AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

OVERSIGHT OF THE STATE DEPARTMENT

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JULY 7, 2016

Serial No. 114–67

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

OVERSIGHT OF THE STATE DEPARTMENT

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JULY 7, 2016

Serial No. 114–67

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

21–323 PDF WASHINGTON : 2016

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
MATT CARTWRIGHT, Pennsylvania
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*
DAVID RAPALLO, *Minority Staff Director*
TRISTAN LEAVITT, *Senior Counsel*
WILLIAM MARX, *Clerk*

CONTENTS

	Page
Hearing held on July 7, 2016	1

WITNESSES

The Hon. James Comey, Director, Federal Bureau of Investigation	
Oral Statement	5
Mr. Steve Linick, Inspector General, Department of State, Accompanied by Ms. Jennifer Costello, Assistant Inspector General for Evaluations and Special Projects, Department of State	
Oral Statement	92
Mr. I. Charles McCullough, III, Inspector General for the Intelligence Community, Office of the Director of National Intelligence	
Oral Statement	92

APPENDIX

Sensitive Compartmented Information Nondisclosure Agreement, signed by Secretary of State Hillary Rodham Clinton, submitted by Rep. Chaffetz	122
Classified Information Nondisclosure Agreement, signed by Secretary of State Hillary Rodham Clinton, submitted by Rep. Chaffetz	124
A July 6, 2016 letter to the House Oversight and Government Reform Committee from Richard W. Painter, S. Walter Richey, Professor of Corporate Law at the University of Minnesota Law School, submitted by Rep. Lawrence	126
Two reports from the Office of Inspector General at the State Department, submitted by Rep. Chaffetz	128
a. "Evaluation of the Department of State's FOIA Process for Requests Involving the Office of the Secretary" January 2016	129
b. "Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements" May 2016	157
Series of memoranda from both the Department of State Inspector General and the ODNI Inspector General, submitted by Rep. Chaffetz	240
Opening Statement submitted by Rep. Elijah E. Cummings	255

OVERSIGHT OF THE STATE DEPARTMENT

Thursday, July 7, 2016

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

The committee met, pursuant to call, at 10:04 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Mica, Duncan, Jordan, Walberg, Amash, Gosar, DesJarlais, Gowdy, Farenthold, Lummis, Massie, Meadows, DeSantis, Mulvaney, Buck, Walker, Blum, Hice, Russell, Carter, Grothman, Hurd, Palmer, Cummings, Maloney, Norton, Clay, Lynch, Cooper, Connolly, Cartwright, Duckworth, Kelly, Lawrence, Lieu, Watson Coleman, Plaskett, DeSaulnier, Boyle, Welch, and Lujan Grisham.

Chairman CHAFFETZ. The Committee on Oversight and Government Reform will come to order.

Without objection, the chair is authorized to declare a recess at any time.

I want to thank Director Comey for being here and doing so on short notice. I have the greatest admiration for the FBI. My grandfather was a career FBI agent.

I have got to tell you, I am here because we are mystified and confused by the fact pattern that you laid out and the conclusions that you reached. It seems that there are two standards, and there is no consequence for these types of activities and dealing in a careless way with classified information. It seems to a lot of us that the average Joe, the average American, that if they had done what you laid out in your statement, that they'd be in handcuffs and they might be on their way to jail, and they probably should, and I think there is a legitimate concern that there is a double standard. If your name isn't Clinton or you're not part of the powerful elite, that Lady Justice will act differently. It is a concern that Lady Justice will take off that blindfold and come to a different conclusion.

Hillary Clinton created this mess. It wasn't Republicans. It wasn't anybody else. She made a very conscious decision. On the very day that she started her Senate confirmation, she set up and got a domain name and set up a system to avoid and bypass the safety, security, and the protocol of the State Department.

Classified information is classified for a reason. It is classified because if it were to get out into the public, there are nefarious actors, nation-states, others that want to do harm to this country, and there are people who put their lives on the line protecting and serving our country, and when those communications are not se-

cure, it puts their lives at jeopardy. This classified information is entrusted to very few, but there is such a duty and an obligation to protect that, to fall on your sword to protect that, and yet there doesn't seem to be any consequence.

You know, I was talking to Trey Gowdy, and he made a really good point with us yesterday. Mr. Gowdy said, you know, in your statement, Mr. Director, you mentioned that there was no precedent for this, but we believe that you have set a precedent, and it's a dangerous one. The precedent is if you sloppily deal with classified information, if you are cavalier about it—and it wasn't just an innocent mistake; this went on for years—that there is going to be no consequence.

We are a different nation in the United States of America. We are self-critical. Most nations would never do this, but we do it in the spirit of making ourselves better. There will be all kinds of accusations about political this and political that. I have defended your integrity every step of the way. You are the definitive voice. I stand by that, but I am mystified, and I am confused, because you listen to your fact pattern and come to the conclusion that there is no consequence, I don't know how to explain that. We will have constituents ask us. They'll get mad. They will pound the—you know, they're frustrated. They have seen this happen time and time again. I don't know how to explain it, and I hope that, through this hearing, we can stick to the facts and understand this, because there does seem to be two standards. There does seem to be no consequence, and I want to understand that, and I want to be able to explain that to the person that's sitting at home, and that is why we are here.

And so I yield back.

I now recognize the ranking member, Mr. Cummings.

Mr. CUMMINGS. Director Comey, thank you for being here today. I want to begin by commending you and the public servants at the FBI for the independent investigation you conducted. You had a thankless task. No matter what recommendation you made, you were sure to be criticized. There is no question that you were extremely thorough. In fact, some may even say you went too far in your investigation. But, of course, that was your job; that is your job.

Secretary Clinton has acknowledged that she made a mistake in using a personal email account, and you explained on Tuesday that she and her colleagues at the State Department were extremely careless with their emails, but after conducting this exhaustive review, you determined that no reasonable prosecutor would bring a case based on this evidence, and you and the career staff recommended against prosecution. Based on the previous cases you examined, if prosecutors had gone forward, they would have been holding the Secretary to a different standard from everyone else.

Amazingly—amazingly—some Republicans who were praising you just days ago for your independence, for your integrity, and your honesty instantly turned against you because your recommendation conflicted with the predetermined outcome they wanted. In their eyes, you had one job and one job only: to prosecute Hillary Clinton.

But you refused to do so, so now you are being summoned here to answer for your alleged transgressions, and in a sense, Mr. Director, you are on trial.

Contrary to the claims of your critics, there is absolutely no evidence that you made your recommendation for political reasons, no evidence that you were bribed or coerced or influenced, no evidence that you came to your conclusion based upon anything but the facts and the law. I firmly believe that your decision was not based on convenience but on conviction.

Today, House Republicans are doing what they always do, using taxpayers' money to continue investigating claims that have already been debunked just to keep them in the headlines one more day. When they hear a political siren, they rush toward it over and over again, even if the evidence is not there. Exhibit A, Majority Leader Kevin McCarthy, who admitted on national television that Republicans established the Benghazi Select Committee to bring down Secretary Clinton's poll numbers. I didn't say that; McCarthy said it. The fact was confirmed by a Republican staffer on that committee who reported that he was fired in part for not going along with the hyper focus on Secretary Clinton.

I give House Republicans credit. They certainly are not shy about what they are doing. They have turned political investigations into an art form.

If our concerns here today are with the proper treatment of classified information, then we should start with the review of our previous hearing on General David Petraeus, who pled guilty last year to intentionally and knowingly compromising highly classified information. The problem is, Mr. Director, we never had that hearing. This committee ignored that breach of national security because it did not match the political goals of the House Republicans.

If our concerns today were with finally addressing a broken classification system in which security levels are arbitrarily changed up and down, that would have been a legitimate goal, that would have been a valuable addition to reforming and improving our government. After all, we are the Government Reform Committee.

We could have held hearings here on Zika, the Zika virus, preventing gun massacres like the one in Orlando, or a host of other topics that could actually save people's lives, but that is not why we are here. That is not why our chairman called this emergency hearing 48 hours after you made your recommendation.

Everyone knows what this committee is doing. Honestly, I would not be surprised—and I say this with all seriousness—I would not be surprised if, tomorrow, Republicans set up a new committee to spend $7 million plus on why the FBI failed to prosecute Hillary Clinton.

Director Comey, let me conclude with this request. Even with all that I have said, I believe that there is a critical role for you today. I have listened carefully to the coverage on this issue, and I have heard people say as recently as this morning, 3 hours ago, that they were mystified by your decision. As a matter of fact, the chairman repeated it a minute ago. And so there is a perceived gap between the things you said on Tuesday and your recommendation. There is a gap, Mr. Director. So, in this moment—and this is a critical moment—I beg you to fill the gap, because when the gap is not

filled by you, it will be filled by others. Share with us, the American people, your process and your thinking; explain how you examined the evidence, the law, and the precedents; describe in clear terms how you and your team, career professionals, arrived at this decision. If you can do that today, if you can do that, that could go a long way toward people understanding your decision.

Finally, I want to make it clear that I condemn these completely unwarranted political attacks against you. They have attacked you personally. They have attacked your integrity. They have impugned your professionalism. And they have even suggested that you were somehow bought and paid for because you made your recommendation based upon the law and the facts.

I know you are used to working in the world of politics, but these attacks have been beyond the pale. So you do not deserve this. Your family does not deserve it. And the highly skilled and dedicated agents of the FBI do not deserve it.

I honor your professionalism and your service to our country. And, again, even if it takes till hell freezes over, I beg you to close the gap, tell us what happened between what you found and your decision so that not only the members of this panel and this Congress will understand but so that Americans will understand. And if you do that, if you do that, then it will be all worth it today.

With that, I yield back.

Mr. MICA. Mr. Chairman——

Chairman CHAFFETZ. I think—hold on one second, with your indulgence.

To the ranking member, of which I have the greatest respect, you asked for a hearing on General Petraeus and how that was dealt with; you got it. We will have one in this Oversight Committee. And the record will reflect that, in the Judiciary Committee, I repeatedly questioned Attorney General Holder, I repeatedly questioned the FBI Director about the disposition of that case, probably more than any Member in the House or Senate. And if you want a hearing, we will do that.

Mr. CUMMINGS. Will the gentlemen yield?

Chairman CHAFFETZ. Yes.

Mr. CUMMINGS. Thank you.

Chairman CHAFFETZ. Number two, you complained that we haven't done a hearing on Zika. The Oversight and Government Reform Committee, I believe, was the very first committee to actually do a hearing on Zika. That was chaired by Mr. Mica, and I am proud of the fact that we did a Zika hearing, and we did it first.

Mr. CUMMINGS. Will the gentleman yield?

Chairman CHAFFETZ. Sure.

Mr. CUMMINGS. Can we have another one, because the problem is still there——

Chairman CHAFFETZ. Absolutely.

Mr. CUMMINGS. —big time.

Chairman CHAFFETZ. Absolutely.

Mr. MICA. Mr. Chairman, I would ask for a unanimous consent request that we put the date of the hearing in the record at this time that I chaired—thank you—on Zika.

Chairman CHAFFETZ. Absolutely.

[The information follows:]

The Subcommittee on Transportation and Public Assets held a hearing on February 24, 2016, titled, "The Zika Virus: Coordination of a Multi- Agency Response."

Chairman CHAFFETZ. And the ranking member knows that we have held multiple hearings on the criminal justice and criminal justice reform. You asked for it. You are passionate about it. And we did do that as well. So to suggest we haven't addressed some of those issues, I think, is inaccurate.

Mr. CUMMINGS. I don't think I did that, Mr. Chairman, but, again, as late as yesterday, with the problem in Minnesota with an African American man being killed, I would like to have some hearings still on the criminal justice system. Thank you.

Chairman CHAFFETZ. Thank you.

Mr. CUMMINGS. Thank you very much.

Chairman CHAFFETZ. Without objection. I am going to work with you on that——

Mr. CUMMINGS. Thank you.

Chairman CHAFFETZ. —as I have every step of the way.

Mr. CUMMINGS. Thank you, Mr. Chairman. I appreciate it.

Chairman CHAFFETZ. Without objection, the chair is authorized to declare a recess at any time. We will hold the record open for 5 legislative days for any members who would like to submit a written statement.

We will now recognize our distinguished witness for our first panel. I am pleased to welcome the Honorable James Comey, the Director of the Federal Bureau of Investigations.

We welcome Director Comey, and thank you for being here.

Pursuant to committee rules, all witnesses are to be sworn before they testify. If you will please rise and raise and right hand.

Do you solemnly swear or affirm that the testimony you are about to give is the truth, the whole truth, and nothing but the truth.

Mr. COMEY. I do.

Chairman CHAFFETZ. Thank you.

Let the record reflect that the witness answered in the affirmative.

Mr. Comey, the floor is yours. You can take as long or as short as you would like. If you have any written statement that you would like to submit afterwards, we are happy to do that as well, and it will be made part of the record. The time is now yours.

Director Comey, you are recognized.

STATEMENT OF THE HONORABLE JAMES COMEY

Mr. COMEY. Thank you, Mr. Chairman, Mr. Cummings, members of the committee. I am proud to be here today representing the people of the FBI, who did this investigation, as they do all their work, in a competent, honest, and independent way. I believe this investigation was conducted consistent with the highest traditions of the FBI. Our folks did it in an apolitical and professional way, including our recommendation as to the appropriate resolution of this case.

As I said in my statement on Tuesday, I expected there would be significant public debate about this recommendation, and I am a big fan of transparency, so I welcome the conversation we are

going to have here today. And I do think a whole lot of folks have questions about, so why did we reach the conclusion we did, and what was our thinking? And I hope very much to get an opportunity to address that and to explain it. And I hope, at the end of day, people can disagree, can agree, but they will at least understand that the decision was made and the recommendation was made the way you would want it to be: by people who didn't give a hoot about politics but who cared about, what are the facts, what is the law, and how have similar people, all people, been treated in the past?

Maybe I could just say a few words at the beginning that would help frame how we think about this. There are two things that matter in a criminal investigation of a subject: What did the person do? And when they did that thing, what were they thinking?

When you look at the hundred years plus of the Justice Department's investigation and prosecution of the mishandling of classified information, those two questions are obviously present: What did the person do? Did they mishandle classified information? And when they did it, did they know they were doing something that was unlawful? That has been the characteristic of every charged criminal case involving the mishandling of classified information. I am happy to go through the cases in particular.

In our system of law, there's a thing called mens rea. It's important to know what you did, but when you did it, this Latin phrase "mens rea" means, what were you thinking? And we don't want to put people in jail unless we prove that they knew they were doing something they shouldn't do. That is the characteristic of all the prosecutions involving mishandling of classified information.

There is a statute that was passed in 1917 that, on its face, makes it a crime, a felony, for someone to engage in gross negligence. So that would appear to say: Well, maybe in that circumstance, you don't need to prove they knew they were doing something that was unlawful; maybe it's enough to prove that they were just really, really careless, beyond a reasonable doubt.

At the time Congress passed that statute in 1917, there was a lot of concern in the House and the Senate about whether that was going to violate the American tradition of requiring that, before you're going to lock somebody up, you prove they knew they were doing something wrong, and so there was a lot of concern about it. The statute was passed. As best I can tell, the Department of Justice has used it once in the 99 years since, reflecting that same concern. I know, from 30 years with the Department of Justice, they have grave concerns about whether it's appropriate to prosecute somebody for gross negligence, which is why they've done it once that I know of in a case involving espionage.

And so when I look at the facts we gathered here, as I said, I see evidence of great carelessness, but I do not see evidence that is sufficient to establish that Secretary Clinton or those with whom she was corresponding both talked about classified information on email and knew, when they did it, they were doing something that was against the law, right?

So, given that assessment of the facts and my understanding of the law, my conclusion was and remains no reasonable prosecutor would bring this case. No reasonable prosecutor would bring the

second case in a hundred years focused on gross negligence. And so I know that's been a source of some confusion for folks. That's just the way it is. I know the Department of Justice. I know no reasonable prosecutor would bring this case. I know a lot of my former friends are out there saying they would. I wonder where they were the last 40 years, because I'd like to see the cases they brought on gross negligence. Nobody would; nobody did.

So my judgment was the appropriate resolution of this case was not with a criminal prosecution. As I said, folks can disagree about that, but I hope they know that view, not just my view but of my team, was honestly held, fairly investigated, and communicated with unusual transparency, because we know folks care about it.

So I look forward to this conversation. I look forward to answering as many questions as I possibly can. I'll stay as long as you need me to stay, because I believe transparency matters tremendously. And I thank you for the opportunity.

Chairman CHAFFETZ. Thank you, Director. I'm going to recognize myself here.

Physically, where were Hillary Clinton's servers?

Mr. COMEY. The operational server was in the basement of her home in New York. The reason I'm answering it that way is because sometimes, after they were decommissioned, they were moved to other facilities, storage facilities, but the live device was always in the basement.

Chairman CHAFFETZ. Was that an authorized or unauthorized location?

Mr. COMEY. It was an unauthorized location for the transmitting of classified information.

Chairman CHAFFETZ. Is it reasonable or unreasonable to expect Hillary Clinton would receive and send classified information?

Mr. COMEY. As Secretary of State? Reasonable that the Secretary of State would encounter classified information in the course of the Secretary's work.

Chairman CHAFFETZ. Via email?

Mr. COMEY. Sure, depending upon the nature of the system. To communicate classified information, it would have to be a classified-rated email system.

Chairman CHAFFETZ. But you did find more than 100 emails that were classified that had gone through that server, correct?

Mr. COMEY. Right. Through an unclassified server, correct.

Chairman CHAFFETZ. Yes. So Hillary Clinton did come to possess documents and materials containing classified information via email on these unsecured servers, correct?

Mr. COMEY. That is correct.

Chairman CHAFFETZ. Did Hillary Clinton lie?

Mr. COMEY. To the FBI? We have no basis to conclude she lied to the FBI.

Chairman CHAFFETZ. Did she lie to the public?

Mr. COMEY. That's a question I'm not qualified to answer. I can speak about what she said to the FBI.

Chairman CHAFFETZ. Did Hillary Clinton lie under oath?

Mr. COMEY. To the—not to the FBI, not in the case we were working.

Chairman CHAFFETZ. Did you review the documents where Congressman Jim Jordan asked her specifically, and she said, quote, "There was nothing marked classified on my emails, either sent or received," end quote?

Mr. COMEY. I don't remember reviewing that particular testimony. I'm aware of that being said, though.

Chairman CHAFFETZ. Did the FBI investigate her statements under oath on this topic?

Mr. COMEY. Not to my knowledge. I don't think there has been a referral from Congress.

Chairman CHAFFETZ. Do you need a referral from Congress to investigate her statements under oath?

Mr. COMEY. Sure do.

Chairman CHAFFETZ. You'll have one. You'll have one in the next few hours.

Did Hillary Clinton break the law?

Mr. COMEY. In connection with her use of the email server, my judgment is that she did not.

Chairman CHAFFETZ. Did you—you're just not able to prosecute it, or did Hillary Clinton break the law?

Mr. COMEY. Well, I don't want to give an overly lawyerly answer, but the question I always look at is, is there evidence that would establish beyond a reasonable doubt that somebody engaged in conduct that violated a criminal statute? And my judgment here is there is not.

Chairman CHAFFETZ. The FBI does background checks. If Hillary Clinton applied for the job at the FBI, would the FBI give Hillary Clinton a security clearance?

Mr. COMEY. I don't want to answer a hypothetical. The FBI has a robust process in which we adjudicate the suitability of people for employment in the Bureau.

Chairman CHAFFETZ. Given the fact pattern you laid out less than 48 hours ago, would a person who had dealt with classified information like that, would that person be granted a security clearance at the FBI?

Mr. COMEY. It would be a very important consideration in the suitability determination.

Chairman CHAFFETZ. You're kind of making my point, Director. The point being, because I injected the word "Hillary Clinton," you gave me a different answer, but if I came up to you and said that this person was extremely careless with classified information; the exposure to hostile actors; had used—despite warnings—created unnecessary burdens and exposure; if they said that they had one device and you found out that they had multiple devices; if there had been email chains with somebody like Jake Sullivan asking for classification changes, you're telling me that the FBI would grant a security clearance to that person?

Mr. COMEY. I'm not—I hope I'm giving a consistent—I'm not saying what the answer would be. I'm saying that would be an important consideration in a suitability determination for anybody.

Chairman CHAFFETZ. And just—personally, I just think that sounds like a bit of a political answer, because I can't imagine that the FBI would grant a security clearance to somebody with that fact pattern. Do you agree or disagree with that?

Mr. COMEY. I'll say what I said before: again, it's very hard to answer in a hypothetical. I'll repeat it. It would be a very important consideration in a suitability determination.

Chairman CHAFFETZ. Did Hillary Clinton do anything wrong?

Mr. COMEY. What do you mean by "wrong"?

Chairman CHAFFETZ. I think it's self-evident.

Mr. COMEY. Well, I'm a lawyer. I'm an investigator. And I'm—I hope—a normal human being.

Chairman CHAFFETZ. Do you really believe there should be no consequence for Hillary Clinton in how she dealt with this?

Mr. COMEY. Well, I didn't say—I hope folks remember what I said on Tuesday. I didn't say there's no consequence for someone who violates the rules regarding the handling of classified information. There are often very severe consequences in the FBI involving their employment, involving their pay, involving their clearances. That's what I said on Tuesday. And I hope folks walk away understanding that, just because someone's not prosecuted for mishandling classified information, that doesn't mean, if you work in the FBI, there aren't consequences for it.

