI, which has an unmatched record in protecting our citizens, preserving the law of this country, and preserving the integrity of government.

And I would say I rest my case. I listened carefully to Director Comey——

Chairman CHAFFETZ. The gentlewoman's time has expired.

We'll now——

Mrs. MALONEY. I was just warming up, Mr. Chairman.

Chairman CHAFFETZ. The gentlewoman yields back.

We'll now recognize the gentleman, Mr. Smith, who's the chairman of the Science, Space, and Technology Committee. We're pleased to have him here today. And we're thankful for the close working relationship we have with the committee. We now recognize him.

Mr. SMITH OF TEXAS. Thank you very much, Mr. Chairman, for inviting me to attend today's hearing to examine the security of former Secretary of State Hillary Clinton's private server.

Secretary Clinton's unique server and email arrangement is of particular importance both to your committee and to the Science, Space, and Technology Committee. The Science Committee has a responsibility to examine ways in which executive branch departments and agencies and private entities can improve their cybersecurity practices.

As part of the Science Committee's ongoing investigation, I have issued subpoenas to three of the companies that performed maintenance and security work on Secretary Clinton's private server. Two of the companies who received lawfully issued subpoenas for information related to work they performed for former Secretary Clinton, Platte River Networks and SECNAP, Inc., have refused to produce responsive documents. Both companies have purposely misinterpreted the plain language of the subpoena, and both companies have stated that they do not have responsive materials, which is demonstrably false.

Unfortunately, these companies' decisions to obstruct the committee's investigation and defy a lawfully issued subpoena continues a Clinton habit of secrecy rather than transparency. In fact, just this morning—and this may be of interest to the gentlewoman from New York who just spoke—SECNAP's counsel confirmed to

my staff that the Clintons' private LLC is actively engaged in directing their obstructionist responses to congressional subpoenas.

This is a clear obstruction of justice. Americans deserve to know the truth, which is now being blocked by the Clinton organization.

One of the companies, Datto, did provide responsive materials to the subpoena. These documents have shed light on the unique arrangement undertaken by Secretary Clinton to set up a private server. This includes the lack of even basic cybersecurity measures applied to the information stored on the server, such as encryption. It is inconceivable that a Secretary of State, who is entrusted with our national security secrets, would not take every available step to safeguard our Nation's classified information.

The information sought through the investigations of the Science Committee, the Oversight and Government Reform Committee, and Senator Ron Johnson of the Senate Homeland Security and Governmental Affairs Committee is crucial in determining the degree to which our national security was unprotected and perhaps endangered.

I look forward to continuing to work with you, Mr. Chairman, and appreciate all the good work you have done.

And if it's all right, I have a couple questions for Mr. Cooper.

Chairman CHAFFETZ. Yes.

Mr. SMITH OF TEXAS. Mr. Cooper, first of all, thank you for being here today and being willing to answer questions. You deserve credit for being willing to do that, and that compares to those who refused to appear today and answer questions and apparently are not interested in helping us try to find out the truth.

Let me ask my first question, which is that, as you heard me say a minute ago, we heard this morning that SECNAP's counsel has said that the Clinton Executive Services Corporation, in effect, is obstructing at least my committee's subpoena. Do you think this is standard practice for the Clinton Executive Services Corporation?

Mr. COOPER. I'm not in a position to comment——

Mr. SMITH OF TEXAS. I'm sorry?

Mr. COOPER. I'm not in a position to comment on that or have any knowledge that that's the situation.

Mr. SMITH OF TEXAS. Have you seen any other instances where SECNAP has tried to prevent information from getting to a committee?

Mr. COOPER. I'm not aware of——

Mr. SMITH OF TEXAS. One way or the other?

Mr. COOPER. I'm not aware at all.

Mr. SMITH OF TEXAS. Okay.

Many of the documents provided by Datto, Inc., include communications with Platte River Networks. Should Platte River Networks have information in its possession about its work related to former Secretary of State Hillary Clinton's server?

Mr. COOPER. Again, my interaction with Platte River Networks was simply handing over some usernames and passwords, and that was the totality of the interaction that I've had with them. I've never had any interaction with them beyond that or with Datto.

Mr. SMITH OF TEXAS. And can you say whether or not they are likely to have information about the server or not?

Mr. COOPER. I have no knowledge.