Chairman CHAFFETZ. So if Hillary Clinton or if anybody had worked at the FBI, under this fact pattern, what would you do to that person?

Mr. COMEY. There would be a security review and an adjudication of their suitability, and a range of discipline could be imposed from termination to reprimand and, in between, suspensions, loss of clearance. So you could be walked out or you could—depending upon the nature of the facts, you could be reprimanded, but there is a robust process to handle that.

Chairman CHAFFETZ. I've gone past my time.

I yield back.

I now recognize the ranking member, Mr. Cummings.

Mr. CUMMINGS. Thank you very much.

Director Comey—and I want to thank you very much for being here today, especially on such short notice. You and your staff should be commended for the thorough and dedicated review you conducted. Unfortunately, some of my colleagues are now attacking you personally because your final recommendation conflicted with their preconceived political outcome in this case.

Some have tried to argue that this case is far worse than the case of General David Petraeus, who was convicted in 2015 of knowingly and intentionally compromising highly classified information. In fact, one very vocal politician we all know said this, and I quote: "If she isn't indicted, the only reason is because the Democrats are protecting her. She is being protected 100 percent, because you look at David—General Petraeus, you look at all the other people that did a fraction of what she did, but she has much worse judgment than he had, and she's getting away with it, and it's unfair to him," end of quote.

Director Comey, you were the Director of the FBI when General Petraeus pled guilty. Is that right?

Mr. COMEY. Yes.

Mr. CUMMINGS. If I understand that case correctly, General Petraeus kept highly classified information in eight personal notebooks at his private residence. Is that correct?

Mr. COMEY. That is correct.

Mr. CUMMINGS. According to the filings in that case, this notebook included the identities of covert officers. They also included war strategy, intelligence capabilities, diplomatic discussions, quotes and deliberative discussions from high-level National Security Council meetings and discussions with the President. General Petraeus shared his information with his lover and then biographer. He was caught on audiotape telling her, and I quote, "I mean, they are highly classified, some of them. They don't have it on—on it, but, I mean, there's code word stuff in there," end of quote.

Director Comey, what did General Petraeus mean when he said he intentionally shared, quote, "code word" information with her? What does that mean?

Mr. COMEY. The Petraeus case, to my mind, illustrates perfectly the kind of cases the Department of Justice is willing to prosecute. Even there, they prosecuted him for a misdemeanor. In that case, you had vast quantities of highly classified information, including special—sensitive compartmented information—that's the reference to code words—a vast quantity of it, not only shared with someone without authority to have it, but we found it in a search warrant hidden under the insulation in his attic, and then he lied to us about it during the investigation.

So you have obstruction of justice. You have intentional misconduct and a vast quantity of information. He admitted he knew that was the wrong thing to do. That is a perfect illustration of the kind of cases that get prosecuted. In my mind, it illustrates, importantly, the distinction to this case.

Mr. CUMMINGS. And General Petraeus did not admit to these facts when the FBI investigators first interviewed him. Did he?

Mr. COMEY. No. He lied about it.

Mr. CUMMINGS. But he did admit to these facts in a plea agreement. Is that correct?

Mr. COMEY. Yes.

Mr. CUMMINGS. Here's what the Department filing said about General Petraeus, and I quote: "The acts taken by defendant David Howell Petraeus were in all respects knowing and deliberate and were not committed by mistake, accident, or other innocent reason," end of quote.

Is that an accurate summary, in your view, Director Comey?

Mr. COMEY. Yes. It actually leaves out an important part of the case, which is the obstruction of justice.

Mr. CUMMINGS. Was he charged with obstruction of justice?

Mr. COMEY. No.

Mr. CUMMINGS. And why not?

Mr. COMEY. A decision made by the leadership of the Department of Justice not to insist upon a plea to that felony.

Mr. CUMMINGS. So the question is, do you agree with the claim that General Petraeus, and I quote, "got in trouble for far less," end of quote?

Mr. COMEY. No.

Mr. CUMMINGS. Do you agree with that statement?

Mr. COMEY. No. It's the reverse.

Mr. CUMMINGS. And what do you mean by that?

Mr. COMEY. His conduct, to me, illustrates the categories of behavior that mark the prosecutions that are actually brought: clearly intentional conduct, knew what he was doing was a violation of the law, huge amounts of information that, even if you couldn't prove he knew it, it raises the inference that he did it—right—an effort to obstruct justice. That combination of things makes it worthy of a prosecution, a misdemeanor prosecution but a prosecution nonetheless.

Mr. CUMMINGS. Sitting here today, do you stand by the FBI's recommendation to prosecute General Petraeus?

Mr. COMEY. Oh, yeah.

Mr. CUMMINGS. Do you stand by the FBI's recommendation not to prosecute Hillary Clinton?

Mr. COMEY. Yes.

Mr. CUMMINGS. Director Comey, how many times have you testified before Congress about the General Petraeus case? Do you know?

Mr. COMEY. I don't think I've ever testified—I don't think I've testified about it at all. I don't think so.

Mr. CUMMINGS. With that, I would yield back.

Chairman CHAFFETZ. I have to check the record, but I believe I asked you a question about it at the time, but maybe not.

Mr. COMEY. You could have. That's why I was——

Chairman CHAFFETZ. Yeah, yeah.

Mr. COMEY. —squinching my face. It could have been at a Judiciary Committee hearing I was asked about it.

Chairman CHAFFETZ. Yeah.

We'll now recognize the gentleman from South Carolina, Mr. Gowdy, for 5 minutes.

Mr. GOWDY. Good morning, Director Comey. Secretary Clinton said she never sent or received any classified information over her private email. Was that true?

Mr. COMEY. Our investigation found that there was classified information sent——

Mr. GOWDY. So it was not true?

Mr. COMEY. Right. That's what I said.

Mr. GOWDY. Okay. Well, I'm looking for a little shorter answer so you and I are not here quite as long.

Secretary Clinton said there was nothing marked classified on her emails either sent or received. Was that true?

Mr. COMEY. That's not true. There were a small number of portion markings on, I think, three of the documents.

Mr. GOWDY. Secretary Clinton said: I did not email any classified material to anyone on my email. There is no classified material.

Was that true?

Mr. COMEY. No. There was classified material emailed.

Mr. GOWDY. Secretary Clinton said she used just one device. Was that true?

Mr. COMEY. She used multiple devices during the 4 years of her term as Secretary of State.

Mr. GOWDY. Secretary Clinton said all work-related emails were returned to the State Department. Was that true?

Mr. COMEY. No. We found work-related emails, thousands, that were not returned.

Mr. GOWDY. Secretary Clinton said neither she nor anyone else deleted work-related emails from her personal account. Was that true?

Mr. COMEY. That's a harder one to answer. We found traces of work-related emails on devices or in slack space, whether they were deleted or whether when a server was changed out, something happened to them. There's no doubt that there were work-related emails that were removed electronically from the email system.

Mr. GOWDY. Secretary Clinton said her lawyers read every one of the emails and were overly inclusive. Did her lawyers read the email content individually?

Mr. COMEY. No.

Mr. GOWDY. Well, in the interests of time and because I have a plane to catch tomorrow afternoon, I'm not going to go through any more of the false statements, but I am going to ask you to put on your old hat.

False exculpatory statements, they are used for what?

Mr. COMEY. Well, either for a substantive prosecution or for evidence of intent in a criminal prosecution.

Mr. GOWDY. Exactly. Intent and consciousness of guilt, right? Is that right?

Mr. COMEY. Right.

Mr. GOWDY. Consciousness of guilt and intent.

Mr. COMEY. Uh-huh.

Mr. GOWDY. In your old job, you would prove intent, as you just referenced, by showing the jury evidence of a complex scheme that was designed for the very purpose of concealing the public record, and you would be arguing, in addition to concealment, the destruction that you and I just talked about or certainly the failure to preserve, you would argue all of that under the heading of content—you would also—intent.

You would also be arguing the pervasiveness of the scheme, when it started, when it ended, and the number of emails, whether they were originally classified or up classified. You would argue all of that under the heading of intent.

You would also probably, under common scheme or plan, argue the burn bags of daily calendar entries or the missing daily calendar entries as a common scheme or plan to conceal.

Two days ago, Director, you said a reasonable person in her position should have known a private email was no place to send and receive classified information. You're right. An average person does know not to do that. This is no average person. This is a former First Lady, a former United States Senator, and a former Secretary of State that the President now contends is the most competent, qualified person to be president since Jefferson. He didn't say that in 2008, but he says it now. She affirmatively rejected efforts to give her a State.gov account, she kept these private emails for almost 2 years, and only turned them over to Congress because we found out she had a private email account.

So you have a rogue email system set up before she took the oath of office, thousands of what we now know to be classified emails, some of which were classified at the time, one of her more frequent email comrades was, in fact, hacked, and you don't know whether

or not she was, and this scheme took place over a long period of time and resulted in the destruction of public records, and yet you say there is insufficient evidence of intent. You say she was extremely careless but not intentionally so.

You and I both know intent is really difficult to prove. Very rarely do defendants announce: On this day, I intend to break this criminal code section. Just to put everyone on notice, I am going to break the law on this date.

It never happens that way. You have to do it with circumstantial evidence, or if you're Congress and you realize how difficult it is to prove specific intent, you will formulate a statute that allows for gross negligence.

My time is out, but this is really important. You mentioned there's no precedent for criminal prosecution. My fear is there still isn't. There's nothing to keep a future Secretary of State or President from this exact same email scheme or their staff. And my real fear is this—it's what the chairman touched upon—this double track justice system that is, rightly or wrongly, perceived in this country that if you are a private in the Army and you email yourself classified information, you will be kicked out, but if you are Hillary Clinton and you seek a promotion to Commander in Chief, you will not be.

So what I hope you can do today is help the average—the reasonable person you made reference to, the reasonable person understand why she appears to be treated differently than the rest of us would be.

With that, I would yield back.

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

Mrs. MALONEY. Director, thank you for your years of public service. You have distinguished yourself as the assistant U.S. attorney for both the Southern District of New York and the Eastern District of Virginia. That's why you were appointed by President Bush to be the Deputy Attorney General at the Department of Justice and why President Obama appointed you as the Director of the FBI in 2013.

Despite your impeccable reputation for independence and integrity, Republicans have turned on you with a vengeance immediately after you announced your recommendation not to pursue criminal charges against Secretary Clinton. Let me give you some examples. Representative Turner said, and I quote: "The investigation by the FBI is steeped in political bias," end quote.

Was your investigation steeped in political bias, yes or no?

Mr. COMEY. No. It was steeped in no kind of bias.

Mrs. MALONEY. Thank you. The Speaker of the House, Paul Ryan, was even more critical. He accused you of not applying the law equally. He said your recommendation shows, and I quote, "the Clintons are living above the law. They're being held to a different set of standards. That is clearly what this looks like," end quote.

How do you respond to his accusations that you held the Clintons to a different set of standards than anyone else? Did you hold them to a different standard or the same standard?

Mr. COMEY. It's just not—it's just not accurate. We try very hard to apply the same standard whether you're rich or poor, white or black, old or young, famous or not known at all.

I just hope folks will take the time to understand the other cases, because there's a lot of confusion out there about what the facts were of the other cases that I understand lead good people, reasonable people, to have questions.

Mrs. MALONEY. Senator Cruz also criticized you. He said that there are, and I quote, "serious concerns about the integrity of Director Comey's decision." He stated that you, quote, you "had rewritten a clearly worded Federal criminal statute."

Did you rewrite the law in any way or rewrite any statute?

Mr. COMEY. No.

Mrs. MALONEY. Now, I hesitate, I truly hesitate to mention the next one, but Donald Trump took these conspiracy theories to a totally new level. He said, and I quote: "It was no accident that charges were not recommended against Hillary the exact same day as President Obama campaigned with her for the first time."

So did you plan the timing of your announcement to help Secretary Clinton's campaign event on Tuesday?

Mr. COMEY. No. The timing was entirely my own. Nobody knew I was going to do it, including the press. I'm very proud of the way the FBI—nobody leaked that. We didn't coordinate it, didn't tell. Just not a consideration.

Mrs. MALONEY. Thank you. Mr. Trump also claimed that Secretary Clinton bribed the Attorney General with an extension of her job and I guess this somehow affected your decision.

I know it's a ridiculous question, but I have to ask it. Did you make your decision because of some kind of bribe to the Attorney General?

Mr. COMEY. No.

Mrs. MALONEY. I tell you, are you surprised, as I am, by the intensity of the attacks from the GOP on you after having made a decision, a thoughtful decision, an independent decision with the professional staff of the FBI?

Mr. COMEY. I'm not surprised by the intense interest and debate. I predicted it. I think it's important that we talk about these things. They inevitably become focused on individual people. That's okay. We'll just continue to have the conversation.

Mrs. MALONEY. I believe that what we're seeing today is that if the GOP does not like the results of an investigation or how it turns out—and we saw they originally were lauding you—the minute you made your announcement, they're now attacking you, the same people. And now I predict they'll be calling for more hearings, more investigations, all at the expense of the taxpayer, and they do this instead of working on what the American people really care about. They want Congress to focus on jobs, the environment, Homeland Security, the security of our Nation, affordable childcare, affordable college educations, and an economy that works and helps all people.

I thank you for performing your job with distinction and the long history of your whole profession of integrity and independence. And thank you very much. My time has expired.

Chairman CHAFFETZ. I thank the gentlewoman.

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

Mr. JORDAN. Thank you, Mr. Chairman.

Director, thank you for being with us. On Tuesday, you said any reasonable person in Secretary Clinton's position should have known that an unclassified system was no place for these conversations. You said on Tuesday some of her emails bore classified markings, and you also said on Tuesday there were potential violations of the appropriate statutes.

Now, I know a bunch of prosecutors back home would look at that fact pattern, look at that evidence, you even referenced in your opening statement, some of your prosecutor—friends in the prosecution business have been on TV and said they would have looked at that same evidence and they would have taken it to a grand jury, but on Tuesday, you said and, today, in your opening statement, you said no reasonable prosecutor would bring such a case. And then in your statement Tuesday, you cite factors that helped you make that decision and make that statement, and one of the factors you said was consider the context of a person's actions.

Now, typically, when I hear "context" in the course of a criminal investigation, it's from the defense side, not the prosecution side; it's at the end of the case, after there's been a trial and a guilty verdict; and it's during the sentencing phase, mitigating circumstances. That's the context we typically think about, but you said it on the front end. You said "consider the context of the person's actions," and so I'm curious, what does "consider the context" mean? Because a lot of Americans are thinking just what the chairman talked about in his opening statement, that there are two standards, one for we the people and one for the politically connected. A lot of folks I get the privilege of representing back in Ohio think that when you said "consider the context," they think that's what Mr. Gowdy just talked about, the fact that she's a former First Lady, former Secretary of State, former Senator, major party's nominee for the highest office in the land, and, oh, by the way, her husband just met with the individual you work with at an airport in Arizona 5 days ago.

So you said none of that influenced your decision, but tell us what "consider the context" means.

Mr. COMEY. Yeah. Thank you, Mr. Jordan. What I was trying to capture is the fact that the exercise of prosecutorial discretion is always a judgment call, it is in every single case, and among the things you consider are, what was this person's background? What was the circumstances of the offense? Were they drunk? Were they inflamed by passion? Was it somebody who had a sufficient level of education and training and experience that we can infer certain things from that, to consider the entire circumstances of the person's offense conduct and background? I did not mean to consider political context.

Mr. JORDAN. Okay. The entire circumstances, and Mr. Gowdy just talked about this scheme, remember what she did, right? She sets up this unique server arrangement. She alone controls it. On that server, on that email system are her personal emails, her work-related emails, Clinton Foundation information, and, now we know, classified information. This gets discovered. We find out this

arrangement exists. Then what happens? Her lawyers, her legal team decides which ones we get and which ones they get to keep. They made the sort on front end. And then we found out the ones that they kept and didn't give to us, didn't give to the American people, didn't give to Congress, the ones they kept, they destroyed them. And you don't have to take my word. I'll take what you said on Tuesday. They deleted all emails that they did not return to the State Department, and the lawyers cleaned their devices in such a way as to preclude complete forensic recovery. Now, that sounds like a fancy way of saying they hid the evidence, right? And you just told Mr. Gowdy thousands of emails fell into those categories. Now, that seems to me to provide some context to what took place here.

Did Secretary Clinton's legal team—excuse me. Let me ask it this way. Did Secretary Clinton know her legal team deleted those emails that they kept from us?

Mr. COMEY. I don't believe so.

Mr. JORDAN. Did Secretary Clinton approve those emails being deleted?

Mr. COMEY. I don't think there was any specific instruction or conversation between the Secretary and her lawyers about that.

Mr. JORDAN. Did you ask that question?

Mr. COMEY. Yes.

Mr. JORDAN. Did Secretary Clinton know that her lawyers cleaned devices in such a way as to preclude complete forensic recovery?

Mr. COMEY. I don't believe that she did.

Mr. JORDAN. Did you ask that question?

Mr. COMEY. Yes.

Mr. JORDAN. Do you see how someone could view the context of what she did? Set up a private system. She alone controlled it. She kept everything on it. We now know from Ms. Abedin's deposition that they did it for that very reason, so no one could see what was there, based on the deposition Ms. Abedin gave. And then when they got caught, they deleted what they had and they scrubbed their devices.

Is that part of the context in evaluating this decision?

Mr. COMEY. Sure. Sure. And understand what inferences can be drawn from that collection of facts, of course.

Mr. JORDAN. All right.

Mr. Chairman, I yield back.

Chairman CHAFFETZ. I thank the gentleman.

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

Ms. NORTON. Thank you, Mr. Chairman.

Director Comey, I appreciate your conduct of this investigation in a nonpartisan way, in keeping with the sterling reputation, which has led Presidents of both parties to appoint you to highly placed law enforcement positions in our Federal Government.

I want to say for the record that this hearing, where you call the prosecutor—and Mr. Comey stands in the place of the prosecutor, because the Attorney General has accepted entirely the FBI's recommendations—where you call the prosecutor to give account for the decision to prosecute or not a particular individual raises seri-

ous questions of separation of powers. And, particularly, when you're questioning the prosecutor's decision with respect to the decision to prosecute or not a particular individual, it raises serious bill of attainder constitutional questions.

These hearings are so often accusatory that they yield no guidance as to how to conduct business in the future, and that's the way it looks. It looks as though that is how this hearing is going.

Now, of course, now, everyone understands in the abstract why it is important for security reasons to use official government mail—or email rather than private accounts—private email if security matters are involved. Now, that's a very broad, wide proposition.

Now, there are no rules, so far as I know, requiring Members of Congress to use their—as to how they use their official email accounts, whether involving security or not. The chairman of this committee lists his personal account, for example, on his business card. I'm—no one says that's wrong. I don't know if it's wrong or right, because there's no guidance. Federal agency employees, Members of Congress often have secure information or at least sensitive information that shouldn't be made public. Some of our Members are on the Intelligence Committee or the defense committee or even this committee and may have such matters. Some of these matters may concern national security issues, and—I don't know—if something as sensitive as the itinerary if you're going on a codel as to the route you are taking and where you will be, all of that could be on people's personal emails.

Of course, this is the legislative branch, and I spoke of the separation of powers, and I'm not indicating that there should be a governmentwide sense that is ordained from on high, but there ought to be rules that everybody understands, especially after the Clinton episode, about the use of personal email. So I'd like your insight for guidance as far as other Federal employees are concerned or even Members of Congress and their staff, because I think we could learn from this episode.

So, strictly from a security standpoint, do you believe that Federal employees, staff, even Members of Congress, should attempt guidance on the issue of the use of personal emails versus some official form of communication? What should we learn from the process the Secretary has gone through? I'm sure there will be questions about how there was even confusion, for example, in the State Department, but what should we learn when it comes to our own use of email or the use of Federal employees on this question?

Mr. COMEY. Can I answer, Mr. Chairman?

Chairman CHAFFETZ. Sure.

Mr. COMEY. The most important thing to learn is that an unclassified email system is no case for an email conversation about classified matters. And by that I mean either sending a document as an attachment over unclassified email that is classified or having a conversation about something that is a classified subject on an unclassified email system. That's the focus of the concern. That's the focus of this investigation. That it was also a personal email adds to the concern about the case because of the security vulnerabilities associated with a personal system, but the root of the problem is people using unclassified systems to conduct busi-

ness that is classified. And so all of us should have access to, if we have access to classified information, classified communication systems. The FBI has three levels: unclassified system, a secret system, and a top secret system. You can email on all three, but you need to make sure you don't email on the unclass system, even if that's a government classified system, about matters that are classified. That's the important lesson learned. Everybody ought to be aware of it. Everybody ought to be trained on it. We spend a lot of time training on it in the FBI to make sure folks are sensitive to the need to move a classified discussion, even if it doesn't involve sending a document, to the appropriate forum.

Ms. NORTON. Members of Congress included?

Mr. COMEY. Of course.

Ms. NORTON. Thank you, Mr. Chairman.

Chairman CHAFFETZ. We'll now recognize the gentleman from Florida, Mr. DeSantis, for 5 minutes.

Mr. DESANTIS. Director, and the reason why that's so important is because if top secret information is compromised, that could damage our national security, correct?

Mr. COMEY. Yes, by definition.

Mr. DESANTIS. And American lives are at stake in some instances, correct?

Mr. COMEY. Yes.