Mr. SMITH OF TEXAS. Okay.

What information, again, have you handed over to them?

Mr. COOPER. Sir, I handed over some usernames and passwords to them at the beginning of the transition process.

Mr. SMITH OF TEXAS. Okay. Thank you.

Thank you, Mr. Chairman. That completes my questions. And, again, I appreciate the opportunity to be a part of your committee's hearing today.

Chairman CHAFFETZ. Well, thanks, Chairman. We do appreciate it.

I will now recognize the gentleman from Georgia, Mr. Carter.

Mr. CARTER. Thank you, Mr. Chairman.

And, Mr. Cooper, thank you for being here, and thank you for staying as long as you have.

Mr. Cooper, in Secretary Clinton's New York and Washington, D.C., homes, did she have a personally owned desktop computer inside the secure areas, or the SCIFs?

Mr. COOPER. We discussed earlier, there were Apple iMacs in both homes that I know were in the rooms that became SCIFs predating their time becoming SCIFs.

Mr. CARTER. How do you know that?

Mr. COOPER. Before they became SCIFs, they were both offices which I had the occasion to work out of.

Mr. CARTER. And you said, what kind of computers were they?

Mr. COOPER. Apple iMacs.

Mr. CARTER. Who was able to open them?

Mr. COOPER. They were there for the purpose of staff visiting the home or the staff that worked in the homes.

Mr. CARTER. Was it ever left unsecured?

Mr. COOPER. "Unsecured" meaning? I'm sorry.

Mr. CARTER. Just left out where someone could get to it?

Mr. COOPER. These were personal computers in their homes secured by the Secret Service.

Mr. CARTER. And who did you say had access to it?

Mr. COOPER. The Clinton family and their staff.

Mr. CARTER. And their staff.

Let me ask you about two occasions in 2011 where you were concerned that someone was trying to hack into Hillary Clinton's private email server. What made you concerned that someone was trying to hack in, as described in the email you sent to Huma Abedin?

Mr. COOPER. I think my concern at the time was—I was colloquially using the word "hack" to describe what was a multiple failed log-in attempt on the server. And what I was really conveying to her, less so the concern of that activity and more so that we were dealing with it by shutting down the server for a period of time and so she should expect her email to be off-line for a period of time.

Mr. CARTER. So later on that day, you email Ms. Abedin, you said there was a second attempt. In fact, you said, "We were attacked again, so I shut the server down for a few minutes."

Mr. COOPER. Yes. Again——

Mr. CARTER. Help me out. Whenever I think of an attack on a computer, I think of somebody who's trying to get in unauthorized.

Mr. COOPER. I understand. I was using very colloquial language.

Mr. CARTER. Very colloquial language.

Mr. COOPER. Correct.

Mr. CARTER. So that's not what you meant when you said "attack"? That someone was——

Mr. COOPER. These were multiple failed log-in attempts on the server.

Mr. CARTER. But wouldn't you describe that as someone who's trying to get in unauthorized?

Mr. COOPER. I would describe it as someone who was trying to get in unauthorized, yes.

Mr. CARTER. So was it the same—was it the same attempt as was the previous day?

Mr. COOPER. I can't recall whether it was the same attempt or be able to determine whether it was the same type of attempt.

Mr. CARTER. Did you shut the server down on that day in January of 2011?

Mr. COOPER. To the best of my recollection, based on the emails that you are describing, yes.

Mr. CARTER. What good would that have done? What was the purpose in doing that?

Mr. COOPER. My understanding was that these were automated attempts, and once they did not ping a server on the other side, they would stop. And that seems to be the practice of what happened.

Mr. CARTER. We've had reports and we've read numerous reports that Mr. Pagliano arranged for you to receive notifications when there were attempted hacks on the server. Did you receive any notification of any attempted attacks on the server?

Mr. COOPER. What Mr. Pagliano had set up were alerts to alert me if there were any failed log-in attempts, which could be from users or nonusers.

Mr. CARTER. Okay. I'm struggling here. Tell me the difference between a failed log-in attempt and a hack.

Mr. COOPER. So a failed log-in attempt is very simply when someone tries to log into the server, in one form or another, into an account or to the server itself——

Mr. CARTER. Okay. All right. What's an attack?