Mr. DESANTIS. You mentioned a lot of people were upset that there were no consequences for Secretary Clinton, but in your statement, you did point out that administrative and security consequences would be appropriate if someone demonstrated extreme carelessness for classified information.

So those consequences, that would include potentially termination of Federal employment?

Mr. COMEY. Correct.

Mr. DESANTIS. It could include revocation of security clearance?

Mr. COMEY. Yes.

Mr. DESANTIS. And it could include ineligibility for future employment in national security positions, correct?

Mr. COMEY. It could.

Mr. DESANTIS. Now, would you as the FBI Director allow someone in the employ of your agency to work in a national security capacity if that person had demonstrated extreme carelessness in handling top secret info?

Mr. COMEY. The best answer to that is we would look very closely at that in a suitability determination. It's hard to answer in the abstract "yes" in all cases, "no" in all cases, but it would be a very important suitability scrub.

Mr. DESANTIS. So there would be instances where someone could be extremely careless but still maintain confidence? I mean, we have a lot of people who are very competent in this country who would love to work for your agency, but yet it would be—potentially you would allow somebody to be extremely careless and continue on?

Mr. COMEY. That's the trouble with answering a hypothetical. I could imagine if it was a long time ago, and it was a small amount of conduct or something. That's why it's hard to say other than it would be a very important part of the——

Mr. DESANTIS. Let's just put it this way. Would being extremely careless in handling top secret information expose an employee of the FBI to potential termination?

Mr. COMEY. Yes.

Mr. DESANTIS. Why shouldn't U.S. officials use mobile devices when traveling to foreign countries, especially if they're discussing classified or sensitive information?

Mr. COMEY. Because the mobile device will transmit its signal across networks that are likely controlled or at least accessed by that hostile power.

Mr. DESANTIS. And that's the guidance that the FBI gives all officials when they're traveling overseas. That's still good guidance, correct?

Mr. COMEY. That's good guidance.

Mr. DESANTIS. How did top secret information end up on the private server? Because your statement addressed Secretary Clinton. You did not address any of her aides in your statement. Attorney General Lynch exonerated everybody. That information just didn't get there on its own, so how did it get there? Were you able to determine that?

Mr. COMEY. Yes. By people talking about a top secret subject in an email communication.

Mr. DESANTIS. So it was——

Mr. COMEY. It's not about forwarding a top secret document; it's about having a conversation about a matter that is top secret.

Mr. DESANTIS. And those were things that were originated by Secretary Clinton's aides and then sent to her, which would obviously be in her server, but it was also included Secretary Clinton originating those emails, correct?

Mr. COMEY. That's correct. In most circumstances, it initiated with aides starting a conversation. In the one involving top secret information, Secretary Clinton, though, also not only received but also sent emails that talked about the same subject.

Mr. DESANTIS. And of that top secret information that you found, would somebody who was sophisticated in those matters, should it have been obvious to them that that was very sensitive information?

Mr. COMEY. Yes.

Mr. DESANTIS. So I guess my issue about knowledge of what you're doing is in order for Secretary Clinton to have access to top secret/SCI information, didn't she have to sign a form with the State Department acknowledging her duties and responsibilities under the law to safeguard this information?

Mr. COMEY. Yes. Anybody who gets access to SCI, sensitive compartmented information, would sign what's called a read-in form that lays that out. I'm sure Members of Congress have seen the same thing.

Mr. DESANTIS. And it stresses in that document and other training people would get that there are certain requirements to handling certain levels of information. For example, a top secret document, that can't even be on your secret system at the FBI, correct?

Mr. COMEY. Correct.

Mr. DESANTIS. So you have to follow certain guidelines. And I guess my question is, is she's a very sophisticated person. She did execute that document, correct?

Mr. COMEY. Yes.

Mr. DESANTIS. And her aides who were getting the classified information, they executed similar documents to get a security clearance, correct?

Mr. COMEY. I believe so.

Mr. DESANTIS. And she knowingly clearly set up her own private server in order to—well, actually, let me ask you that. Was the reason she set up her own private server, in your judgment, because she wanted to shield communications from Congress and from the public?

Mr. COMEY. 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.

Mr. DESANTIS. So the question is, is very sophisticated—this is information that clearly anybody who had knowledge of security information would know that it would be classified—but I'm having a little bit of trouble to see, how would you not then know that that was something that was inappropriate to do?

Mr. COMEY. Well, I just want to take one of your assumptions about sophistication. I don't think that our investigation established that she was actually particularly sophisticated with respect to classified information and the levels and the treatment, and so far as we can tell——

Mr. DESANTIS. Isn't she an original classification authority, though?

Mr. COMEY. Yes, sir. Yes, sir.

Mr. DESANTIS. Good grief. Well, I appreciate you coming. And I yield back the balance of my time.

Chairman CHAFFETZ. I thank the gentleman. I ask unanimous consent to enter into the record two documents that Mr. DeSantis referred to. One is the Sensitive Compartmented Information Nondisclosure Agreement. The other one is the Classified Information Nondisclosure Agreement. Both signed by Hillary Rodham Clinton. Without objection, so ordered.

Chairman CHAFFETZ. I now recognize the gentleman from Missouri, Mr. Clay, for 5 minutes.

Mr. CLAY. Thank you, Mr. Chairman. And thank you, Director Comey, for being here today and for the professionals whom you lead at the FBI. Two years ago after my urgent request to then-former Attorney General Eric Holder for an expedited Justice Department investigation into the tragic death of Michael Brown in Ferguson, Missouri, I witnessed firsthand the diligence, professionalism, and absolute integrity of your investigators. And I have no doubt that was the case in this matter as well. I did not think it was possible for the majority to exceed their unprecedented arrogant abuse of official channels and Federal funds that we have witnessed over the past 2 years as they have engaged in a partisan political witch hunt at taxpayer expense against Secretary Clinton.

But I was wrong. This proceeding is just a sequel to that very bad act. And the taxpayers will get the bill. It is a new low, and

it violates both House rules and the rules of this committee. So with apologies to you and the FBI for this blatantly partisan proceeding, let me return to the facts of this case as you have clearly outlined them.

First question: Did Secretary Clinton or any member of her staff intentionally violate Federal law?

Mr. COMEY. We did not develop clear evidence of that.

Mr. CLAY. Did Secretary Clinton or any member of her staff attempt to obstruct your investigation?

Mr. COMEY. We did not develop evidence of that.

Mr. CLAY. In your opinion, do the mistakes Secretary Clinton has already apologized for and expressed regret for rise to a level that would be worthy of Federal prosecution?

Mr. COMEY. As I said Tuesday, our judgment, not just mine, but the team's judgment at the FBI, is that the Justice Department would not bring such a case. No Justice Department under any—whether Republican or Democrat administration.

Mr. CLAY. Thank you for that response. I know the FBI pays particular attention to groups by training agents and local law enforcement officers and participating in local hate crime working groups. Is that right?

Mr. COMEY. Yes, sir.

Mr. CLAY. Some of these organizations seem relatively harmless. But others appear to be very dangerous and growing. Some even promote genocide in their postings and rhetoric online. In your experience, how dangerous are these groups and have they incited violence in the past?

Mr. COMEY. I think too hard to answer, Congressman, in the abstract. There are some groups that are dangerous. There are some groups that are exercising important protection—protected speech under the First Amendment.

Mr. CLAY. Okay. Let me ask a more direct question. A gentleman named Andrew Anglin is the editor of a Web site called The Daily Stormer that is dedicated to the supremacy of the white race as well as attacking Jews, Muslims, and others. The Web site features numerous posts with the hashtag "white genocide" to protest what they contend is an effort to eliminate the white race. Are you familiar with this movement?

Mr. COMEY. I'm not.

Mr. CLAY. Okay. Well, this hashtag has been promoted all over social media by a growing number of white supremacists. For example, one Nazi sympathizer tweeted repeatedly using the handle @whitegenocidetm. Are you concerned as some groups are increasing their followers in this way, particularly if some of those followers in this way, particularly if some of those followers could become violent?

Mr. COMEY. I don't know the particular enough to comment, Congressman. We are always concerned when people go beyond protected speech, which we do not investigate, to moving towards acts of violence. And so our duty is to figure out when have people walked outside the First Amendment protection and are looking to kill folks or hurt folks. But I don't know enough to comment on the particular.

Mr. CLAY. I see. Well, one of my biggest concerns is that certain public figures are actually promoting these dangerous groups even further. And as you may know, one of our most vocal candidates for President retweeted @whitegenocidetm. Three weeks later, he did it again. Two days after that, he retweeted a different user whose image also included the term "white genocide," and that's not even all of them. Director Comey, don't these actions make it easier for these racist groups to recruit even more supporters?

Mr. COMEY. I don't think I'm in a position to answer that in an intelligent way sitting here.

Mr. CLAY. Well, I appreciate you trying. And thank you, Mr. Director, for your exceptional and principled service to our country. I yield back.

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

Mrs. LUMMIS. Welcome, Director. And thank you so much for being here. My phone has been ringing off the hook in my Washington office, in my Wyoming office, from constituents who don't understand how this conclusion was reached. So I appreciate your being here to help walk us through it. And here's the issue that the people that are calling me from Wyoming are having. They have access to this statute. It's Title 18 U.S. Code 1924. And I'm going to read you this statute. It says, "Whoever being an officer, employee, contractor, or consultant to the United States and by virtue of his office employment, position, or contract becomes possessed of documents or materials containing classified information of the United States knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year or both."

Armed with that information, they're wondering how Hillary Clinton, who is also an attorney, and attorneys are frequently held to a higher standard of knowledge of the law, how this could not have come to her attention. She was the Secretary of State. Of course, the Secretary of State is going to become possessed of classified materials. Of course she was an attorney. She practiced with a prominent Arkansas law firm, the Rose Law Firm. She knew from her White House days with her husband, the President, that classified materials can be very dangerous if they get into the wrong hands.

She had to have known about this statute because she had to have been briefed when she took over the job as the Secretary of State. So how, given that body of knowledge and experience, could this have happened in a way that could have potentially provided access by hackers to confidential information?

Mr. COMEY. No, it's a good question, a reasonable question. The protection we have as Americans is that the government in general, and in that statute in particular, has to prove before they can prosecute any of us, that we did this thing that's forbidden by the law, and that when we did it, we knew we were doing something that was unlawful. We don't have to know the code number, but that we knew we were doing something that was unlawful. That's the protection we have. And it's one I've worked for very hard. When I was in the private sector, I did a lot of work with the

Chamber of Commerce to stop the criminalization of negligence in the United States.

Mrs. LUMMIS. May I interrupt and suggest that this statute says "knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location." The intent here in the statute is to retain the documents at an unauthorized location. It's not intent to pass them on to a terrorist, or to someone out in Internetland. It's just the intent to retain the documents or materials at an unauthorized location.

Mr. COMEY. It's more than that, though. You'd have to show that and prove criminal intent, both by law, that's the way the judge would instruct a jury, and practice at the Department of Justice. They have reserved that statute, even though it's just a misdemeanor, for people who clearly knew they were breaking the law. And that's the challenge. So should have known, must have known, had to know, does not get you there. You must prove beyond a reasonable doubt that they knew they were engaged in something that was unlawful.

Mrs. LUMMIS. Okay. Then——

Mr. COMEY. That's the challenge.

Mrs. LUMMIS. Then may I turn to her attorneys. Did all of Secretary Clinton's attorneys have the requisite clearances at the time they received all of her emails, especially those that were classified at the time they were sent?

Mr. COMEY. No.

Mrs. LUMMIS. They destroyed, as has been noted, 30,000 emails of Secretary Clinton's. Do you have 100 percent confidence that none of the 30,000 emails destroyed by Secretary Clinton's attorneys was marked as classified?

Mr. COMEY. I don't have 100 percent confidence. I'm reasonably confident some of them were classified. There were only three in the entire batch we found that bore any markings that indicated they were classified. So that's less likely. But surely, it's a reasonable assumption that some of the ones they deleted contained classified information.

Mr. BLUM. Thank you, Director. Thank you, Mr. Chairman. I yield back.

Chairman CHAFFETZ. I now recognize the gentleman from Massachusetts, Mr. Lynch, for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. Thank you, Director Comey, for appearing here to help the committee with its work. Director Comey, Secretary Clinton's certainly not the only Secretary of State to use a personal email account with information later identified as being classified. I just want to show you. This is a book that was written by former Secretary of State Colin Powell. And in his book, he says, "To complement the official State Department computer in my office, I installed a laptop computer and on a private line. My personal email account on a laptop allowed me direct access to anyone online. So I started shooting emails to my principal assistants, to individual ambassadors, and increasingly, to my foreign minister colleagues who like me were trying to bring their ministries into the one 186,000 miles per second world." Were

you aware of this, that Secretary Colin Powell actually had a private server as well?

Mr. COMEY. Not a private server. I think he used a commercial email account for State Department business.

Mr. LYNCH. Private line, unprotected.

Mr. COMEY. Correct. Not a State Department email system.

Mr. LYNCH. Right. Right. He went rogue, so to speak. Right?

Mr. COMEY. I don't know whether I'd say that.

Mr. LYNCH. Yeah. All right. Okay. I'm not going to put words in your mouth. But do you think this was careless for him to do that, just to start—you know, get his own—he got his own system. He installed a laptop computer on a private line. "My personal email account was on a laptop and allowed me direct access to anyone, anyone online." That's his own statement. I'm just trying to compare Secretaries of State, because Secretary Powell's never been here. As a matter of fact, when we asked him for his emails, unlike the 55,000 that we received from Secretary Clinton, he said, "I don't have any to turn over." This is a quote. This was on ABC's This Week. He explained, "I don't have anything to turn over. I didn't keep a cache of them. I did not print them off. I do not have thousands of pages somewhere on my personal files." But he was Secretary of State, and he operated, you know, on a private system. Were you aware of that?

Mr. COMEY. Not at the time 15 years ago. But I am now.

Mr. LYNCH. Yeah. Okay. So recently—well, back in October 2015, the State Department sent Secretary Powell a letter requesting that he contact his email provider, AOL, to determine whether any of his emails are still on the unclassified systems. Are you aware of that ongoing investigation?

Mr. COMEY. I don't know of an investigation. I am——

Mr. LYNCH. Well, that request for information from former Secretary Powell.

Mr. COMEY. Yes, I am.

Mr. LYNCH. You're aware of that. Are you surprised that he has never responded?

Mr. COMEY. I don't know enough to comment. I don't know exactly what conversation he had with the State Department.

Mr. LYNCH. All right. I'm trying to look at the—you know, where we have a lot of comparisons in other cases. And there seems, like all the cases where prosecutions have gone forward, the subject of the investigation has demonstrated a clear intent to deliver classified information to a person or persons who were unauthorized to receive that. So if you look at the, you know, PFC Bradley Manning, now Chelsea Manning, that was a court martial. But he demonstrated a clear intent to publish that information, which was classified. Julian Assange, the WikiLeaks editor, I guess, and publisher.

Again, a wide and deliberate attempt to publish classified information. General Petraeus, which we talked about earlier today, shared information with his biographer. And Jeffrey Sterling sending stuff to The New York Times. Former CIA officer Kiriakou, who was interested in writing a book, so he hung on to his information. And even former Director of the CIA, John Deutch, who retained classified information on a couple of servers, one in Belmont, Mas-

sachusetts, and one in Bethesda, Maryland. And that was after he became a private citizen.

So in all those cases, there's a clear intent. As you said before, you look at what people did and what they were thinking when they did that. And I would just ask you: Is there a clear distinction between what those people did and what Secretary Clinton did in her case?

Mr. COMEY. In my view, yes. The Deutch case illustrates it perfectly. And he took huge amount of documents, almost all at the TS/SCI level, had them in hard copy at his house, had them on an unclassed system connected to the Internet, attempted to destroy some of them when he got caught. Admitted: I knew I wasn't supposed to be doing this. So you have clear intent, huge amounts of documents, obstruction of justice, those are the kinds of cases that get prosecuted. That's what I said when—I meant it when I said it. In my experience, which is three decades, no reasonable prosecutor would bring this case. I know that frustrates people. But that's the way the law is. And that's the way the practice is at the Department of Justice.

Mr. LYNCH. Thank you for your testimony and for your service. I yield back.

Chairman CHAFFETZ. Thank you gentleman.

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

Mr. MEADOWS. Thank you, Mr. Chairman. Director Comey, thank you. There has been much said today about criticizing you and your service. And I want to go on record that even though many of my constituents would love for me to criticize your service because of the conclusion you reached, never have I, nor will I, criticize your service. And we appreciate your service to this country and the integrity. So I'm going to focus on the things that you said, not the conclusion that you drew.

And Congressman Trey Gowdy and I talked a little bit about this, but on February 4, 2016, Secretary Clinton, during a presidential debate said, "I never sent or received any classified material. They are retroactively classifying it," closed quote. And so in your statement on July 5, you said that there were indeed 110 emails, 52 email chains, which there was classified information on it at the time it was sent or received. So those two statements, both of them cannot be true. Is that correct? Your statement and her statement?

Mr. COMEY. Yeah. It's not accurate to say that she did not send or receive——

Mr. MEADOWS. So she did not tell the truth during that presidential debate that she never sent or received classified information, and it was retroactively classified?

Mr. COMEY. Yeah. I don't think that's a question I should be answering what was in her head——

Mr. MEADOWS. Well, either your statement's not true or hers is not true. Both of them cannot be true. So is your statement true?

Mr. COMEY. That I can speak to. My——

Mr. MEADOWS. Okay. Your statement is true. So the American people will have to judge with her statement not being true. So let me go on to another one. On October 22 she said, "There was noth-

ing marked classified on emails either sent or received." And in your statement you said, "A very small number of emails contained classified information bore markings indicating the presence of classified information at the time." So she makes a statement that says there was no markings. You make a statement that there was. So her statement was not true.

Mr. COMEY. Well, that one actually I have a little bit of insight into her statement, because we asked her about that. There were three documents that bore portion markings where you're obligated, when something is classified, to put a marking on that paragraph.

Mr. MEADOWS. Right.

Mr. COMEY. And there were three that bore C in parens, which means that's confidential classified——

Mr. MEADOWS. So a reasonable person who has been a Senator, a Secretary of State, a First Lady, wouldn't a reasonable person know that that was a classified marking as a Secretary of State?

Mr. COMEY. Yeah.

Mr. MEADOWS. A reasonable person. That's all I'm asking.

Mr. COMEY. Yeah. Before this investigation I probably would have said yes. I'm not so sure. I don't find it incredible——

Mr. MEADOWS. Director Comey, come on. I mean, I've only been here a few years, and I understand the importance of those markings. So you're suggesting that a long length of time that she had no idea what a classified marking would be? That's your sworn testimony today?

Mr. COMEY. No, no, not that she would have no idea what a classified marking would be. But it's an interesting question as to whether she—this question about sophistication came up earlier. Whether she was actually sophisticated enough to understand what a C in parens mean.

Mr. MEADOWS. So you're saying this former Secretary of State is not sophisticated enough to understand a classified marking.

Mr. COMEY. No. That's not what I'm saying.

Mr. MEADOWS. That's a huge statement.

Mr. COMEY. That's not what I'm saying. You asked me did I assume that someone would know. Probably before this investigation, I would have. I'm not so sure of that answer any longer. I think it's possible, possible, that she didn't understand what a C meant when she saw it in the body of an email like that.

Mr. MEADOWS. After years in the Senate, and Secretary of State? I mean, that's hard for me and the American people to believe, Director Comey. And I'm not questioning your analysis of it, but wouldn't a reasonable person think that someone who has the highest job of handling classified information understand that?

Mr. COMEY. I think that's a conclusion a reasonable person would draw. It may not be accurate.

Mr. MEADOWS. So in that, let me go a little bit further. Because that last quote actually came on October 22, 2015, under sworn testimony before the Benghazi Committee. So if she gave sworn testimony that a reasonable person would suggest was not truthful, isn't it a logical assumption that she may have misled Congress, and we need to look at that further?

Mr. COMEY. Well, the reasonable person test is not what you look at for perjury or false statements. But like I said, I can understand why people would ask that question.

Mr. MEADOWS. All right. So let me, in the last little portion of this, in your 3–1/2 hour interview on Saturday, did she contradict some of these public statements in private? Because you said she didn't lie to the FBI. But it's apparent that she lied to the American people. So did she change her statements in that sworn testimony with you last Saturday?

Mr. COMEY. I haven't gone through that to parse that. I have——

Mr. MEADOWS. Can you do that and get back to this committee? Because it's important, I think, to the American people and to transparency.

Mr. COMEY. I'm sure. And as the chairman and I have talked about, I'm sure the committee's going to want to see documents in our investigation and whatnot, and we'll work to give you whatever we can possibly give you under our law. But I haven't done that analysis at this point.

Mr. MEADOWS. Will you, and get that back to us?

Chairman CHAFFETZ. The gentleman's time has expired. And we'll now recognize the gentleman from Tennessee, Mr. Cooper, for 5 minutes.

Mr. COOPER. Thank you, Mr. Chairman. And thank you, Director Comey. I hate to see one of America's most distinguished public servants pilloried before this committee. We're all highly partisan here. We're good back seat drivers. We're all today apparently armchair prosecutors. And you stated the truth when you said that you didn't know of anyone who would bring a case like this. And some of the prosecutors have had decades to do that. I hope that this committee's effort is not intended to intimidate you or the FBI or law enforcement in general, or government employees.