Mr. COOPER. I'm sorry—with a username or a password that's not valid. So that could be a legitimate user who has mistyped their password or a legitimate user whose password has expired——

Mr. CARTER. Okay, I get that. Just define an attack for me.

Mr. COOPER. Again, the word "attack" is colloquial.

Mr. CARTER. No, no. Describe what you would define "attack" as.

Mr. COOPER. Multiple failed log-in attempts, trying different usernames, in no specific pattern.

Mr. CARTER. Would you agree that most people describe "attack" as much more than that?

Mr. COOPER. I would agree with that.

Mr. CARTER. Okay.

We've been told and we've discovered that Hillary Clinton's old phones were destroyed with a hammer—with a hammer. Were these phones connected to the private email server in question?

Mr. COOPER. Yes. I described earlier that when Secretary Clinton would transition from one device to the next we'd take the old device, back it up, make sure all of the content was transferred onto the new device, linked with the server so any information that came from the server was on the new device; then, once that was completed, wiped the old device using the BlackBerry tool to do so; and then, on occasion, I would render them unusable.

Mr. CARTER. Why did you use that kind of method? It seems somewhat, if you will, barbaric. I mean, a hammer to a phone?

Mr. COOPER. I think it's practical to not just throw a cold device into some sort of garbage receptacle where someone might pick it up out of curiosity and try to use it.

Mr. CARTER. Okay.

You know, I mean, here we are—and with all due respect, sir, the definition of "attack" that you have and the definition of "attack" that I have and I think most people have are completely different.

And then, you know, we're taking an old phone and destroying it with a hammer. Were you instructed to do that?

Mr. COOPER. No, that was not something I was instructed to do.

Mr. CARTER. But you say that was normal procedure? Is this the way you do away with everybody's old phones?

Mr. COOPER. I felt that that was a good practice at the time.

Mr. CARTER. Okay.

Mr. Chairman, I've exceeded my time, and I yield.

Chairman CHAFFETZ. I thank the gentleman.

A few other questions as we conclude here. And, again, I give you great credit for being here and answering the questions. I do appreciate it.

Why were there no backup images prior to June 23rd, 2013, made available to the FBI as part of their criminal investigation?

Mr. COOPER. That's not something that I have knowledge or insight into.

Chairman CHAFFETZ. But, I mean, you and Mr. Pagliano were running this ship here. So why were there no backup——

Mr. COOPER. Technically, Mr. Pagliano handled that component of the server, and I was not managing the backup component.

Chairman CHAFFETZ. The FBI report states that the so-called Pagliano server was backed up to an external hard drive between May of 2009 and June of 2011. Is that your understanding?

Mr. COOPER. It is only my understanding from reading the same report that you have read.

Chairman CHAFFETZ. The report further states that you would periodically delete the records maintained in the backup as disk space ran out. Is that correct?

Mr. COOPER. Again, I was not the one responsible for those deletions. I'd refer you to Mr. Pagliano.

Chairman CHAFFETZ. You didn't do any of those deletions?

Mr. COOPER. No.

Chairman CHAFFETZ. Was there any consideration to get a backup or external hard drive?

Mr. COOPER. I believe at one point we upgraded the backup system that was attached to the server.

Chairman CHAFFETZ. So, rather than backing this stuff up, you just went ahead and deleted it?

Mr. COOPER. I was not the one responsible for or doing any deletions.

Chairman CHAFFETZ. The FBI was unable to locate or procure any of the 13 mobile devices used by Secretary Clinton during her tenure. Are you aware of the location of any of these devices?

Mr. COOPER. I am not aware of the location of any of those devices.

Chairman CHAFFETZ. Secretary Clinton, did she ever use the computer that you set up for her?

Mr. COOPER. The computers that were in their homes?

Chairman CHAFFETZ. Yeah.

Mr. COOPER. I can't say specifically whether she ever——

Chairman CHAFFETZ. You never saw her? Did she know how to use the computer?

Mr. COOPER. I don't know that she did or used those computers.

Chairman CHAFFETZ. So you bought a computer, set up the computer, but you never saw her use it.

Mr. COOPER. I don't believe I ever saw her use a computer.

Chairman CHAFFETZ. And who had access to this computer?

Mr. COOPER. She has household staff in each home, and I think her personal aides who would come to her house before or after she traveled, who would predominantly, to my knowledge, use those computers to print off, you know, clips and briefing materials.