And I'm thankful at this moment that you have such a lifetime record of speaking truth to power. Because that's very important. It's also very important that apparently you're a lifelong Republican. You're just here to do your job, to state the facts. I think the key issue here is whether, in fact, there's a double standard, where some Americans are being treated differently than others. And I think I can rely on my Republican colleagues to make sure that Hillary Clinton's treated no better than anybody else. There should be some attention given to make sure that she's not treated any worse than anybody else.

I think we all know that we wouldn't be having this hearing, especially on an emergency basis, unless she were running for President. My colleague from Massachusetts has just pointed out that previous Secretaries of State are not being called on the carpet, whether that be Condoleezza Rice or Colin Powell or others.

But I think the grossest double standard here today is the fact that all the members of this committee, every Member of Congress, is not subject to the same law that Secretary Clinton was subject to. And as lawmakers, that means that we have exempted ourselves from the standard of other Federal employees. My colleague from D.C., Ms. Norton, referred to this. Why did we exempt ourselves from the same rules? Apparently our chairman lists his pri-

vate email account on his business card. We all have access to classified information.

So I would like to challenge my Republican colleagues here today. Let's work together and introduce legislation to make the same laws apply to us as apply to the executive branch and to Secretary Clinton. I would be happy to join in such legislation to make sure that we're not being hypocritical on this panel, that we're holding ourselves to the same standards as Secretary Clinton, and not trying to accuse her of things that we may be guilty of ourselves.

I bet my colleagues would be the first to complain if, for example, emails were retroactively classified. That's a situation that most people in public service would object to pretty strongly. How did you know at the time if you had no idea? So I think it's very important if we want as Congress to have the trust of the American people to not be hypocritical, to uphold the same standards that we want to see upheld by others, and I'm just thankful at this moment in our history that we have someone like you who's in charge of the FBI. Because too many things are highly politicized. And the last thing we should do is criminalize our political system.

I didn't see any of my Republican colleagues complain when former Governor Bob McDonald was exonerated by an 8–0 vote at the Supreme Court for having done certain things that I think most Americans would find highly objectionable. But our court, on a bipartisan, unanimous basis, exonerated him just a week or two ago.

So I think this is a moment for committee members to reflect, to take a deep breath, to calm down and realize exactly what you said, that no reasonable prosecutor would have brought this case. And thank you for stating that so clearly and publicly. I yield back the balance of my time.

Mr. CUMMINGS. Will the gentleman yield?

Mr. COMEY. I yield to the ranking member.

Mr. CUMMINGS. Mr. Director, let me ask you this: First of all, I associate myself with everything the gentleman just said. You were talking about some markings a little bit earlier. Is that right? Can you describe what those markings are like? Markings on documents. I think you said there were three documents with certain markings on them——

Mr. COMEY. Yeah.

Mr. CUMMINGS. —that indicated classified. Go ahead.

Mr. COMEY. Yeah, there were three emails that down in the body of the email, in the three different emails, there were paragraphs that, at the beginning of the paragraph, had a parenthesis, a capital C, and then a parenthesis. And that is a portion marking to indicate that——

Mr. CUMMINGS. That paragraph.

Mr. COMEY. —that paragraph is classified at the confidential level, which is the lowest level of classification.

Mr. CUMMINGS. And so out of the 30,000 documents, you found these three markings? Is that what you're saying?

Mr. COMEY. Three emails for C markings down in the body. None of the emails had headers, which is at the top of a document that

says it's classified. Three had within the body the portion marking for C.

Mr. CUMMINGS. Thank you.

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

Mr. DUNCAN. Thank you, Mr. Chairman. Mr. Meadows mentioned one instance in which Secretary Clinton said that she did not mail any classified material to anyone. Actually, she said that several other times. But it is accurate, Director Comey, that you found at least 110 instances of when she had emailed classified material?

Mr. COMEY. 110 that she either received or sent.

Mr. DUNCAN. Right. And it also is accurate that, quote, "Clinton's lawyers cleaned their devices in such a way as to preclude complete forensic recovery"?

Mr. COMEY. Correct.

Mr. DUNCAN. And also when she said—when Secretary Clinton said that nothing she sent was marked classified, and you said, in your press conference, "but even if information is not marked classified in an email, particularly are participants who know or should know that the subject matter's classified are still obligated to protect it." Do you feel that Secretary Clinton knew, or should have known, that she was obligated to protect classified information?

Mr. COMEY. Yes.

Mr. DUNCAN. With her legal background and her long experience in government. Also, she said at one point that she has directed all emails, work-related emails, to be forwarded to the State Department. Is it also accurate that you discovered thousands of other emails that were work-related other than the 30,000 that she submitted?

Mr. COMEY. Correct.

Mr. DUNCAN. Before I came to Congress, I spent several years as a criminal court judge. I presided over several hundred felony criminal cases. And I can assure you that I saw many cases where the evidence of criminal intent was flimsier than the evidence in this case. But do you realize that great numbers of people across this country felt that you presented such an incriminating case against Secretary Clinton in your press conference that they were very surprised or even shocked when you reached the conclusion to let her off? You doubt that great numbers feel that way?

Mr. COMEY. No. I think so. And I understand the question. And I wanted to be as transparent as possible. We went at this very hard to see if we could make a case. And I wanted the American people to see what I honestly believed about the whole thing.

Mr. DUNCAN. Well, do you understand, as the chairman said earlier, that great numbers of people feel now that there's a one standard of justice for the Clintons and another for regular people?

Mr. COMEY. Yeah, I've heard that a lot. It's not true, but I've heard it a lot.

Mr. DUNCAN. Well, even the ranking member who was here, who, of course as we understand, had to defend Secretary Clinton as strongly as possible, he almost begged you to explain the gap between the incriminating case that you presented and the conclusion

that was reached. Did that surprise you that he felt so strongly that there was this big gap?

Mr. COMEY. No. Not at all. These—it's a complicated matter. It involves understanding how the Department of Justice works across decades, house prosecutorial discretion is exercised. I get that folks see disconnection, especially when they see a statute that says "gross negligence." Well, the Director just said she was extremely careless. So how is that not prosecutable? So it takes an understanding of what's one on over the last 99 years. What's the precedent? How do we treat these cases. I totally get people's questions. And I think they're in good faith.

Mr. DUNCAN. We talked about gross negligence here. And you said that Secretary Clinton was extremely careless with this classified material, and how dangerous it could be, how threatening, even to people's lives that it could be to disclose classified material. Do you agree that there is a very thin line between gross negligence and extreme carelessness? And would you explain to me what you consider to be that difference?

Mr. COMEY. Sure, Judge—Congressman. As a former judge, you know there isn't actually a great definition in the law of gross negligence. Some courts interpret it as close to willful, which means you know you're doing something wrong. Others drop it lower. My term extremely careless is—I'm trying to be kind of an ordinary person. That's a commonsense way of describing it sure looks real careless to me. The question of whether that amounts to gross negligence, frankly, is really not at the center of this, because when I look at the history of the prosecutions and see it's been one case brought on a gross negligence theory, I know from 30 years, there's no way anybody at the Department of Justice is bringing a case against John Doe or Hillary Clinton for the second time in 100 years based on those facts.

Mr. DUNCAN. You ended your statement to Congressman Cooper a while ago saying once again that no reasonable prosecutor could have brought this case. Yet you also mentioned earlier today that you'd seen several of your friends and other prosecutors who've said publicly, many across this country, that they would have been glad to prosecute this case.

Mr. COMEY. I smile because they're friends. And I haven't talked to them. And I want to say: Guys, so where were you over the last 40 years? Where were these cases? They just have not been brought. For reasons that I said earlier, it's a good thing that the Department of Justice worries about prosecuting people for being careless. I don't like it. As a citizen I want people to show they knew they were breaking the law, and then we'll put you in jail.

Mr. DUNCAN. Of course, you know many people have been prosecuted for gross negligence by the Federal Government, by the FBI.

Chairman CHAFFETZ. The gentleman's time has expired.

Mr. DUNCAN. Thank you.

Chairman CHAFFETZ. We'll now recognize the gentleman from Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. Thank you. And welcome, Director Comey. And although our politics are different, I gather you're a Republican. Is that correct?

Mr. COMEY. I have been a registered Republican for most of my adult life. I'm not registered any longer.

Mr. CONNOLLY. We don't register by party in Virginia. But many have suspected my politics as being Democratic. And I thank you for your integrity. As my colleague said, and I said in my opening statement, your career has been characterized as speaking truth to power. And you're doing it again today. Just to set the context, Director Comey, not that you're unaware of this.

Today's hearing is political theatre. There's not even the pretense of trying to get at the truth. This is a desperate attempt under an extraordinary set of circumstances, an emergency hearing. I don't know what the emergency is other than one side is about to nominate somebody who is a pathological narcissist who, you know, is talking about banning Muslims and Mexicans crossing the border who are all rapists and women who are pigs and terrified at the prospect of the consequences of that in the election. So let's grab onto whatever we can to discredit or try to discredit the other nominee, punitive nominee. And you took away their only hope.

And so the theater today is actually trying to discredit you. Subtlety in some cases. My friend from South Carolina uses big words like "exculpatory." And kind of goes through what a prosecutor would do. The insinuation being you didn't do your job. My friend from Wyoming is apparently flooded with citizens in her home State who are reading the statute that governs classification. Lot of time on their hands back there, I guess. But, yeah, this is all designed to discredit your finding. Now, the FBI interviewed Secretary Clinton. Is that correct?

Mr. COMEY. Yes.

Mr. CONNOLLY. Did she lie to the FBI in that interview?

Mr. COMEY. I have no basis for concluding that she was untruthful with us.

Mr. CONNOLLY. And is it a crime to lie to the FBI?

Mr. COMEY. Yes, it is.

Mr. CONNOLLY. David Petraeus did lie to the FBI.

Mr. COMEY. Yes.

Mr. CONNOLLY. And he prosecuted for that—well, could have been.

Mr. COMEY. Could have been, was not for that——

Mr. CONNOLLY. Right. That's always a judgment call.

Mr. COMEY. Correct.

Mr. CONNOLLY. Was she evasive?

Mr. COMEY. I don't think the agents assessed she was evasive.

Mr. CONNOLLY. How many emails are we talking about, total universe, that were examined by your team?

Mr. COMEY. Tens of thousands.

Mr. CONNOLLY. Tens of thousands. And how many are in a questionable category that maybe could have, should have been looked at more carefully because there could be some element of classification? Apparently, my friend from North Carolina assumes we're all intimately familiar with the fact that if a C appears, it means a classification, though there seems to be some dispute about that because the State Department, as I understand it, has actually said some of those were improperly marked and shouldn't have had the C. Are you aware of that?

Mr. COMEY. Yes.

Mr. CONNOLLY. Yes. So could it be that in her 100-trip, 4 years—100 overseas trips to 100 countries as Secretary of State trying to restore U.S. credibility that had been destroyed in the previous 8 years overseas, and tens of thousands of email communications, not including phone calls and classified conversations in SCIFs and the like, that maybe the small percentage of emails, she didn't pay as much attention to them as maybe in retrospect one would hope she would have. Is that a fair conclusion? Could that be a fair conclusion?

Mr. COMEY. I don't usually deal in maybes. It's possible.

Mr. CONNOLLY. Well, you do deal in distinguishing between willful and inadvertent.

Mr. COMEY. Sure.

Mr. CONNOLLY. And in this case, you concluded it has to be in the latter category. It wasn't willful.

Mr. COMEY. We concluded there was not adequate evidence of willful conduct.

Mr. CONNOLLY. Right. So there's no obfuscation here, unlike the Petraeus case. And there's no evasion. There's no lying. There's no willful intent to compromise classified material, despite the insinuations of my friends on the other side of the aisle. And the only hope left in this political theatre is to discredit you and your team in the hopes that, therefore, you won't have credibility and we can revisit this monstrous crime of using a private server, that server being the server of the former President of the United States that maybe Mrs. Clinton thought would be more secure than the leaky system at the State Department. I yield back.

Chairman CHAFFETZ. We now recognize the gentleman from Texas, Mr. Hurd, for 5 minutes.

Mr. HURD. Thank you, Mr. Chairman. Mr. Chairman, I'm offended. I'm offended by my friends on the other side of the political aisle saying this is political theatre. This is not political theatre. For me, this is serious. I spent 9–1/2 years as an undercover officer in the CIA. I was the guy in the back alleys collecting intelligence, passing it to lawmakers. I've seen my friends killed. I've seen assets put themselves in harm's way. And this is about protecting information, the most sensitive information the American government has. And I wish my colleagues would take this a little bit more seriously.

Mr. Comey, Director Comey, excuse me, SAP, Special Access Program. You alluded to earlier that includes SCI information. Does SCI information include HUMINT and SIGINT?

Mr. COMEY. Yes.

Mr. HURD. HUMINT and SIGINT. Human intelligence information collected from people that are putting themselves in harm's way to give us information to drive foreign policy. Signals intelligence. Some of the most sensitive things to understand; what Al Qaeda is doing; what ISIS is doing. So the former Secretary of State had an unauthorized server, those are your words, in her basement, correct?

Mr. COMEY. Correct.

Mr. HURD. Who was protecting that information? Who was protecting that server?

Mr. COMEY. Well, not much. There was a number of different people who were assigned as administrators of the server.

Mr. HURD. And at least seven email chains, or eight that was classified as TS/SCI.

Mr. COMEY. Correct.

Mr. HURD. So the former Secretary of State, one of the President's most important advisors on foreign policy and national security, had a server in her basement that had information that was collected from our most sensitive assets, and it was not protected by anyone? And that's not a crime? That's outrageous. People are concerned. What does it take for someone to misuse classified information and get in trouble for it?

Mr. COMEY. Well, it takes mishandling it and criminal intent.

Mr. HURD. And so an unauthorized server in the basement is not mishandling?

Mr. COMEY. Well, no, there is evidence of mishandling here. This whole investigation at the end focused on is there sufficient evidence of intent.

Mr. HURD. Was this unanimous opinion within the FBI on your decision?

Mr. COMEY. Well, the whole FBI wasn't involved, but the team of agents, investigators, analysts, technologists, yes.

Mr. HURD. Did you take into any consideration the impact that this precedence can set on our ability to collect intelligence overseas?

Mr. COMEY. Yes. My primary concern is the impact on what other employees might think in the Federal Government.

Mr. HURD. And you don't think this sends a message to other employees that if a former Secretary of State can have an unauthorized server in their basement that transmits top secret information, that that's not a problem?

Mr. COMEY. Oh, I worry very much about that. That's why I talked about that in my statement, because an FBI employee might face severe discipline. And I want them to understand that those consequences are still going to be there.

Mr. HURD. Director Comey, do you have a server in your basement?

Mr. COMEY. I do not.

Mr. HURD. Does anybody in the FBI have a server in their basement or in their house?

Mr. COMEY. I don't know.

Mr. HURD. Do you think it's likely?

Mr. COMEY. I think it's unlikely.

Mr. HURD. I would think so, too. I would think so, too. Because I've always been proud to serve alongside the men and women that you represent. So there was no dissenting opinion when you made this decision. It's your job to be involved in counterintelligence as well?

Mr. COMEY. Yes.

Mr. HURD. So that means protecting our secrets from foreign adversaries collecting them. Is that correct?

Mr. COMEY. Correct.

Mr. HURD. Did this activity you investigated make America's secrets vulnerable to hostile elements?

Mr. COMEY. Yes.

Mr. HURD. Do you think that pattern of behavior would continue?

Mr. COMEY. I'm sorry?

Mr. HURD. Do you think that pattern of behavior would continue?

Mr. COMEY. Would continue?

Mr. HURD. By our former Secretary of State.

Mr. COMEY. I'm not following you. You mean if we hadn't—if this had not come to light, you mean?

Mr. HURD. Right now, based on what we see, do you think there's going to be other elements within the Federal Government that think it's okay to have an unauthorized server in their basement?

Mr. COMEY. Well, they better not. That's one of the reasons I'm talking about——

Mr. HURD. So, but what is the ramifications of them doing that? You know, how is there going to be any consequences levered if it's not being levered here? Because, indeed, you're setting a precedent.

Mr. COMEY. Yeah. The precedent—I want people to understand, again, I only am responsible for the FBI, that there will be discipline from termination to reprimand and everything in between for people who mishandle classified information.

Mr. HURD. Director Comey, I'm not a lawyer, and so I may misstate this. Is there such a thing as the case of first impression? And why was this not possibly one of those?

Mr. COMEY. There is such a thing, which just means the first time you do something. The reason this isn't one of those is that's just not fair. That would be treating somebody differently because of their celebrity status, or because of some other factor doesn't matter. We have to treat people—the bedrock of our system of justice, we treat people fairly. We treat them the same based on their——

Mr. HURD. And that person mishandling the most sensitive information that this government can collect is not fair—it's not fair to punish someone who did that?

Mr. COMEY. Not on these facts. It would be fair—if that person worked for me, it would be fair to have a robust disciplinary proceeding. It's not fair to prosecute that person on these facts.

Mr. HURD. Mr. Chairman, I yield back the time I do not have.

Chairman CHAFFETZ. Thank the gentleman. We'll now recognize the gentleman from Pennsylvania, Mr. Cartwright, for 5 minutes.

Mr. CARTWRIGHT. Thank you, Mr. Chairman. And I'd like to open by acknowledging my colleague from North Carolina, Mr. Meadows, here he comes back in the room, for acknowledging your integrity, Director Comey. I think bipartisan sentiments like that are few and far between around here. And I appreciate Congressman Meadows' remark. You are a man of integrity, Director Comey. It's troubling to me that that remark from Congressman Meadows is not unanimous at this point. It used to be. Just weeks ago, our chairman, Representative Chaffetz, stated on national TV that Republicans, quote, "Believe in James Comey," unquote. He said this, and I quote, "I do think that in all of the government, he is a man of integrity and honesty. His finger's on the pulse of this. Nothing

happens without him. And I think he is going to be the definitive person to make a determination or a recommendation."

But just hours after your actual recommendation came out, Chairman Chaffetz went on TV and accused you of making a, quote, "political calculation." And then our Speaker of the House, weeks ago, referring to you, Director Comey, said, "I do believe that his integrity is unequalled. So you're integrity—it was unanimous about your integrity before you came to your conclusion. But after, not so much. That's troubling. And I want to give you a chance, Director Comey, how do you respond to that? How important to you is maintaining your integrity before the Nation?

Mr. COMEY. I think the only two things I have in life that matter are the love of my family and friends and my integrity. So I care deeply about both.

Mr. CARTWRIGHT. All right. Now, Director Comey, you discussed your team a little bit. And they deserve a lot of credit for all of the hard work and effort that went into this investigation. And I think you just said that they were unanimous. That everyone who looked at this agreed that no reasonable prosecutor would bring a case. Am I correct in that?

Mr. COMEY. Yes.

Mr. CARTWRIGHT. How many people were on this team?

Mr. COMEY. It changed at various times, but somewhere between 15 and 20, and then we used a lot of other FBI folks to help from time to time.

Mr. CARTWRIGHT. And how many hours were spent on this investigation?

Mr. COMEY. We haven't counted yet. They—I said to them they moved—they put 3 years of work into 12 calendar months.

Mr. CARTWRIGHT. And how many pages of documents did the FBI review in this investigation?

Mr. COMEY. Thousands and thousands and thousands.

Mr. CARTWRIGHT. And the agents doing the document review, were they qualified or were they unqualified?

Mr. COMEY. They were an all-star team. They are a great group of folks.

Mr. CARTWRIGHT. How about Secretary Clinton? Did she agree to be interviewed?

Mr. COMEY. Yes.

Mr. CARTWRIGHT. Come in voluntarily without the need of a subpoena?

Mr. COMEY. Yes.

Mr. CARTWRIGHT. Was she interviewed?

Mr. COMEY. Yes.

Mr. CARTWRIGHT. Was she interviewed by experienced critical veteran agents and law enforcement officers, or by some kind of credulous gullible newbies doing their on-the-job training, Director?

Mr. COMEY. She was interviewed by the kind of folks the American people would want doing the interview. Real pros.

Mr. CARTWRIGHT. All right. You were asked about markings on a few documents. I have the manual here, Marking Classified National Security Information. And I don't think you were given a full chance to talk about those three documents with the little Cs on

them. Were they properly documented? Were they properly marked according to the manual?

Mr. COMEY. No.

Mr. CARTWRIGHT. According to the manual, and I ask unanimous consent to enter this into the record, Mr. Chairman.

Chairman CHAFFETZ. Without objection, so ordered.

Mr. CARTWRIGHT. According to the manual, if you're going to classify something, there has to be a header on the document, right?

Mr. COMEY. Correct.

Mr. CARTWRIGHT. Was there header on the three documents that we've discussed today that had the little C in the text someplace?

Mr. COMEY. No. They were three emails. The C was in the body, in the text. But there was no header on the email or in the text.

Mr. CARTWRIGHT. So if Secretary Clinton really were an expert at what's classified and what's not classified, and were following the manual, the absence of a header would tell her immediately that those three documents were not classified. Am I correct in that?

Mr. COMEY. That would be a reasonable inference.

Mr. CARTWRIGHT. All right. I thank you for your testimony, Director. I yield back.

Chairman CHAFFETZ. I thank the gentleman. We'll now recognize the gentleman from Colorado, Mr. Buck, for 5 minutes.

Mr. BUCK. Good morning, Director Comey.

Mr. COMEY. Good morning, sir.