Chairman CHAFFETZ. And they could access that when it became a SCIF?

Mr. COOPER. I don't know if that was the situation.

Chairman CHAFFETZ. Well, you were there. I mean, you were in the household on a regular basis. Did you ever use it in the SCIF?

Mr. COOPER. I don't remember using those computers once they were in the SCIF. There was a separate computer that was not in a SCIF in the home in Chappaqua which was regularly used for basic printing purposes.

Chairman CHAFFETZ. And would it print her emails?

Mr. COOPER. I can't say that it would—to know that it would print her emails.

Chairman CHAFFETZ. I'm sorry, the what?

Mr. COOPER. I don't know that it printed her emails.

Chairman CHAFFETZ. Okay, but did you ever see the computer in her SCIF?

Mr. COOPER. I have seen the SCIF, and I know the computer was in there, so it's hard to parse the times——

Chairman CHAFFETZ. You've been in the SCIF?

Mr. COOPER. —from those rooms, you know, which I spent time in over many years——

Chairman CHAFFETZ. Right.

Mr. COOPER. —prior to them becoming SCIFs.

Chairman CHAFFETZ. You put a little qualifier on there. Are you telling me for 4 years you never went in that room?

Mr. COOPER. I can't recall a specific occasion where I walked into that room, but there may have been an occasion. I can't——

Chairman CHAFFETZ. So if you're talking to the Secretary and she walks in that room, you stopped at the door and——

Mr. COOPER. I don't recall any situation of that type.

Chairman CHAFFETZ. All right.

Do you know how the SCIF was secured?

Mr. COOPER. I was there when the SCIFs were set up, and I believe they had locks on the doors.

Chairman CHAFFETZ. All right.

What happened when the FBI showed up? Did they seize things? Were you there?

Mr. COOPER. I'm sorry?

Chairman CHAFFETZ. Were you there when the FBI came?

Mr. COOPER. To?

Chairman CHAFFETZ. To her home in New York.

Mr. COOPER. No.

Chairman CHAFFETZ. I'm not 100-percent certain that they came to her home in New York. Are you aware that they seized anything?

Mr. COOPER. I'm not aware of that.

Chairman CHAFFETZ. Okay.

Let's go back one more time. The very same day that Hillary Clinton started her Senate confirmations is the very same day that you registered ClintonEmail.com and evidently set up the server, correct?

Mr. COOPER. That was the day, I believe, that we registered ClintonEmail.com. I'm not sure that that's the day we set up the server.

Chairman CHAFFETZ. Why that day? I mean, what was she doing 3 days before that?

Mr. COOPER. I have no recollection of where she or I were 3 days before that.

Chairman CHAFFETZ. Why not set up a Gmail account?

Mr. COOPER. I think the consideration was that there was an existing server used by President Clinton's small group of staff that provided an option for her to maintain a personal email address using that system.

Chairman CHAFFETZ. Did she have a personal email address before she got ClintonEmail.com?

Mr. COOPER. She was using an AT&T BlackBerry address up to that point, which had limited ability to retain emails or view them in any other way besides on the BlackBerry.

Chairman CHAFFETZ. Okay.

We have some additional—do you still advise Teneo Holdings?

Mr. COOPER. Yes, I still advise Teneo.

Chairman CHAFFETZ. Okay.

Listen, again, I want to reiterate how much I appreciate your being here, subjecting yourself to questions before Congress. It's not a comfortable thing. I'm sure it's not something you set out early in life to do. But, nevertheless, the committee did call you, and you are here, and you've answered—you're attempting to answer all of the questions. And for that, we're very much appreciative. That's the way the system is supposed to work. And so we're very grateful for that.

Let me recognize before we recess here Mr. Cummings.

Mr. CUMMINGS. How's your business doing?

Mr. COOPER. Okay.

Mr. CUMMINGS. I ask that because, you know, a lot of times we have these hearings, and a lot of people sometimes don't seem to realize that there's life after the hearing.

And do you have a family? Do you have family?

Mr. COOPER. I do not.

Mr. CUMMINGS. And then, you know, you—I, too, want to thank you for your testimony. I think you've been very straightforward. And I thank you for your cooperating with the FBI. And your testimony has been very helpful.