Mr. BUCK. Thank you for being here. I also respect your commitment to law and justice and your career. And the first question I want to ask you is this hearing unfair? Has it been unfair to you?

Mr. COMEY. No.

Mr. BUCK. Thank you. One purpose of security procedures for classified information is to prevent hostile nations from obtaining classified information. Is that fair?

Mr. COMEY. Yes.

Mr. BUCK. And did hostile nations obtain classified information from Secretary Clinton's servers?

Mr. COMEY. I don't know. It's possible. But we don't have direct evidence of that. We couldn't find direct evidence.

Mr. BUCK. I want to, without making this a law school class, I want to try to get into intent. There are various levels of intent in the criminal law. Everything from knowingly and willfully doing something all the way down to strict liability. Would you agree with me on that?

Mr. COMEY. Yes.

Mr. BUCK. And in Title 18, most of the criminal laws in Title 18 have the words "knowingly" and "willfully" in them. And that is the standard typically that United States attorneys prosecute under.

Mr. COMEY. Most do. Unlawfully, knowingly, and willfully is our standard formulation for charging a case.

Mr. BUCK. And there are also a variety of others between the knowingly and willfully standard and the strict liability standard. And many, like environmental crimes, have a much lower standard

because of the toxic materials that are at risk of harming individuals. Is that fair?

Mr. COMEY. That's correct.

Mr. BUCK. Okay. Let's talk about this particular statute, 18 U.S.C. 1924. I take it we could all agree—or you and I can agree on a couple of the elements. She, Secretary Clinton, was an employee of the United States.

Mr. COMEY. Correct.

Mr. BUCK. And as the result of that employment, she received classified information.

Mr. COMEY. Correct.

Mr. BUCK. And there's no doubt about those two elements. Now, I don't know whether the next element is one element or two, but it talks about knowingly removes such materials without authority, and with the intent to retain such material at an unauthorized location. So I'm going to treat those as two separate parts of the intent element.

First of all, do you see the word "willfully" anywhere in the statute?

Mr. COMEY. I don't.

Mr. BUCK. Okay. And that would indicate to you that there is a lower threshold for intent?

Mr. COMEY. No, it wouldn't.

Mr. BUCK. Why?

Mr. COMEY. Because we often, as I understand the Justice Department's practice and judicial practice, will impute to any criminal statute at that level with a knowingly also requirement that you know that you're involved in criminal activity of some sort. A general mens rea requirement.

Mr. BUCK. And you would apply that same standard to environmental crimes?

Mr. COMEY. No. If it specifically says it's a negligence-based crime, I don't think a judge would impute that.

Mr. BUCK. But Congress specifically omitted the word "willfully" from this statute. And yet you are implying the world "willfully" in the statue. Is that fair?

Mr. COMEY. That's fair.

Mr. BUCK. Okay. So what the statute does say is knowingly removes such materials without authority. Is it fair that she knew that she didn't have authority to have this server in her basement?

Mr. COMEY. Yes. That's true.

Mr. BUCK. And she knew that she was receiving materials, classified information, in the emails that she received on her BlackBerry and other devices?

Mr. COMEY. I can't answer—I'm hesitating as a prosecutor because it's always—to what level of proof? I do not believe there's evidence beyond a reasonable doubt that she knew she was receiving classified information in violation of the requirements.

Mr. BUCK. But that's not my question. My question, in fairness, is did she know that she was receiving information on the servers at her location?

Mr. COMEY. Oh, I'm sorry. Of course. Yes. She knew she was using her email system.

Mr. BUCK. And as Secretary of State, she also knew that she would be receiving classified information.

Mr. COMEY. Yes. In general.

Mr. BUCK. Okay. And did she then have the intent to retain such material at an unauthorized location? She retained the material that she received as Secretary of State at her server in her basement and that was unauthorized?

Mr. COMEY. You're asking me did she have the—and I'm going to ask you the burden of proof question in a second. But did she have the intent to retain classified information on the server, or just to retain any information on the server?

Mr. BUCK. Well, we've already established that she knew, as Secretary of State, that she was going to receive classified information in her emails. And so did she retain such information that she received as Secretary of State on her servers in her basement?

Mr. COMEY. She did, in fact. There is, in my view, not evidence beyond certainly probable cause. There's not evidence beyond a reasonable doubt that she knew she was receiving classified information, or that she intended to retain it on her server. There's evidence of that. But when I said there's not clear evidence of intent, that's what I meant. I could not, even if the Department of Justice would bring that case, I could not prove beyond a reasonable doubt those two elements.

Mr. BUCK. Thank you very much.

Chairman CHAFFETZ. Thank the gentleman. We'll now go to the gentlewoman from Illinois, Ms. Duckworth, for 5 minutes.

Ms. DUCKWORTH. Thank you, Mr. Chairman. When I first entered Congress 3 years ago, like many freshman members, I, unlike many freshman members, I actually sought out this committee. I wanted to be on this committee because I wanted to tackle the challenges of good government, like working to eliminate improper payments or prevent wasteful programs, duplication. Before I joined Congress, I had the privilege of serving in the Army for 23 years. And I, you know, and as I tackled those challenges and in the challenges of helping reduce veterans' homelessness, I witnessed firsthand the real-world importance of improving and streamlining government operations. How even the best policies in the world will not work without proper implementation.

And so when it comes to implementing true and lasting reforms that will make sure the electronic records and other records and the history of our great Nation are preserved for future generations, I've done my best to approach this goal seriously. I'm focused on making sure that our Nation sustains a long-term commitment to modernizing our Federal records keeping system, from improving the laws governing what needs to be collected, to ensuring our civil servants across government have the necessary tools to achieve what should be nonpartisan and a shared goal.

With respect to examining the tough lessons learned from numerous recordkeeping incidents that our committee has dealt with, which transcend any one agency or any single administration, my mission is clear: Make sure that we here in Congress move beyond partisan politics and engage in the serious hard work of ensuring that the laws written in an era of pen and paper are overhauled to meet the digital challenges of the 21st century.

Director Comey, the Office of Management and Budget and the National Archives and Records Administration released a memorandum known as the Managing Government Records Directive in 2012. And this directive states, and I quote, "By December 31, 2016, Federal agencies will manage both permanent and temporary email records in an accessible electronic format. Federal agencies must manage all email records in an electronic format. Email records must be retained in an appropriate electronic system that supports records management and litigation requirements which may include preservation-in-place models, including the capability to identify, retrieve, and retain the records as long as they are needed."

As a Director of a Bureau who deals with sensitive information on a daily basis, do you believe that this directive is necessary and attainable for agencies across the board within that 4-year timeframe from August 2012 to December 2016.

Mr. COMEY. I don't know enough to say both. I can say it's certainly necessary. I don't know whether it's achievable.

Ms. DUCKWORTH. Okay. Are you familiar with the Capstone Approach? That's the Federal—it's approach that says that Federal agencies should save all emails for select senior level employees, and that the emails of other employees would be archived for a temporary period set by the agency so that senior employees' emails are kept forever and those by other lower level employees are actually archived for a short period, a shorter period.

Mr. COMEY. I'm aware generally. I know what applies to me and when I was Deputy Attorney General in the Bush Administration.

Ms. DUCKWORTH. Yes. In fact, I understand that the FBI is currently actively using this approach, according to the agency's senior agency official for records—Office for Records Management fiscal year 2015 annual report. My understanding is the Capstone Approach is aimed at streamlining the recordkeeping process for emails and reducing the volume of records that an agency has to maintain. Nearly all agencies will be required to comprehensively modernize their approach to managing Federal records in the near future. As the head of a component agency, Director Comey, within the Department of Justice, which appears to be a leader in adopting the innovative Capstone Approach across the agency, would you agree that with respect to instituting foundational reforms that will strengthen records preservation, the Capstone Approach used by DOJ should be accelerated and wrote out across the Federal Government?

Mr. COMEY. I think we're doing it in a pretty good way. I don't know—I'm not an expert enough to say whether everybody should do it the way we do it, honestly.

Ms. DUCKWORTH. Are you satisfied with the way that you're doing it?

Mr. COMEY. I am, but I don't want to sound overconfident, because I'm sure there's a way we can do it better. But I think we're doing it in a pretty good way.

Ms. DUCKWORTH. Do you have any one person within the FBI that continually reviews the—your records keeping? And also do they report directly to you? As well as is there periodic review of how you're implementing this process?

Mr. COMEY. Yes. We have an entire division devoted to records management. That assistant director reports up to the deputy director, who reports to me. We have—it's an enormous operation, as you might imagine, requiring constant training. And so that's what I mean when I say I think we're doing it in a pretty good way. And we have record-marking tools, we prompt with dialogue boxes requiring employees to make a decision what's the nature of this record you're creating now and where should it be stored. So I think we're doing it in a pretty good way. That's why I say that.

Ms. DUCKWORTH. Have you seen that in any of the other agencies that you have interacted with, or have you had a chance, an occasion to look at what some of the other agencies are doing with their sensitive and classified information? Are they following the same technique as you're doing in the FBI?

Mr. COMEY. I don't know enough to say, I personally.

Ms. DUCKWORTH. Okay.

I am out of time, but thank you.

Mr. COMEY. Okay

Chairman CHAFFETZ. I thank the gentlewoman.

We'll now recognize the gentleman from Michigan, Mr. Walberg, for 5 minutes.

Mr. WALBERG. I thank the chairman.

And thank you, Director Comey, for being here.

Mr. Chairman, thank you for holding this hearing.

And, Director Comey, for making it very clear that you believe we've done this respectfully, with good intention. And I wish some of my colleagues that had instructed us on our intent were here. They have a great ability to understand intent better than, I guess, the Director of the FBI.

But it is an intent that's important here, that we understand we are Oversight and Government Reform Committee. And if indeed the tools aren't there to make sure that our country is secure and that officials at the highest levels in our land don't have the understanding on what it takes to keep our country secure, that we do the necessary government reform to put laws in place that will be effective and will meet the needs of distinguished agencies and important agencies like the FBI.

So thank you, Mr. Chairman, for doing this hearing. It's our responsibility to do oversight and reform as necessary.

Going back, Director Comey, to paraphrase the Espionage Act, people in the Seventh District of Michigan understand it from this perspective and common sense, what it says, that whoever being entrusted with information related to national defense, through gross negligence permits the information to be removed from its proper place in violation of their trust, shall be fined or imprisoned under the statute.

There doesn't seem to be a double standard there. It doesn't express intent. You've explained your understanding of why intent is needed, and we may agree or disagree on that, but the general public looking at that statute says it's pretty clear.

The question I would ask, Director Comey, what's your definition of extremely careless, if you could go through that?

Mr. COMEY. I intended it as a commonsense term. It's kind of one those kind of you know it when you see it sort of things. Somebody

who is—should know better, someone who is demonstrating a lack of care that strikes me as—there's ordinary accidents and then there's just real sloppiness. So I think of that as kind of real sloppiness.

Mr. WALBERG. So you stated that you had found 110 emails on Secretary Clinton's server that were classified at the time they were sent or received, yet Secretary Clinton has insisted for over a year publicly that she never sent or received any classified emails.

The question I have from that, would it be difficult for any Cabinet-level official, and specifically any Cabinet official, let alone one who is a former White House resident or U.S. senator, to determine if information is classified?

Mr. COMEY. Would it be difficult for them to——

Mr. WALBERG. Would it be difficult?

Mr. COMEY. That's hard to answer in the abstract. We're trying to find the context in which they're hearing it or seeing it. Obviously, if it's marked, which is why we require markings, it's easy. It's just too hard to answer, because there are so many other situations you might encounter it.

Mr. WALBERG. But with the training that we receive and certainly a Secretary of State would receive or someone who lives in the White House, that goes a little above and beyond just the commonsense individual out there trying to determine. Knowing that classified information will be brought and to remove to an unauthorized site ought to cause a bit of pause there, shouldn't it?

Mr. COMEY. Yeah. And if you're a government official, you should be attentive to it——

Mr. WALBERG. Absolutely.

Mr. COMEY. —because you know that the matters you deal with could involve sensitive information. So sure.

Mr. WALBERG. So Secretary Clinton's revised statement that she never knowingly sent or received any classified information is probably also untrue?

Mr. COMEY. Yeah. I don't want to comment on people's public statements. We did not find evidence sufficient to establish that she knew she was sending classified information beyond a reasonable doubt to meet that—the intent standard. But like I said, I understand why people are confused by the whole discussion, I get that. But you know what would be a double standard? If she were prosecuted for gross negligence.

Mr. WALBERG. But your statement on Tuesday said there is evidence to support a conclusion that any reasonable person in Secretary Clinton's position should have known that an unclassified system was no place for that conversation.

Mr. COMEY. I stand by that.

Mr. WALBERG. And that's very clear.

Mr. COMEY. That's the definition of carelessness, of negligence.

Mr. WALBERG. Which happened——

Mr. COMEY. Oh, yeah.

Mr. WALBERG. —as a result of our Secretary of State's—former Secretary of State's decisions.

Mr. COMEY. Yes.

Mr. WALBERG. Is it your statement, then, before this committee that Secretary Clinton should have known not to send classified material, and yet she did?

Mr. COMEY. Well, certainly she should have known not to send classified information. As I said, that's the definition of negligent. I think she was extremely careless, I think she was negligent. That, I could establish. What we can't establish is that she acted with the necessary criminal intent.

Mr. WALBERG. Do you believe that since the Department of Justice hasn't used the statute Congress passed, it's invalid?

Mr. COMEY. No, I think they're worried that it's invalid, that it will be challenged on constitutional grounds, which is why they've used it extraordinarily sparingly in the decades.

Mr. WALBERG. Thank you. I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We'll now go to—we'll now recognize Mr. Lieu of California for 5 minutes.

Mr. LIEU. Thank you, Mr. Chair.

As I read some of my Republican colleagues' press statements, and as I sit here today, I am reminded of that quote from "Macbeth": "full of sound and fury, signifying nothing."

I've heard some sound and fury today from members of the committee, and the reason they largely signify nothing is because of two fundamental truths that are self-evident. The first of which, none of the members of this committee can be objective on this issue. I can't be objective. I've endorsed Hillary Clinton for President, as have the Democratic members of this committee. My Republican colleagues can't be objective. They oppose Hillary Clinton for President.

Which is why we have you. You are a nonpartisan, career public servant that has served our Nation with distinction and honor. And not only can you be objective, it is your job to be objective, to apply the law fairly and equally regardless of politics.

I think it would be important for the American people to get a fuller appreciation of your public service. So let me ask you, before you were FBI Director, how many years did you serve as a Federal prosecutor?

Mr. COMEY. I think 15.

Mr. LIEU. For a period of time, you were at Columbia Law School as a scholar and you specialized in national security law. Is that correct?

Mr. COMEY. Sometimes I fantasize I still am.

Mr. LIEU. All right. Thank you.

When you served in the Republican administration of President George W. Bush, you were then the second-highest ranking member of the Department of Justice. Is that right?

Mr. COMEY. Yes. President Bush appointed me to be U.S. Attorney in Manhattan and then the number two in the Department of Justice.

Mr. LIEU. When you were confirmed for the FBI Director position, the vote was 93–1. Is that correct?

Mr. COMEY. That's correct.

Mr. LIEU. With that strong bipartisan support, it's not surprising that Senator Grassley, a Republican, said during your confirma-

tion, and I quote: "Director Comey has a reputation for applying the law fairly and equally regardless of politics."

In this case, did you apply the law fairly and equally regardless of politics?

Mr. COMEY. Yes.

Mr. LIEU. Did you get any political interfere reasons from the White House?

Mr. COMEY. None.

Mr. LIEU. Did you get any political interference from the Hillary Clinton campaign?

Mr. COMEY. None.

Mr. LIEU. One of the reasons you're appointed to a fixed term of 10 years, a very long term, is to help insulate you from politics. Isn't that right?

Mr. COMEY. That's correct.

Mr. LIEU. The second fundamental truth today about this hearing is that none of the members of this committee have any idea what we're talking about, because we have not reviewed the evidence personally in this case.

When I served on Active Duty in the U.S. Air Force in the 1990s, one of my duties was a prosecutor. One of the first things I learned as a prosecutor is it is unprofessional and wrong to make allegations based on evidence that one has not reviewed.

So let me ask you, has any member of this committee, to the best of your knowledge, reviewed the 30,000 emails at issue in this case?

Mr. COMEY. I don't know. Not to my knowledge.

Mr. LIEU. Has any member of this committee sat through the multiple witness interviews that the FBI conducted in this case?

Mr. COMEY. No. That I know. No.

Mr. LIEU. Has any member of this committee received any special information about the files that you kept or other FBI agents kept on this case?

Mr. COMEY. Not to my knowledge.

Mr. LIEU. Now let's do a little bit of math here. One percent of 30,000 emails would be 300 emails. Is that right?

Mr. COMEY. I think that's right.

Mr. LIEU. Thirty emails would be one-tenth of 1 percent, and three emails would be 1 one hundredth of 1 percent of 30,000, right?

Mr. COMEY. I think that's right.

Mr. LIEU. Okay. So of those three emails, 1 one hundredth of 1 percent of 30,000, they bore these tiny little classified markings, which is, as you described, a C with parentheses, correct?

Mr. COMEY. Correct.

Mr. LIEU. It is certainly possible that a busy person who has sent and received over 30,000 emails just might miss this marking of a C with parentheses. It is possible, correct?

Mr. COMEY. Correct.

Mr. LIEU. Okay. So let me now just conclude by stating what some of my colleagues have, which is, there is just the strongest whiff of hypocrisy going on here. The American public might be interested in knowing that all Members of Congress receive security clearances just for being a Member of Congress. We get to have pri-

vate email servers, we get to have private email accounts, we can use multiple devices, we can take devices overseas.

And really at the end of the day, when the American people look at this hearing, they need to ask themselves this question: Do they trust the biased, partisan politicians on this committee who are making statements based on evidence we have not reviewed, or do they trust the distinguished FBI Director? I would trust the FBI Director.

I yield back.

Chairman CHAFFETZ. Thank you.

We'll now recognize the gentleman from Florida, Mr. Mica, for 5 minutes.

Mr. MICA. Thank you, Mr. Chairman.

Director, how long did you investigate this matter?

Mr. COMEY. Just about a year.

Mr. MICA. A year. And do you believe you conducted a legitimate investigation?

Mr. COMEY. Yes, sir.

Mr. MICA. And it was a legitimate subject that was something that you should look into, you had that responsibility. Is that correct?

Mr. COMEY. Yes.

Mr. MICA. We have a responsibility to hear from you on the action that you took. This weekend—well, tomorrow we'll go back to our districts, and we have to explain people, I'll be at a couple of cafes where I see folks, in meetings, and they're going to ask a lot of questions about what took place.

Have you seen the Broadway production "Hamilton"?

Mr. COMEY. Not yet. I'm hoping to.

Mr. MICA. I haven't either, but I understand it won the choreography Tony Award. I think you and others know that.

The problem I have in explaining to my constituents is what's come down, it almost looks like choreography. Let me just go over it real quickly with you.

Last Tuesday, not this week, 1 week ago, former President Clinton meets with the Attorney General in Phoenix. The next Friday, last Friday, Mrs. Lynch, the AG, says she is going to defer to the FBI on whatever you came up with. On Saturday morning, I saw the vans pull up, this is this past Saturday, and you questioned Secretary Clinton for 3 hours. Is that—I guess that's correct?

Mr. COMEY. Yeah. Three and a half.

Mr. MICA. Okay. And then on Tuesday morning, the morning after July Fourth, we watched in our office, I had my interns, I said, "Come in, we've got the FBI Director, let's hear what he has to say," we're all kind of startled, and you basically said you were going to recommend not to prosecute, correct?

Mr. COMEY. Uh-huh. Yes, sir.

Mr. MICA. And then Tuesday, well, we had President Obama and Secretary Clinton arrive in Charlotte at 2 o'clock, and shortly thereafter we had the Attorney General is closing the case.

This is rapid fire. I mean, now, my folks think that there's something fishy about this. I'm not a conspiracy theorist, but there are a lot of questions on how this came down. I have questions about how this came down.

Did you personally interview the Secretary on Saturday morning?

Mr. COMEY. I didn't personally, no.

Mr. MICA. And how many agents did?

Mr. COMEY. I think we had five or six in the room.

Mr. MICA. Did you talk to all of those agents after the interview?

Mr. COMEY. I did not speak to all of them, no.

Mr. MICA. Did she testify or talk to them under oath?

Mr. COMEY. No.

Mr. MICA. She did not. Well, that's a problem. But——

Mr. COMEY. It's still a crime to lie to us.

Mr. MICA. I know it is. Do you have a transcript of that—that——

Mr. COMEY. No. We don't record our——

Mr. MICA. Do you have a 302, I guess it's called, analysis?

Mr. COMEY. I do. I don't have it with me, but I do.

Mr. MICA. Did you read it?

Mr. COMEY. Yes.

Mr. MICA. You did. Can we get a copy of it since the case is closed?

Mr. COMEY. I don't know the answer to that.

Mr. MICA. I would like a copy of it provided to the committee.

I would like also for the last 30 days, any communications between you or any agent or any person in the FBI with the Attorney General or those in authority in the Department of Justice on this matter. Could you provide us with that?

Mr. COMEY. We'll provide you with whatever we can under the law and under our policy. It would actually be easy in my case.

Mr. MICA. You see, the problem that I have, though, is I have to go back and report to people what took place.

Mr. COMEY. Sure.