And, you know, having practiced law for many years, it's painful, I'm sure, to have to pay legal bills, because it's expensive, and that's money that you could probably be doing some other things with. But, you know, I'm sorry you have to go through all of this. But the fact is that, you know, it's part of life. But I just want to thank you very much.

And I can understand, based on your testimony, why Director Comey came to the conclusions that he did, particularly with regard to you. So thank you very much.

Chairman CHAFFETZ. It is the intention of the chair to recess the hearing and reconvene at a later date. We'll provide ample notice of the date and time of the reconvening.

The committee stands in recess.

[Whereupon, at 12:36 p.m., the committee recessed, subject to the call of the chair.]

EXAMINING PRESERVATION OF STATE DEPARTMENT FEDERAL RECORDS

Thursday, September 22, 2016

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The committee met, pursuant to call, at 10:01 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Duncan, Jordan, Walberg, Gowdy, Farenthold, Lummis, Massie, Meadows, DeSantis, Walker, Blum, Hice, Carter, Palmer, Cummings, Norton, Lynch, Connolly, Lawrence, Plaskett, and DeSaulnier.

Chairman CHAFFETZ. The Committee on Oversight and Government Reform will reconvene. This is a continuation of our September 13 hearing on the "Examining the Preservation of State Department Federal Records."

We are scheduled to have Mr. Pagliano attend this hearing. Due to his absence and his violation of a duly issued subpoena by the Committee on Oversight and Government Reform, we intend to adjourn this hearing and immediately convene a business meeting to reconsider a resolution and report holding Mr. Pagliano in contempt of Congress.

Mr. Cummings, do you have a statement or ——

Mr. CUMMINGS. Yes, I have ——

Chairman CHAFFETZ.—can we go ahead and adjourn?

Mr. CUMMINGS. I have a brief statement.

Chairman CHAFFETZ. Sure.

Mr. CUMMINGS. Well, let me just say this. This is certainly no surprise to anyone. Mr. Pagliano's attorney told us last week he wouldn't be here. They told us it would be an abuse to force him to appear for a second time before Congress just to assert his Fifth Amendment rights. And they sent us another letter last night saying exactly the same thing.

Let me read from one portion of the letter so there is no question about what is going on here. "We have corresponded extensively with you and the committee's attorneys over the past two weeks on this subject. The facts have not changed." Continuing the quote, "You and the committee have been told from the beginning that Mr. Pagliano will continue to assert his Fifth Amendment rights and will decline to answer any questions put to him by your committee."

The letter explains that he already asserted his Fifth Amendment rights before the Benghazi Select Committee, and he should not be forced to do so a second time.

The letter continues, "A subpoena issued by a congressional committee is required by law to serve a valid legislative purpose, and there is none here. The demand under the present circumstances that Mr. Pagliano again assert his constitutional rights in front of

video cameras six weeks before the presidential election betrays a naked political agenda and furthers no valid legislative aim."

I ask unanimous consent that this full letter from Mr. Pagliano's attorney, sent last night to the committee, be entered into the official record.

And I have nothing else on that, Mr. Chairman.

Chairman CHAFFETZ. Without objection, so ordered.

[The information follows:]

Akin Gump
STRAUSS HAUER & FELD LLP

MARK J. MACDOUGALL
+1 202.887.4510/fax: +1 202.887.4288
mmacdougall@akingump.com

September 21, 2016

VIA ELECTRONIC DELIVERY

Hon. Jason Chaffetz
Chairman
The Committee on Oversight and Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, D.C. 20515-6143

Re: *Subpoena ad testificandum* issued on September 16, 2016 to Bryan Pagliano

Dear Chairman Chaffetz:

We are writing in response to the subpoena that you caused to be served on our client Bryan Pagliano at his place of employment on September 16, 2016, seeking his appearance and testimony before the Committee on Thursday, September 22, 2016 at 10:00 AM. We are likewise responding to your letter of September 15, 2016 (the "September 15 Letter") as it relates to that subpoena.

We have corresponded extensively with you and the Committee's attorneys over the past two weeks on this subject. The facts have not changed. Mr. Pagliano previously appeared before the Benghazi Committee – in this same Congress – in response to a subpoena seeking the same testimony. Mr. Pagliano declined to answer all questions asked of him by the Benghazi Committee in reliance on his rights under the Fifth Amendment and was excused by Chairman Gowdy (who is also a Member of this Committee). You and the Committee have been told from the beginning that Mr. Pagliano will continue to assert his Fifth Amendment rights and will decline to answer any questions put to him by your Committee. In an effort to resolve this matter, Mr. Pagliano has offered to assert his rights on the record before this Committee in Executive Session. You have flatly refused that offer and continue to insist that Mr. Pagliano appear in a public session where his further and repeated assertion of his constitutional right not to testify can be videotaped and broadcast.