Mr. MICA. Now, did you write the statement that you gave on Tuesday?

Mr. COMEY. Yes.

Mr. MICA. You did. And did you write—and you said you didn't talk to all of the agents. But all of the agents, did they meet with you? And then is that the group that said that we all vote to not recommend prosecution?

Mr. COMEY. Well, yeah, I did not meet with all of the agents. I've met with—I guess I've met—I've with all of them at various times.

Mr. MICA. But we're getting the word that it was, like, unanimous out of every—out of FBI that we don't prosecute.

Mr. COMEY. What's your question, Congressman?

Mr. MICA. Well, again, I want to know who counseled you. You read their summary, okay. She was not under oath. And it appears—I mean, members have cited here where she lied or misled to Congress, which will lead now to the next step of our possibly giving you a referral on this matter. You're aware of that?

Mr. COMEY. Yes. Someone mentioned that earlier.

Mr. MICA. And that probably will happen.

Thank you for shedding some light on what took place.

Mr. COMEY. Can I, Mr. Chairman——

Chairman CHAFFETZ. Sure. Go ahead.

Mr. COMEY. —can I respond just very briefly?

I hope what you'll tell the folks in the cafe is: Look me in the eye and listen to what I'm about to say. I did not coordinate that with anyone. The White House, the Department of Justice, nobody outside the FBI family had any idea what I was about to say. I say that under oath. I stand by that. There was no coordination. There was an insinuation in what you were saying that I don't mean to get strong in responding, but I want to make sure I was definitive about that.

Thank you, sir.

Chairman CHAFFETZ. Thank you.

We'll now recognize the gentlewoman from the Virgin Islands, Ms. Plaskett, for 5 minutes.

Ms. PLASKETT. Thank you, Mr. Chairman.

And thank you all for being here.

Director Comey, I would rather be here talking with you about the FBI's investigations and their resources to those individuals who are acting under color of law who have apparently committed egregious violations in the killings that we've seen in the recent days.

But instead, Mr. Chairman, I'm sitting here and I've listened patiently as a number of individuals have gone on national TV and made accusations against Director Comey, both directly and indirectly, because he recommended against prosecution based upon facts.

I've listened just very recently here in this hearing as my esteemed colleague from Florida tries to insinuate the condensation of an investigation into 1 week that actually occurred over a much, much longer period of time, and using that condensation and conspiracy theory to say that there's some orchestration. And that they have accused Mr. Director Comey of basing his decision on political considerations rather than facts. I've heard chuckles and laughter here in this hearing, and I don't think there's anything to be smiling or laughing about.

Because I want to say something to those individuals who are chuckling and laughing and making attacks on Director Comey for doing his job: You have no idea who you're talking about. Your accusations are completely off base, utterly offensive to us as American people.

I know this because I've had the honor of working for Director Comey during my own service at the Department of Justice. From 2002 to 2004, I served as senior counsel to the deputy attorney general. I worked with both the deputy attorney general, Larry Thompson, and Deputy Attorney General Jim Comey when he became deputy as a staff attorney. And I know from my own experiences that Director Comey is a man of impeccable integrity.

There are very few times when you as an attorney or as an individual can work with individuals or a gentleman who is completely that, someone who is above the fray. Anyone who suggests or implies that he made his recommendations on anything but the facts simply does not know James Comey.

We've used the term "no reasonable prosecutor." Well, I know that James Comey doesn't act as what a reasonable prosecutor would do, because he is the unyielding prosecutor, he is the pros-

ecutor who does what is politically not expedient for himself, his staff, but for the law.

And I'm not the only person in this hearing, in this committee, who has worked with Director Comey or for him. Representative Gowdy himself also commended Director Comey, and he said this, and I quote: "I used to work with him. I think Comey is doing exactly what you want. He's doing a serious investigation behind closed doors, away from the media's attention, and I'm going to trust him until I see a reason not to."

Representative Gowdy referred to Director Comey as honorable and apolitical. He said this is exactly what you want in law enforcement. Well, it's exactly what you want in law enforcement until the decision is not the decision that you want.

Director Comey, Chairman Chaffetz, as it was said by one of my colleagues, went on television and accused you of making, quote, "a political calculation." He said that your recommendation was nothing more than, quote, "a political determination in the end."

I'm going to ask you, how do you respond to that? Were your actions in any way, shape, or form governed by political consideration?

Mr. COMEY. No, not in any way.

Ms. PLASKETT. And did anyone with Secretary Clinton's campaign or the administration influence your recommendation for political reasons?

Mr. COMEY. No. They didn't influence it in any way.

Ms. PLASKETT. I'm going to take you at your word, because I know, and those who will go through the record of your long tenure as a career prosecutor and they'll look at examples, will see that you have taken decisions that have not been that which your supervisors, which the President, which others have wanted you to take.

As a Federal prosecutor who believed that the facts must come above politics, I'm thankful that we have you. And, Director Comey, I want to thank you for your service to our country, and you have our support.

We would like to see as much documents. And I'm grateful that you want to keep the transparency so that the American public can understand the difference between what they hear in the media and the elements of a crime necessary for criminal prosecution.

Thank you.

Chairman CHAFFETZ. I thank the gentlewoman.

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

Mr. FARENTHOLD. Thank you very much, Director Comey.

I want to talk a little bit about cybersecurity. The State Department's inspector general report detailed instances of multiple attacks on Secretary Clinton's computer as well as her replying to suspicious email from the personal account of the Undersecretary of State.

Director, you said that hostile actors successfully gained access to the commercial email accounts of people Secretary Clinton regularly communicated with. In the case of the Romanian hacker, Guccifer, accessing Sidney Blumenthal's account. And, you know, that's been public for some time.

During your investigation, were there other people in the State Department or that regularly communicated with Secretary Clinton that you can confirm were successfully hacked?

Mr. COMEY. Yes.

Mr. FARENTHOLD. And were these folks that regularly communicated with the Secretary?

Mr. COMEY. Yes.

Mr. FARENTHOLD. And were you able to conclude definitively that the attempted hacks referenced in the IG report were not successful?

Mr. COMEY. We were not able to conclude that they were successful. I think that's the best way to say it.

Mr. FARENTHOLD. All right. So while you said that given the nature of Clinton's server, you would be unlikely to see evidence one way or the other of whether or not it had been successfully hacked, how many unsuccessful attempts did you uncover? Did you find any there?

Mr. COMEY. There were unsuccessful attempts. I don't know the number off the top of my head.

Mr. FARENTHOLD. Do you have an idea, were they from foreign governments? Where did they come from?

Mr. COMEY. I want to be careful what I say in an open setting, and so I—we can give you that information, but I don't want to give any foreign governments knowledge of what I know. So there——

Mr. FARENTHOLD. All right. But would you be so far as to say they probably weren't American high school students fooling around?

Mr. COMEY. Correct. It was not limited to——

Mr. FARENTHOLD. All right.

Mr. COMEY. —criminal activity.

Mr. FARENTHOLD. During your investigation, did you or anyone in the FBI interview the hacker Guccifer?

Mr. COMEY. Yes.

Mr. FARENTHOLD. And he claimed he gained access to Sid Blumenthal's email account and traced him back to Clinton's private server. Can you confirm that Guccifer never gained access to her server?

Mr. COMEY. Yeah, he did not. He admitted that was a lie.

Mr. FARENTHOLD. All right. Well, at least that's good to hear.

All right. Section 793 of Title 18 of the United States Code makes it a crime to allow classified information to be stolen through gross negligence. Were you to discover that hostile actors had actually gotten into Secretary Clinton's email, would that have changed your recommendation with respect to prosecuting her?

Mr. COMEY. Unlikely, although we didn't consider that question, because we didn't have those facts.

Mr. FARENTHOLD. All right. I want to go back to the question of intent real quick for just a second. I'm a recovering attorney, it's been decades since I actually practiced law, but you kept referring to she had to know it was illegal to have the requisite criminal intent. I was always taught in law school, and I don't know where this changed, that ignorance of the law was no excuse. If I'm driving along at 45 miles an hour and didn't see the 35-mile-an-hour

speed limit, I was still intentionally speeding even though I didn't know it.

Now, I might not have had the requisite criminal intent if maybe my accelerator were jammed or something like that, but even though I didn't know the law was 35, I was driving 45, I'm going to get a ticket and I'm probably going to be prosecuted for that.

So how can you say ignorance of the law is an excuse in Mrs. Clinton's case?

Mr. COMEY. Well, the comparison to petty offenses, I don't think is useful. But the question of ignorance of the law is no excuse. But here's the distinction. You have to have general criminal intent. You don't need to know what particular statute you're violating, but you must be aware of the generally wrongful nature of your conduct. That's what——

Mr. FARENTHOLD. Now, so Congress, when they enacted that statute, said gross negligence.

Mr. COMEY. Yep.

Mr. FARENTHOLD. That doesn't say intent. So what are we going to have to enact to get you guys to prosecute something based on negligence or gross negligence? So are we going to have to add, "And, oh, by the way, we don't mean you—we really do mean you don't have to have intent there"?

Mr. COMEY. Well, that's a conversation for you all to have with the Department of Justice, but it would have to be something more than the statute enacted in 1917, because for 99 years they've been very worried about its constitutionality.

Mr. FARENTHOLD. All right. Well, I think that's something this committee and Congress as a whole, the Judiciary Committee that Mr. Chaffetz and I also sit on, will be looking at it.

And I was on television this morning, and I just want to relay a question that I received from a caller into that television commercial, and it's just real simple. Why should any person follow the law if our leaders don't?

And we can argue about intent or not, but you laid out the fact that she basically broke the law but you couldn't prove intent. Maybe I'm putting words in your mouth, but I do want to know why any person should follow the law if our leaders don't have to. Maybe that's rhetorical, but I'll give you an opportunity to comment on that.

Mr. COMEY. Yeah. That's a question I'm no more qualified to answer than any American citizen. It's an important question.

In terms of my work in my world, my folks would not be—one of my employees would not be prosecuted for this. They would face consequences for this. So the notion that it's either prosecute or you walk around, you know, smiling all day long is just not true for those people who work for the government. The broader question is one for a democracy to answer, it's not for me.

Mr. FARENTHOLD. And I guess the ultimate decision as to whether or not Mrs. Clinton works in government or not is not in—is in everybody's hands.

Chairman CHAFFETZ. I thank the gentleman.

Mr. FARENTHOLD. Yield back.

Chairman CHAFFETZ. We'll now recognize the gentleman from Pennsylvania, Mr. Boyle, for 5 minutes.

Mr. BOYLE. Thank you, Mr. Chairman.

And thank you, Director Comey, for appearing, especially on such short notice.

I want to share with you actually something a friend of mine was expressing when watching your press conference 48 hours ago, and this is someone who's not in any way political; in fact, probably typical of most American citizens today in being depressed about the remarkable level of cynicism we have in our government, but specifically those of us who are in government make decisions first and foremost because of the party hat we wear and not necessarily based on the facts and the evidence.

And he texted me after watching your 15-minute presentation: Oh, it's nice to see a real pro. You can tell that he would make the decision based on the facts and the evidence and not what party he wears.

I think that's so important if we're ever going to get to a place in this country where we restore some of the faith that we had in government. If you looked at the poll numbers from the 1940s and 1950s and you look at faith in government among the American public, and you look at those numbers today, the numbers today are anemic, they're nowhere near the levels that they were decades ago.

So for that, I want to say thank you. And I think that many citizens have the same impression.

When I first met you a couple years ago at a weekend session in Colonial Williamsburg, you might remember that we had a discussion about my biggest concern, frankly, facing the security of the American people, and that is the possibility of a lone wolf terrorist, someone becoming self-radicalized and acting based on that. We had an exchange that I'll keep private, but I think I can characterize that you share my concern.

I'm just thinking, for the last 2–1/2 hours that we've been here, we've had the FBI Director, asking questions on this matter, when, frankly, I would have much rather your time spent dealing with the potential of lone wolf terrorists and other coordinated attacks that we face.

But since this is the Oversight and Government Reform Committee, trying to find something that we can now take and possibly use in a systemic way, not just the celebrity of Secretary Clinton and the fact, because it involves her, let's face it, that's the reason why we're here, but I want to try to take something out of this very expensive and long investigation and try to use it in a productive way toward reforming government that possibly we can get something good out of it.

So toward that end, I'm really concerned about this issue of up-classification, because it seems as if, and I was not aware of this until the investigation, there is quite a strong discrepancy between not just former Secretary Clinton, but even former Secretary Powell, what he thinks should be classified, and then what is classified after the fact. And I think you—if I'm right, there were some 2,000 emails that were up-classified? I was wondering if you could speak to that.

Mr. COMEY. Yeah. It actually was not a concept I was real familiar with before this. It's the notion that something might not have

been classified at the time, but that in hindsight, as a government agency considers releasing it, they raise the classification level to protect it because it would—it's a candid assessment of a foreign leader or something like that.

I think it is largely a State Department thing, because their diplomats will often be conversing in an unclassified way, that when they look at releasing it in response to a FOIA request, they think it ought to be protected in some fashion.

But, honestly, I kind of pushed those to the side.

Mr. BOYLE. Right.

Mr. COMEY. The important thing here was what was classified at the time, that's what matters.

Mr. BOYLE. Right. And that for a law enforcement official matters. But I'm just wondering if you could share with us any of your impressions about a system that exists where there is such gray area and discrepancy in what is classified and what's not, and if you or your agents had any suggestions for us, either in Government Reform, or I happen to be on the Foreign Affairs Committee that has oversight of State Department.

Do you believe that this is a matter that we should take up where there is such discrepancy on what's classified, what's not classified? I think of one example. Ambassador Ross put something in a book that wasn't classified, and then it was up-classified after the book came out. But what good does that do us as a country in terms of trying to protect the intelligence of the United States.

Mr. COMEY. Yeah. I'm not an expert in this up-classification business, but I do suspect it would be a fertile ground for trying to figure out whether there are ways to do it in a more predictable, reliable way.

Mr. BOYLE. Yeah. Well, thank you again for your service.

And I yield back my time.

Chairman CHAFFETZ. I thank the gentleman.

We'll now recognize the gentleman from Georgia, Mr. Hice, for 5 minutes.

Mr. HICE. Director Comey, your statement on Tuesday clearly showed that Secretary Clinton not only was extremely careless in handling classified information, but that also any reasonable person should have known better, and that also, in doing so, she put our national security at risk with her reckless behavior.

So it seems to me that the American people are only left, based on your assessment, with just a few options. Either Secretary Clinton herself is not a reasonable person, or she is someone who purposefully, willfully exhibited disregard for the law, or she is someone who sees herself as above the law.

And to muddy the water even further, after listening to you lay out the facts of the investigation, much of what you said directly contradicted her in previous statements that she had made.

I think it's all this compiled, putting the—connecting the dots that so many American people are irate, that after all of this there was not a recommendation for Secretary Clinton to be prosecuted.

Now, I do greatly appreciate the fact that you came out with much more information on this than you would have in other cases, and I think that was the right the thing to do. Undeniably, this is not a typical case. This is something of great public interest, obvi-

ously the subject of the investigation, former Secretary of State, former senator, and all those things that we have talked about, former first lady, and so forth.

And in addition to this, her husband, who happens to be the former President of the United States, is meeting privately with the Attorney General right before all of this interview takes place. Obviously, this is very suspicious, just the optics of it all. And at the same time that you're coming out, or more or less the same time that you are announcing the decision, Secretary Clinton is flying around in Air Force One with the President doing a campaign event.

I mean, there's nothing about this case that's ordinary, there's nothing about the subject that's ordinary.

So let me ask you this, Director: Did Secretary Clinton in fact, comply with the Department's policies or the Federal Records Act?

Mr. COMEY. I don't think so. I know you have the State inspector general here, who's more of an expert on all the Department's policies, but at least in some respects, no.

Mr. HICE. So keeping the servers at home and all these types of things, obviously, is not in compliance with the Department's policies?

Mr. COMEY. Yes. And I've read the inspector general's report on that. That's part of the reason I can answer that part with some confidence.

Mr. HICE. Okay. And yet she said publicly that she fully complied. So there again is another issue.

If you had the same set of facts but a different subject, a different individual involved, say, just an average, ordinary State Department employee or an anonymous contractor, what would have been the outcome?

Mr. COMEY. I'm highly confident there would be no criminal prosecution no matter who it was. There would be some range of discipline. They might get fired, they might lose their clearance, they might get suspended for 30 days. There would be some discipline, maybe just a reprimand, I doubt it, I think it would be higher on the discipline spectrum, but some sort of discipline.

Mr. HICE. So is it your opinion that there should likewise be some discipline in this case?

Mr. COMEY. That's not for me to say. I can talk about what would happen if it was a government employee under my responsibility.

Mr. HICE. Well, then, what you're laying out is that there is a double standard. For someone else, a different subject, an anonymous contractor or someone at the State Department, there would absolutely be discipline, but because of who the subject is, you're not willing to say there should be discipline. So there's—again, this whole issue, this is what the American people are so upset about.

Let me say that, when you stated that no reasonable prosecutor would pursue this case, is that because the subject of this investigation was unique?

Mr. COMEY. No. Huh-uh. There's no double standard there. And there's no double standard, either, in the sense that if it was John Doe, a former government employee, you'd be in the same boat. We wouldn't have any reach on the guy. He wouldn't be prosecuted.

Mr. HICE. But he would have some discipline?

Mr. COMEY. Well, not if he had left government service.

Mr. HICE. Had they lied about having servers, had they lied about sending and receiving classified emails, had they lied about not deleting those emails to the public, had they lied about not having any marked classified, the statements are clearly documented, and you're saying that an average person would experience discipline, by your own words, but Secretary Clinton does not deserve to be disciplined?

Mr. GOWDY. [Presiding.] The gentleman's time has expired, but the Director may answer if he wants to.

Mr. COMEY. An average employee still in government service would be subject to a disciplinary process. Now, if they'd left, you'd be in the same boat.

Mr. GOWDY. The gentleman from Georgia yields back.

The chair will now recognize the gentleman from Vermont, Mr. Welch.

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

Thank you, Director Comey.

The prosecutor has really awesome power. The power to prosecute is the power to destroy and it has to be used with restraint. You obviously know that. You're being asked to—you had to exercise that responsibility in the context of a very contested Presidential campaign, enormous political pressure.

You had to do it once before. And I go back to that evening of March 10, 2004, when the question was whether a surveillance program authorized after 9/11 by President Bush was going to continue despite the fact that the Justice Department had come to an independent legal conclusion that it actually violated our constitutional rights.

That's a tough call, because America was insecure, the President was asserting his authority as Commander in Chief to take an action that was intended to protect the American people, but you and others in the Justice Department felt that, whatever that justification was, the Constitution came first and you were going to defend it.

And as I understand it, you were on your way home and had to divert your drivers to go back to the hospital to be at the bedside of a very sick at that time Attorney General, and you had to stand in the way of the White House chief of staff and the White House counsel.

I'm not sure that was a popular decision or one that you could have confidently thought would be a career booster, but I want to thank you for that.

Fast forward, we've got this situation of a highly contested political campaign. And there is substantive concern it's legitimate by Democrats and Republicans for independent political reasons, but you had to make a call that was based upon your view of the law, not your view of how it would affect the outcome of who would be the next Commander in Chief.

Others have asked this for you, but I think I'm close to the end. I want to give you a chance to just answer, I think, the bottom line questions here. Had you, after your thorough investigation, found evidence that suggested that criminal conduct occurred, is there

anything, anything or anyone, that could have held you back from deciding to prosecute?

Mr. COMEY. No. I mean, I don't have the power to decide prosecution, but I'd have worked very hard to make sure that a righteous case was prosecuted.

Mr. WELCH. And you would have make that recommendation to the Attorney General?

Mr. COMEY. Yes.

Mr. WELCH. Was there any interference, implicit or explicit, from the President of the United States or anyone acting on his behalf to influence the outcome of your investigation and the recommendation that you made?

Mr. COMEY. No.

Mr. WELCH. Was there anyone in the Hillary Clinton campaign or Hillary Clinton herself who did anything, directly or indirectly, to attempt to influence the conclusion that you made to recommend no prosecution?

Mr. COMEY. No.

Mr. WELCH. At this moment, after having been through several hours of questioning, is there anything in the questions you've heard that would cause you to change the decision that you made?

Mr. COMEY. No. I don't—you know, I don't love this, but it's really important to do, and I understand the questions and concerns. I just want the American people to know, we really did this the right way. You can disagree with us, but you cannot fairly say we did it in any kind of political way. We don't carry water for anybody. We're trying to do what the right thing is.

Mr. WELCH. Well, I very much appreciate that, and I very much appreciate that it takes strong people of independent judgment to make certain that we continue to be a Nation of laws.

Mr. Chairman, just one final thing, and I'll yield to Mr. Cummings. We've got a political debate where a lot of these issues that are going to be—that have been raised are going to be fought in the campaign, and we've got Secretary Clinton who's going to have to defend what she did. She's acknowledged it's a mistake. We've got that great constitutional scholar, Mr. Trump, who's going to be making his case about why this was wrong. But that's politics, that's not really having anything to do with the independence of prosecutorial discretion.

Thank you, Director Comey.

And I yield whatever additional time I have to Mr. Cummings.

Chairman CHAFFETZ. I think the gentleman's going to yield back. I've spoken with Mr. Cummings.

We'll now recognize the gentleman from Kentucky, Mr. Massie, for 5 minutes.

Mr. MASSIE. Thank you, Mr. Chairman.

And thank you, Director Comey, for showing up and your willingness to be transparent and answer a lot of unanswered questions.

A few hours before this hearing started I went onto social media and asked people to submit questions, and I've got over 500 questions, and I don't think I'll get to ask them all in these 5 minutes, but I'm sure you'll be willing to answer them.

One of the common things that I came in here to ask, but I realized it's not the right question now, is what's the difference be-

tween extremely careless and gross negligence. But in the process of this hearing, what I'm hearing you say is, that's not what we—that's not what your reluctance is based on, it's not based on—the reluctance to prosecute, by the way. Your reluctance to recommend a prosecution or an indictment is not based on parsing those words, it's based on your concern for this statute, with this statute, is that correct, from your opening statement?

Mr. COMEY. It's broader than that, actually, the statute, and it fits within a framework of fairness and also my understanding of what the Department of Justice has prosecuted over the last 50 years.

Mr. MASSIE. So when you say a reasonable prosecutor wouldn't take this case, it's not because you don't think she made—that she lied in public or that maybe she was negligent, it's because you have concern with the prosecutorial history of the statute?

Mr. COMEY. And not just that statute, but also 1924, which is the misdemeanor. I also don't see cases that were prosecuted on facts like these. So both, both 793 and 1924.

Mr. MASSIE. But you did find one prosecution. And has it been overturned by the Supreme Court?

Mr. COMEY. No. There was one time it was charged in an espionage case, and the guy ended up pleading guilty to a different offense, so it was never adjudicated.

Mr. MASSIE. So, you know, so that your concern is with the negligence threshold, that you think it requires mens rea, or knowing the crime. But in all 50 States isn't there a negligent homicide statute and aren't people prosecuted for that all the time, and doesn't the Supreme Court and all the courts below that uphold those prosecutions, just on the basis of negligence?

Mr. COMEY. I don't know whether all 50 States. I think negligent homicide and manslaughter statutes are relatively common.

Mr. MASSIE. Okay. So but don't all 50 States have something like that, and aren't those sustained in the upper courts, those convictions?

Mr. COMEY. I don't know whether all 50 States have something like that. But, again, I think it's very common and I think those are sustained.

Mr. MASSIE. So don't we have a history of—you know, you implied that the American judicial system doesn't have a history of convicting somebody for negligence, but don't we in other domains of justice?

Mr. COMEY. We do. I know the Federal system best. There are very few in the Federal system. They're mostly, as we talked about earlier, in the environmental and Food and Drug Administration area.

Mr. MASSIE. Okay. Thank you.

Now, I want to ask another question that's come up here. You've basically related to us that this information, this top secret or classified information, got into these email chains because of conversations people were having, they were relating what they heard before in other settings. Is that correct?

Mr. COMEY. No. Maybe in some cases, but it was people having an email conversation about a classified subject.

Mr. MASSIE. Okay. So they were having an email conversation, but how in this email conversation did this bore marking show up? Like, if they're not sophisticated enough, as you said before, even Hillary Clinton wasn't sophisticated enough to recognize a bore marking, the C with the parentheses for confidential or classified, how did—if they weren't that sophisticated, how did they recreate that bore marking in their emails when they were having these discussions?

Mr. COMEY. Yeah. Somebody—a lot of what ended up on Secretary Clinton's server were stuff that had been forwarded up a chain and gets to her from her staff, a lot of that forwarding, and then she comments sometimes on it.

Someone down in the chain, in typing a paragraph that summarized something, put a portion marking, C—paren, C paren, on that paragraph.

Mr. MASSIE. Can you—doesn't it take a lot of intent to take a classified document from a setting that's, you know, authorized and secure to one that's not? Wouldn't it require intent for somebody to recreate that classification marking in an unsecure setting?

Mr. COMEY. I don't know. It's possible, but also I could——

Mr. MASSIE. I mean, did they accidentally type open parentheses, C, close parentheses, and indent the paragraph?

Mr. COMEY. Oh, no. You wouldn't accidentally type that.

Mr. MASSIE. Right. Someone——

Mr. COMEY. Right.

Mr. MASSIE. Someone down the chain——

Mr. COMEY. Okay.

Mr. MASSIE. So this is my question, is someone down the chain being investigated? Because they had the intent, clearly, if they had the sophistication, which Hillary Clinton, you insinuate, may have lacked, if they had the sophistication to know what this bore marking was, they had the—had to have the intent to recreate it or the intent to cut, copy, paste from a secure system to an unsecure system. Wouldn't that be correct?

Mr. COMEY. Potentially, but we're not—there's not an open criminal investigation of that person way down the chain at the State Department.

Mr. MASSIE. Shouldn't there be?

Mr. COMEY. A criminal investigation?

Mr. MASSIE. An investigation if there's intent, which is what you—I mean, and I think you may be reasonable in requiring that threshold, but don't we treat everybody the same, whether it's at the top of the chain or the bottom of the chain?

Mr. COMEY. Sure. You want to if the conduct is the same. But we did not criminally investigate whoever started that chain and put the C on those paragraphs, we didn't.

Mr. MASSIE. Okay. I would suggest maybe you might want to do that.

And I will yield back to the chairman.

Chairman CHAFFETZ. I thank the gentleman.

We'll now recognize the gentlewoman from Michigan, Mrs. Lawrence, for 5 minutes.

Mrs. LAWRENCE. Director Comey, how many years have you been the Director?

Mr. COMEY. Two—well, 3 years. I know the exact date count, I think, at this point.

Mrs. LAWRENCE. Okay. So how many cases have you investigated, approximately, that you had to render a decision?

Mr. COMEY. The Bureau investigates tens of thousands of cases. The Director only gets involved in a very small number of them.

Mrs. LAWRENCE. So about how many?

Mr. COMEY. I think I've been deeply involved in probably 10 to 20.

Mrs. LAWRENCE. Have you ever been called before Congress on any of those other decisions?

Mr. COMEY. No, this is the first time.

Mrs. LAWRENCE. Thank you.

There are some Republicans who support you. Not surprisingly, they're the ones who actually know you.

And I have a letter here and I would like to enter into the record from Richard Painter, Mr. Chair. He was President Bush's chief ethics lawyer. And may it be entered into the record?

Chairman CHAFFETZ. She's asking unanimous consent. Without objection, so ordered.

Mrs. LAWRENCE. Mr. Painter refers to Mr. Comey as a man of, and I quote, a man of the utmost integrity, who calls the shots as he saw them without regard to political affiliation or friendship.

He states, and I quote: Throughout the FBI investigation of Secretary Clinton's email server, I have been convinced that the Director would supervise the investigation with being impartial and strict adherence to the law, as well as prosecutorial precedent.

He also adds: Although I'm aware of very few prosecutions for carelessness in handling classified information as opposed to intentional disclosure, I knew that the Director would recommend prosecution in any and all circumstances where it was warranted. I cannot think of someone better suited to handle such a politically sensitive investigation.

Finally, and I quote: I urge all Members of the United States Congress to stop from inferring in specific decisions, particularly those involving political allies or opponents. During my tenure in the White House, there were very unfortunate allegation that powerful senators sought politically motivating firing of a United States Attorney. Whether or not such allegations were true, it is imperative, and I'm still quoting, that members of the Senate or the House never again conduct themselves in a manner where such interference could be suspected.

And I want to be on the record, I wholeheartedly agree with Mr. Painter.

Director, you have demonstrated yourself, you sat here and answered the questions. And I would never oppose to finding the answers to any situation that is directly related to Federal agencies which we on this committee are responsible for. But I want to be clear that Congress has no business—no business—interfering with these types of decisions that are coming in this—in your responsibility.

These type of attacks are not only inappropriate, but they're dangerous. They're dangerous because they could have a chilling effect on the future investigations.

And I asked that question, how long have you been in this position and how many times have you made decisions and yet were not pulled in 24 hours before this committee? How many times? And then we say it's not political.

And you have said repeatedly, regardless of who it was, you conducted the investigation as required under your responsibility. And here you have Republicans who are saying you are an honorable man, and till this day, I have not heard any complaints of your judgment.

So I sit here today as a Member of Congress on the record that the slippery slope that we're seeing today in this hearing, I want every Member to be cautious of what we're saying, that in America when we have investigations, that we will allow our own elected Congress and Senate to make this a political agenda to attack, but only if it's in their agenda. This goes for Democrats and Republicans. We are not here to do that.

Thank you, and I yield back my time.

Chairman CHAFFETZ. I thank the gentlewoman.

We'll now recognize the gentleman from Iowa, Mr. Blum.

Mr. BLUM. Thank you, Mr. Chairman.

Thank you, Director Comey, for being here today, and thanks for hanging in there till every last question is answered.

I'm not a lawyer. That's the good news. I'm a career businessman. I've spent most of my career operating in the high-tech industry. And today I've heard words such as common sense, reasonable person, carelessness, judgment, or lack thereof. I like these words. I understand these words. I think the average American does as well. So I'd like to focus on that.

Last Tuesday, Director Comey, you said, and I quote: "None of these emails should have been on any kind of an unclassified system, but their presence is especially concerning because all these emails were housed on unclassified personal servers not even supported by full-time security staff, like those found at agencies of the United States Government, or even with a commercial email service such as Gmail."

Director Comey, my small Iowa business doesn't even use Gmail for our email, because it's not secure enough. I know some security experts in the industry. I checked with them. The going rate to hack into somebody's Gmail account, $129. For corporate emails, they can be hacked for $500 or less. If you want to hack into an IP address, it's around $100. And I'm sure the FBI could probably do it cheaper. This is the going rate.

Director Comey, are you implying in that statement that the private email servers of Secretary Clinton's were perhaps less secure than a Gmail account that is used for free by a billion people around this planet?

Mr. COMEY. Yes. And I'm not looking to pick on Gmail. Their security is actually pretty good. The weakness is in the individual users.

But, yes, Gmail has full-time security staff and thinks about patching and logging and protecting their systems in a way that was not the case here.

Mr. BLUM. I'd like to ask you, what kind of judgment—we talked a lot about judgment today—does this decision to potentially ex-

pose to hackers classified information on an email service that's less secure than Gmail—your words—what does that suggest to you? What type of judgment does that suggest to you?

Mr. COMEY. It suggests the kind of carelessness that I talked about.

Mr. BLUM. In August of last year, Secretary Clinton was asked by Ed Henry of Fox News whether she had wiped her entire server, meaning did she delete all the emails on her server. Her response: "You mean with a cloth?"

March of 2015, during a press conference, Secretary Clinton assured us her private email server was secure, saying the server was on private property guarded by the Secret Service.

Now, this would be laughable if it wasn't so serious. I know, you know, my constituents in eastern Iowa know you don't need to be a cat burglar to hack into an email server and you don't need a cloth to wipe a server clean. One would think that a former United States senator, one would think that a former secretary of state would know this as well. Would you agree with that statement?

Mr. COMEY. You would think, although as I said before, one of the things I've learned in this case is that the Secretary may not have been as sophisticated as people assume. She didn't have a computer in her office at the State Department, for example. So I don't think—so I would assume the same thing about someone who had been a senator and a high-ranking official. I'm not sure it's a fair assumption in this case.

Mr. BLUM. In your opinion, Director Comey, did Secretary Clinton know that a server could, in fact, be wiped clean electronically and not with a cloth?

Mr. COMEY. Well, I assume that—I don't know.

Mr. BLUM. Would you assume she knows that?

Mr. COMEY. I would assume that it was a facetious comment about a cloth, but I don't know. I don't know in particular on that one.

Mr. BLUM. Would you also assume, Director, that Secretary Clinton knew that a server could be wiped clean electronically, that it could be hacked electronically, not physically, you don't need a cat burglar to hack a server? Would you assume—would it be reasonable to assume she knows that?

Mr. COMEY. To some level it would be reasonable, to some level of understanding.

Mr. BLUM. Then, once again, for someone who knew these things, or we assume to some level she knew these things, what kind of judgment does the decision to expose classified material on personal servers suggest to you, what type of judgment?

Mr. COMEY. Well, again, it's not my place to assess judgment. I talk in terms of a state of mind, negligence in particular. I think there was carelessness here, and in some circumstances extreme carelessness.

Mr. BLUM. Was her server hacked?

Mr. COMEY. I don't know. I can't prove that it was hacked.

Mr. BLUM. So that answer says to me it could have been hacked.

Mr. COMEY. Sure. Yeah.

Mr. BLUM. And if it was hacked, potentially damaging material damaging to American secrets, damaging to American lives, could have been hacked. Could have been exposed, correct?

Mr. COMEY. Yeah.

Mr. BLUM. Lives could have been put at risk if that server was indeed hacked?

Mr. COMEY. I'm not prepared to say yes as to that last piece. That would require me going into in a way I can't here the nature of the classified information. But there's no doubt that it would have potentially exposed the information that was classified. The information was classified because it could damage the United States of America.

Mr. BLUM. So it could have happened. The FBI just isn't aware?

Mr. COMEY. Correct.

Mr. BLUM. Thank you very much. Thank you for being here. I yield back the time I do not have.

Chairman CHAFFETZ. Thank the gentleman. I now recognize the gentlelady from New Jersey, Mrs. Watson Coleman, for 5 minutes.

Mrs. WATSON COLEMAN. Thank you. And thank you, Director. I've got a number of questions. So I'm going to, like, zip through these.

Mr. COMEY. Okay.

Mrs. WATSON COLEMAN. This is a question I'm going to ask and you, and may not even have the answer to it because you may not have known this. This is about the classification marking issue that you've been asked about earlier. According to the State Department, which addressed this issue yesterday, a spokesman said that the call sheets appear to bear classified markings. But this was actually a mistake. To quote, "Generally speaking, there's a standard process for developing call sheets for the Secretary of State. Call sheets are often marked, but it's not untypical at all for them to be marked at the confidential level prior to a decision by the Secretary that he or she will make that call. Oftentimes, once it is clear the Secretary intends to make a call, the Department will then consider the call sheet SBU, sensitive but unclassified, or unclassified altogether and then mark it appropriately, and then prepare it for the Secretary's use and actually marking the call."

"The classifications of a call sheet, therefore, is not necessarily fixed in time and staffers in the Secretary's office who are involved in preparing and finalizing these call sheets, they understand that. Given this context, it appears that markings in the appropriate—in the documents raised in the media reports were no longer necessary or appropriate at the time. They were sent as an actual email. Those markings were human error. They didn't need to be there." Did you know this?

Mr. COMEY. No.

Mrs. WATSON COLEMAN. Thank you, Mr. Director. Can you tell me, based upon your information, has there been, and is there any evidence that our national security has been breached or at risk as a result of these emails, and their being on this server? Is there any evidence?

Mr. COMEY. There's no direct evidence of an intrusion.

Mrs. WATSON COLEMAN. Thank you very much. I have to tell you that while I think that this should conclude this discussion, I know

we're going to hear this issue ad nauseam. But I am concerned about another issue that I think really is resonating with the people in this country.

And that issue has to do with experiences that we had just the last 2 days. Mr. Director, I want to bring this up for your consideration, because I want to ask you what can the FBI do—FBI do in this issue? This morning we woke up to another graphic and deeply disturbing video that actually brought me to tears when my staff played it for me wherein a Minnesota woman's boyfriend was—has been shot as her young child set in the back seat after apparently telling the officer he was licensed to carry a weapon, he had it on him, and was going to reach for his identification.

Just the other day there was an incident in Baton Rouge involving a Mr. Alton Sterling, an African American man who was shot while pinned to the ground by police officers in Baton Rouge. An interaction tape by two bystanders with cell phones captured this.

So I think that we have got an issue here. An issue of real national security. And I want to ask you, Mr. Director, do we have an opportunity to direct our time and resources in your department to those issues? Is it not important that we say their names to remind people of the loss of a Tamir Rice, to an Eric Garner, to an Alton Sterling, to a John Crawford, III, to a Michael Brown, to a Walter Scott, and even a Sandra Bland? Deaths in the hands of police custody, or by police happening. Are these not happening at an alarming rate? And is this not a legitimate space for the FBI to be working in?

Mr. COMEY. Yes, is the emphatic answer. Those are incredibly important matters. As you know, the FBI spends a lot of time on them because they—they're very, very important. We have an investigation open on the Baton Rouge case. I was briefed this morning on the Minnesota case. And I would expect we'll be involved in that as well. It's an important part of our work.

Mrs. WATSON COLEMAN. Do you feel that you have the sufficient resources from the legal imperative to the funding to address these cases and what seems to be a disturbing pattern in our country today?

Mr. COMEY. I'm a bad bureaucrat, but I believe I have sufficient resources and we are applying them against those situations. Because I believe the individual cases matter enormously, but also, the people's confidence in law enforcement is one of the bedrocks of this great country of ours. So I have the resources, and we're applying them.

Mrs. WATSON COLEMAN. And, in addition, we believe that our law enforcement is, by and large, of high integrity and has the desire to keep us protected and safe. But when we find out that there are these occasions, and when there's an indication that there's a pattern that is taking place in this country, we have a responsibility to ensure that everyone in this country is safe. And simply because you're a black man or a black woman does not make you a target. Thank you. I yield back my time.

Chairman CHAFFETZ. Thank the gentlewoman. We'll now recognize the gentleman from North Carolina, Mr. Walker.

Mr. WALKER. Thank you, Mr. Chairman. Thank you, Director Comey, for being here. A few things in this town that people agree

on both sides of the aisle. And one is your reputation. Reminded the passage in James, "Swift to hear, slow to speak, slow to wrath." I am a little disappointed in some of the things that I've heard from my colleagues about some of the attacks on your character and your integrity. I haven't heard those, and I hope that we have not experienced that. I also struggle with the change of heart that we're hearing today. Because I have a list of elected officials who have questioned your investigation, even attacked it. In fact, the former President Clinton said this is a gain. In fact, just last Friday, Ms. Wasserman Schultz, Congresswoman Wasserman Schultz said Secretary Clinton is not the target of this investigation or whatever you want to call it. My question to you today is do you feel like this has been a Republican witch hunt? This hearing.

Mr. COMEY. No.

Mr. WALKER. Okay. Thank you for——

Mr. COMEY. No, I said at the beginning I understand people's questions and interest. And I'm a huge fan of transparency. I think that's what makes our democracy great.

Mr. WALKER. I think those are one of the reasons of why you are so respected. To me, this hearing is about understanding and disseminating the facts, how you saw them, and how the American public sees them. And specifically, in the areas of where there was wrongdoing admitted under your investigation, where there was obviously breaking the law. But also some coverups. Did Congress ask you to pursue this investigation?

Mr. COMEY. No. It was a referral from the inspector general of the intelligence community.

Mr. WALKER. So it wasn't Republicans either. Was it?

Mr. COMEY. No.

Mr. WALKER. How did you go about collecting the evidence?

Mr. COMEY. We used the tools that we normally use in a criminal investigation.

Mr. WALKER. Did or do you receive a congressional referral for all the information that you collected?

Mr. COMEY. Not to my knowledge.

Mr. WALKER. Well, then one of the things that I'm struggling with, or that I would like to know specifically is, under oath, Ms. Clinton made these three comments that we now know are untrue in the Benghazi hearing. Number one, she's turned over all her work-related emails; number two, telling the committee that her attorneys went through every single email; and then finally, and probably the one that continues to stick the most, there was, and I quote, "Nothing marked classified on my emails," end quote. Now, earlier, when the chairman questioned you about this, you said something about needing a congressional referral recommendation. My question is, something of this magnitude, why or can you help me understand, why didn't it rise to your investigation, or someone bringing that to your knowledge as far as saying this is a problem, here she is, again, Secretary Clinton lying under oath, specifically about our investigation?

Mr. COMEY. Well, we, out of respect for the legislative branch being a separate branch, we do not commence investigations that focus on activities before Congress without Congress asking us to get involved. That's a longstanding practice of the Department of

Justice and the FBI. So we don't watch on TV and say: We ought to investigate that. You know, Joe Smith said this in front of the committee. It requires the committee to say: We think we have an issue here. Would you all take a look at it.

Mr. WALKER. But with all due respect, if you had the Secretary Clinton, who is under oath speaking about your very investigation, and you talked about your wonderful staff, and certainly have no reason to deny that, why wouldn't that rise to the level of suspicion? Here she is saying this under oath. I mean, lying under oath is a crime. Is it not?

Mr. COMEY. Yes.

Mr. WALKER. And what's the penalty on that? That's considered perjury, right?

Mr. COMEY. Perjury. It's a felony. I forget the exact—it's potentially years in prison.

Mr. WALKER. But I don't understand. Would you help me understand why somebody wouldn't have tipped you off that she's talking about the very specific case under oath that you're investigating.

Mr. COMEY. Well, there's a difference between us being aware of testimony and us opening a criminal investigation for potential perjury. Again, it's not this case in particular, but all cases. We don't do that without a committee saying we think there was an issue in testimony given in this separate branch of the government.

Mr. WALKER. You also mentioned earlier, and it's been quoted several times that no reasonable prosecutor would move forward with some of the facts. Is there any room at all that somebody would differ a little bit on the opinion? I know that former United States Attorney General Michael Mukasey said would the illegal server disqualify her from ever holding any Federal office? So there are some people of high esteem that may differ, obviously not privy to the exact facts, but can you make any room—you said no reasonable person. Do you understand why the American people, or would you understand why other people may say that she has stepped across the line or broken enough law here that you would come to a different conclusion?