In the September 15 Letter you insist that the limited use immunity agreement between Mr. Pagliano and the Department of Justice – whatever its terms – will somehow permit the Committee to interrogate our client and demand that he answer despite the assertion of his Fifth Amendment rights. Your stated position betrays a fundamental misunderstanding of the law.[1]

[1] "Use" immunity does not provide blanket immunity from prosecution: "The only benefit as far as the witness is concerned is that . . . any information directly or indirectly derived from such testimony may not be used

Mr. Pagliano has not waived his constitutional rights and he is free to continue to assert those rights before your Committee and all the other congressional bodies that demand his appearance.

A subpoena issued by a congressional committee is required by law to serve a valid legislative purpose – and there is none here. Your demand under the present circumstances, that Mr. Pagliano again assert his constitutional rights in front of video cameras six weeks before the presidential election, betrays a naked political agenda and furthers no valid legislative aim. The Committee lawyers who may be participating in this effort should give serious consideration to the consequences of their conduct.[2] In the event the Committee carries out your threat of a contempt citation and a referral to the U.S. Attorney for the District of Columbia, Mr. Pagliano will rely on his constitutional rights to vigorously defend himself in any such action. He will exercise the right to obtain discovery from the Committee and all those involved in this episode and to summon and confront witnesses to appear in federal court for examination.

---

against him in a subsequent criminal prosecution." *In re Corrugated Container Antitrust Litig.*, 662 F.2d 875, 887 (D.C. Cir. 1981). In other words, a grant of "use" immunity does not prevent the government from prosecuting; it merely limits the government's sources of evidence. The Supreme Court has squarely held that a nonparty deponent retains the right, despite a grant of "use" immunity by the DOJ under 18 U.S.C. § 6002, to rely on the Fifth Amendment in declining to testify. *See Pillsbury Co. v. Conboy*, 459 U.S. 248, 263-64 (1983). In *Conboy*, a district court held a nonparty deponent in contempt for asserting the Fifth Amendment privilege in response to a series of deposition questions that were identical to those asked during his grand jury testimony, which testimony was subject to a separate grant of "use" immunity under Section 6002. *Id.* at 250. The Supreme Court agreed that the contempt order was improper because the deponent was entitled to the protection of the Fifth Amendment. *Id.* The Court held that a nonparty "deponent's civil deposition testimony," even where it "closely track[s] his prior immunized testimony, is not, without duly authorized assurance of immunity at the time, immunized testimony within the meaning of § 6002." *Id.* at 263-64. For example, the witness's answers that merely repeated prior immunized testimony verbatim might reflect his "current, independent memory of events" and might be used in a future prosecution. *Id.* at 255 (describing petitioner's argument). The Court thus held that "District Courts are without power to compel a civil deponent to testify over a valid assertion of his Fifth Amendment right, absent a separate grant of immunity pursuant to § 6002." *Id.* at 257 n.13.

[2] The Committee lawyers enjoy no immunity for ethical misconduct and proceed in this matter at their professional peril. *See* D.C. Bar Ethics Opinion 31 (1977) (concluding that it is a violation of the D.C. Rules of Professional Conduct to summon a witness when "it is known in advance that no information will be obtained and the sole effect of the summons will be to pillory the witness.").

Mr. Pagliano is defending a critical principal of individual liberty and the constitutional right of a private citizen to resist partisan political forces masquerading as proper government functions. We earnestly hope that the Committee will further reflect on this matter, and recognize the needless expense and institutional harm that will follow from continued pursuit of the course of action that you have threatened.

Sincerely,

Mark J. MacDougall
Stanley M. Brand
Sean D'Arcy
Constance D. O'Connor
Connor Mullin
Abigail Kohlman
Counsel for Bryan Pagliano

cc: Hon. Elijah Cummings
Ranking Member

Chairman CHAFFETZ. The hearing is adjourned.
[Whereupon, at 10:04 a.m., the committee was adjourned.]

○