Mr. COMEY. Sure. I respect different opinions. My only point is, and I said earlier I smile because those folks are my friends. I've worked with them for a long time. None of those guys in my position, I believe, knowing what I know, would think about it differently. But I also respect that they have a different view from the outside.

Mr. WALKER. Thank you, Mr. Chairman. Yield back.

Chairman CHAFFETZ. I thank the gentleman. I now recognize the gentleman from California, Mr. DeSaulnier.

Mr. DESAULNIER. Thank you, Mr. Chairman. Director, I just want to thank you as others have and I know you don't need this, but I think the American people clearly need to hear it. And you've done a wonderful job today. But there are moments in my political life and as an American I despair for the future of this country. Not often. But in those moments comes an individual like yourself either by providence or good fortune or by the framework of the U.S. Constitution, and I really believe you have served this country and all Americans well, irrespective of their party affiliation.

So really two questions. Two lines of questions, I should say. One is, and another colleague has brought this up. But you mentioned in just previous testimony about the bedrock and the importance of public confidence in public safety institutions, yours and all. So I just want to give you an opportunity, I think you have responded to this multiple times, but give you a little more opportunity, because I think it's important for the American public to know that the system isn't rigged, that there are people such as yourself, and the 15 individuals who worked on this case and others that do their job and believe in the Constitution of the United States. And if you have any further comments about comments that would say that the system's rigged and Americans should give up on the system?

Mr. COMEY. No, I—one of reasons I welcome this opportunity to have this conversation is I was raised by great parents who taught me you can't care what other people think about you. Actually, in my business, I have to and deeply do, that people have confidence, that the system's not fixed against black people, for rich people, for powerful people. It's very, very important that the American people understand that there really are people that you pay for with your tax dollars who don't give a rip about Democrats or Republicans or this or that, who care about finding out what is true.

And I am lucky to lead an organization that is that way to its core. I get a 10-year term to ensure that I stay outside of politics. But in a way, it's easy. I lead an organization that is resolutely apolitical. We are tough, aggressive people. If we can make a case, we'll make a case. We do not care what the person's stripes are or what their bank account looks like.

And I worry very much when people doubt that. It's the reason I did the press conference I did 2 days ago. I care about the FBI's reputation. I care about the Justice Department. I care about the whole system deeply. And so I decided I'm going to do something no Director's ever done before. I'm not going to tell the Attorney General or anybody else what I'm going to say, or even that I'm going to say it. They didn't know, nor did the media know, until I walked out what I was going to talk about.

And then I offered extraordinary transparency, which I'm sure confused and bugged a lot of people. It's essential in this democracy that people see as much as they can so they can make their judgment. Again, you may—they may conclude I'm an idiot. I should reason differently. But what I hope they will not conclude is that I am a dishonest person.

I am here trying to do the right thing in the right way. And I lead 36,000 people who have that as their spine. That's what I want them to know. I don't care that people agree or disagree. That's what's wonderful about our democracy. But at its core, you need to know there are good people trying to do the right thing all day long. And you pay for them, and we'll never forget that.

Mr. DESAULNIER. I appreciate that. And within the context of these are human institutions, pretty clear to me as a nonlawyer that you got a bright line in terms of your decision about pursuing prosecution. But you did spend an extended period of time talking about what I think I take from you as being fairly objective analysis of what was careless in terms of handling of it, either ascribed

to the former Secretary of State or to the Department. And you said, and I quote, during your comments, "While not the focus of our investigation, we also developed evidence that the security culture of the State Department in general and respect to the use of unclassified email systems in particular was generally lacking in the kind of care for classified information found elsewhere in the government." That's accurate. Isn't it?

Mr. COMEY. Yes, sir.

Mr. DESAULNIER. So struggling with this, and this is in the context of this hearing, Oversight and State Department, and this committee, as to how do we go from here and be clearer about how the State Department, we'll talk about this with the IG, and some of the comments that former Secretary Powell has made, including that the absurdity of the retroactive classification. And now we have 1,000 of these emails from Secretary Clinton that's out in the public and are being spread even further.

So there are other people involved. Sitting there, how does this committee go forward to make sure that the State Department can still function in the way it does with human beings and have conversations that are both transparent but also national security? What are the things we need to do to make sure that this doesn't happen again?

Mr. COMEY. Well, I think a good start—I think the reason the chairman has the IG from the State Department here is to start that conversation. The IG knows deeply the culture of a Department, and is far better equipped than I to say you ought to focus here, you ought to focus there to make it better. So I think that's place to start.

Mr. DESAULNIER. Thank you, Mr. Director. I yield back.

Chairman CHAFFETZ. Thank you. We'll now recognize the gentleman from Tennessee, Mr. DesJarlais, for 5 minutes.

Mr. DESJARLAIS. Director Comey, thank you for appearing so quickly on short notice. I think it's really important that you're here. Because of the way you laid out the case on Tuesday, there is a perception that you felt one way and then came to another conclusion. I, like many of my colleagues, put a post up back in my district and let them know you were coming. And in less than 24 hours, I had 750 questions sent to ask you.

So, again, thank you for being here. But a common theme, just to summarize, a lot of those concerns were that in this case, Clinton was above the law. That there was a double standard. And a lot of that was based on the way you presented your findings. Now, your team, you said you did not personally interview her on Saturday but your team did for about 3–1/2 hours, correct?

Mr. COMEY. Yes.

Mr. DESJARLAIS. Okay. Do you know in reading the review or the summary, did they ask Hillary Clinton about her comment that she had never sent or received classified information over private email?

Mr. COMEY. I think so. But I can't—I can't remember specifically.

Mr. DESJARLAIS. Okay.

Mr. COMEY. It's a very long 302. I'd have to check.

Mr. DESJARLAIS. And we'll get access to that. Do you know if they asked her when she said that there was nothing marked classified on my email sent or received?

Mr. COMEY. Same answer. I'm not sure.

Mr. DESJARLAIS. Okay. And so the same answer then when she said, "I did not email any classified material to anyone on my email. There is no classified material." You don't know whether they asked her that?

Mr. COMEY. I don't know whether they asked her that question. The entire interview was going—was focused on so what did you know, what did you see, what is this document. That kind of thing.

Mr. DESJARLAIS. Do you know if they asked her whether she stands by the fact that she said she just used one device and that was for her convenience?

Mr. COMEY. I don't know. I know they established from talking to her she used many devices during here 4 years. So I don't know whether they asked her specifically about that statement.

Mr. DESJARLAIS. Okay. I guess my——

Mr. COMEY. That's easy to check, though.

Mr. DESJARLAIS. I guess my point is, you're trying to get inside the head of Hillary Clinton in this investigation and know whether there was intent. And so we all know what she told the people. That's been well-documented. She said that she did not do those things, that she did not send or receive classified emails, that she used one server and one device for her convenience, and since then, I think even in your statement you recognize that those were not correct. Is that fair?

Mr. COMEY. I really don't want to get in the business of trying to parse and judge her public statements. And so I think I've tried to avoid doing that sitting here.

Mr. DESJARLAIS. Why do you feel that's important?

Mr. COMEY. Because what matters to me is what did she say to the FBI. That's obviously first and foremost for us.

Mr. DESJARLAIS. Right. Honest people don't need to lie. Is that right?

Mr. COMEY. Honest people don't need to lie? I hope not.

Mr. DESJARLAIS. Okay. Well, in this case, for some reason, she felt the need to misrepresent what she had done with this server all throughout the investigation. And you guys, after a year, brought her in on Saturday. And in 3–1/2 hours, came out with the conclusion that she shouldn't be prosecuted because there was no intent. Is that right?

Mr. COMEY. No.

Mr. DESJARLAIS. Okay. So I don't want to put words in your mouth, but is it fair to say that your interpretation of Hillary Clinton's handling of top secret information and classified documents was extremely careless?

Mr. COMEY. Yes.

Mr. DESJARLAIS. And is it fair to say that you said that you went on to define "extremely careless" that Hillary Clinton's handling of top secret information was sloppy or represented sloppiness?

Mr. COMEY. Yeah. That's another way of trying to express the same concept.

Mr. DESJARLAIS. Okay. And then just a few minutes ago, you also stated that you now believe that Hillary Clinton is not nearly as sophisticated as people thought. Is that correct?

Mr. COMEY. Yeah. I think that's fair, actually. No, not as people thought, but as people would assume about somebody with that background. I'm sorry. I should be clear about this. Technically sophisticated. I'm not opining in other kinds of sophistication.

Mr. DESJARLAIS. All right. In the last minute, Director, I want to talk a little bit about precedent. Because I think my colleague, Trey Gowdy, made a great point that there still is really no precedence in terms of punishment for this type of behavior. Are you familiar with Brian Nishimura's case?

Mr. COMEY. Yes.

Mr. DESJARLAIS. Okay. He's a Naval Reservist for those who don't know. And he was prosecuted. What is the difference between his case and Hillary Clinton's case in terms of extremely carelessness and gross negligence, because we're dealing with statute 793, section (f), where it does not require intent. Is that correct?

Mr. COMEY. I'm sorry. 793(f) is the gross negligence standard.

Mr. DESJARLAIS. Right. And is that why Brian Nishimura was punished?

Mr. COMEY. No. Nishimura was prosecuted under the misdemeanor statue 1924 on facts that are very different. If you want me to go through them, I'll go through them, but very different that——

Mr. DESJARLAIS. Okay. I think that there's been a review of this case, and they're very similar. And that's why people feel that there's a double standard.

Mr. COMEY. What they're reading in the media is not a complete accounting of the facts in that case.

Mr. DESJARLAIS. Well, would you agree, then, with Representative Gowdy that there still is really no precedence for punishing someone like Hillary Clinton and she could really go in—potentially be elected President and do this again without fear of being punished?

Mr. COMEY. I don't think I'm qualified to answer that question.

Mr. DESJARLAIS. My time's expired. Thank you for your time.

Chairman CHAFFETZ. Thank the gentleman. I now recognize the gentlewoman from New Mexico, Ms. Lujan Grisham.

Ms. LUJAN GRISHAM. Thank you, Mr. Chairman. I've had the benefit of when you're last, or nearly last to really have both the benefit and then the question, the kinds of statements and the dialogue back and forth. And where I am settled at this point in time is in a couple of places. But particularly, I don't think there's any member in this committee or, quite frankly, any Member in Congress who doesn't both want and expect that the FBI and the Department of Justice to be and to operate in a fair, unbiased, highly independent manner. Otherwise, you can't appropriately uphold or enforce Federal law. And while we have all—this has been stated in a couple of different ways, I'm going to see if we can't—I want to get direct answers.

So, Mr. Comey, is there any evidence, given that that's the standard that we all want, desire, and expect, to suggest that Hillary Clinton was not charged by the Department of Justice due to inap-

propriate political influence, or due to her current or previous public positions?

Mr. COMEY. Zero. And if there is such evidence, I'd love folks to show it to me.

Ms. LUJAN GRISHAM. In that regard, was there a double standard?

Mr. COMEY. No. In fact, I think my entire goal was to avoid a double standard, to avoid what sometimes prosecutors call celebrity hunting and doing something for a famous person that you would never do for an ordinary Joe or Jane.

Ms. LUJAN GRISHAM. Thank you. And I really appreciate that you're here today, and explaining the process in great detail, frankly, and I've—this committee works at getting specific detail about a variety of reviews, investigations, policies, concepts throughout Federal Government. And I think I can say that this committee often finds that we don't get very much clarity or specific responses to the majority of questions that we ask. So I really appreciate that. And that in explaining that what led the FBI to conclude that Hillary Clinton should not be charged.

Saying that, however, I'm still concerned, frankly, that the use of this hearing and some of the public statements made by elected officials accusing the Department of Justice of using a double standard without any evidence at all to support that statement, leaning on accusations of such, in fact, jeopardizes the very thing that we want the most, which is an apolitical and independent Department of Justice. And we have every right to ask these tough questions.

And to be clear that the process that you use for everyone, including elected officials, works. And that there's a responsibility not to substitute your own political preferences to the outcome of an independent and apolitical Department of Justice investigation on any level, whether it involves Hillary Clinton or anybody else. Do you agree with that general statement?

Mr. COMEY. Yes.

Ms. LUJAN GRISHAM. For me, that's a really important ethical line that I believe should never be crossed. I worry that some of what we did today could be, frankly, interpreted as violating that very standard. And for that, I certainly want the American people and my constituents who are watching to understand that very important line, and to be sure that our responsibility is better served making sure that we do have, in fact, an independent body whose aim it is to bring about truth and justice and uphold the Federal law. And, sir, based on everything that you've said today, I don't see any reason to disagree with your statements, your assessments, or the explanation of that process.

With the little time I do have left, I do want to say that given that some of the classified material that we have both debated and talked about today can be classified later or up-classified, or that other agencies have different determinations of what constitutes classified and not. I do think that's a process that warrants refining. And if something can come out of this hearing about making sure that we do something better in the future for everyone, not just appointed or elected officials, that that ought to be something that we do.

I'm often confused by some of the things that are clearly told to us in a classified briefing that appear to be different or already out in the public in some way. And I'm not sure who's making those decisions. I honor my responsibility to the highest degree, but I think that's a process that could use some significant refining, and that's my only suggestion, sir. Thank you for being here today.

Mr. COMEY. Thank you.

Chairman CHAFFETZ. Thank the gentlewoman. We'll now recognize the gentleman from Georgia, Mr. Carter, for 5 minutes.

Mr. CARTER. Thank you, Mr. Chairman. And, Director Comey, thank you for being here today. I appreciate it. I'm over here. And I'm going to be real quick and try to be succinct. I want to clarify some things that you said. And, look, I don't want to go over everything that everybody's been through today. I mean, we've had some great questions here that have asked you about you said this, she said that. Representative Gowdy made a great case of, you know, this is what she said under oath and publicly, and yet you dispute that and say, No, this is the case. But, look, I've just got a couple of questions. Okay? First of all, did I understand you correctly that your decision—that this decision was made within 3–1/2 hours of an interview and that was all?

Mr. COMEY. No. We investigated for a year.

Mr. CARTER. But you interviewed her for 3–1/2 hours last week and then came to the conclusion?

Mr. COMEY. Correct. We interviewed her on Saturday for 3–1/2 hours. The last step of a yearlong investigation.

Mr. CARTER. Now, as I understand it, Hillary Clinton has testified that the servers that she used were always safe and secure. Yet you refute that and say, No, that is not the case at all. Were they ever secure? Were the servers that she were using, were they ever secure?

Mr. COMEY. Well, the challenge, security's not binary. It's just degrees of security. It was less security than, one, at the State Department, or, as I said, even one at a private commercial provider, like a Gmail.

Mr. CARTER. Well, let me ask you this: She's got staff and she's got people around her. Did they know she was doing this? Did they know that she was using these other devices? Did anybody ever bring it to her attention and say, Hey, you're not supposed to be doing that?

Mr. COMEY. I think a lot of people around the Secretary understood she have was using a private personal email setup.

Mr. CARTER. Then why didn't they say something? Don't they have a responsibility as well?

Mr. COMEY. That's an important question that goes to the culture of the State Department that's worth asking.

Mr. CARTER. I mean, look, we all surround ourselves with good people and we depend on them to help us. I don't understand—should they be held responsible for that, for not bring that to someone's attention? If I see someone who's breaking—who's not following protocol, is it my responsibility to report them?

Mr. COMEY. Yes.

Mr. CARTER. Well——

Mr. COMEY. Especially when it comes to security matters. You have an obligation to report a security violation that you may witness, whether it's involving you or one of your co-workers. But this is about so——

Mr. CARTER. What about Bryan Pagliano? Did he ever know? Do you know if he knew that she was not following proper protocol here?

Mr. COMEY. He helped set it up.

Mr. CARTER. He helped set it up. So obviously he knew.

Mr. COMEY. Yeah. Obviously, he knew that——

Mr. CARTER. Okay. Is anything going to be done to him? Any prosecution or any discipline, any——

Mr. COMEY. I don't know about discipline, but there's not going to be a prosecution of him.

Chairman CHAFFETZ. Will the gentleman yield?

Mr. CARTER. I yield.

Chairman CHAFFETZ. My understanding, Director, is that you offered him immunity. Why did you offer him immunity, and what did you get for it?

Mr. COMEY. Yeah. That I have to—I'm not sure what I can talk about in open setting about that.

Chairman CHAFFETZ. Well, he's not going to be prosecuted. So——

Mr. COMEY. Right. But I want to be careful. I'm doing this 24 hours after the investigation closed. I want to be thoughtful because we're, as you know, big about the law, that I'm following the law about what I can disclose about that. So I'll have to get back to you on that one. I don't want to answer that off the cuff.

Mr. CARTER. Director Comey, I am not a lawyer. I'm not an investigator. I'm a pharmacist. But I'm a citizen. And citizens are upset. I watched, with great interest, last—earlier this week when you laid out your case. And I'm telling you, you laid it out, bam, bam, bam. Here's what she did wrong, wrong, wrong, wrong. And then all of a sudden, you used the word "however." And it was like you could hear a gasp throughout the country of people saying, Oh, here we go again. Do you regret presenting it in a way like that?

Mr. COMEY. No. And I'm highly—I think I didn't use the word "however." I try never to use that in speaking. But I did lay it out, I thought, in the way that made sense and that I hoped was maximum transparency for people.

Mr. CARTER. I'm sorry, but that's the point. It didn't make sense. The way you were laying it out it would have made sense and the way that the questions have been asked here and we've made all these points of where she was—obviously told lies under oath, that it would have been, Okay, we finally got one here.

Mr. COMEY. I think it made sense. I just hope folks go back maybe with a cup of tea and open their minds and read my statement again carefully. But again, if you disagree, that's okay. But——

Mr. CARTER. But when we—look, I've only been here 18 months. And I want to tell you, this inside-the-beltway mentality, no wonder people don't trust us.

Mr. COMEY. I have—I know who you're talking about. I have no kind of inside-the-beltway mentality.

Mr. CARTER. But this is an example of what I'm talking about here. It just as a nonlawyer, as a noninvestigator, it would appear to me you have got a hell of a case.

Mr. COMEY. Yeah. And I'm telling you we don't. And I hope people take the time to understand why.

Mr. CARTER. Mr. Chairman, I yield back.

Chairman CHAFFETZ. Thank the gentleman. I will now recognize the gentleman from Arizona, Mr. Gosar. Oh, let's go ahead and go to the gentleman from South Carolina, Mr. Mulvaney, first.

Mr. MULVANEY. Thank the gentleman. Director Comey, earlier today you heard a long list of statements that Mrs. Clinton has made previously, both to the public and to Congress that were not factually accurate. I think you went down the whole long list. When she met with you folks on Saturday last week, I take it she didn't say the same things at that interview?

Mr. COMEY. I'm not equipped sitting here without the 302 in front of me to answer in that broad——

Mr. MULVANEY. But it's your testimony——

Mr. COMEY. I have no basis that—we do not have a basis for concluding she lied to the FBI.

Mr. MULVANEY. Gotcha. Did anybody ask her on Saturday why she told you all one thing and told us another?

Mr. COMEY. I don't know as I sit here. I mean, I'll figure that out——

Mr. MULVANEY. Would that have been of interest to you in helping to establish intent?

Mr. COMEY. It could have been, sure.

Mr. MULVANEY. More importantly, I think, did anybody ask her why she set up the email system as she did in the first place?

Mr. COMEY. Yes.

Mr. MULVANEY. And the answer was convenience?

Mr. COMEY. Yeah. It was already there. It was a system her husband had. And so she just jumped onto it.

Mr. MULVANEY. Were you aware that just earlier this week, her assistant actually said it was for an entirely different reason? It was to keep emails from being accessible, and that it was for concealment purposes? And Huma Abedin was asked in her deposition why it was set up. And it was said to keep her personal emails from being accessible. The question, to whom. To anybody. Were you aware of that testimony?

Mr. COMEY. Generally, yes.

Mr. MULVANEY. Okay. So here's sort of the summary I take from what we've done today, which is that over the course of the entire system, what she did, she intentionally set up a system. According to your testimony, your findings, she was careless regarding its technical security. I think you've said that even a basic free account, a Gmail account had better security than she had. And she did that, according to her own staffer's sworn deposition for the purpose of preventing access to those emails. As a result of this, she exposed top secret information to potential hack by foreign actors. You've seen the emails, we have not. I think you've said earlier that the emails could be of the sort that would put national security at risk, and I think we had testimony earlier that got you acknowledge that it might even put our agents overseas at risk.

Mr. COMEY. Yeah. I don't think I agree with that. But it's still important.

Mr. MULVANEY. Okay. All right. She kept all of that secret until after she left the State Department. She lied about it, or at least made untrue statements about it after it finally came to light. She, thereafter, ordered the destruction of evidence, evidence that was destroyed so thoroughly that you folks could not do an adequate recovery. Yet she receives no criminal penalty. So I guess this is my question to you: Are we to assume, as we sit here today, that if the next President of the United States does the exact same thing, on the day he or she is sworn into office, sets up a private email service for the purpose of concealing information from the public or from anybody, that as a result of that, potentially exposes national security level information to our enemies, lies about it, and then destroys the evidence during an investigation, that there will be no criminal charges if you're the FBI Director against that person?

Mr. COMEY. That's not a question the FBI Director should answer. I mean——

Mr. MULVANEY. No, I'm asking if she does the exact same thing as President as she's done today, your result will be the exact same as it was 48 hours ago. There will be no criminal findings, right?

Mr. COMEY. If the facts were exactly the same?

Mr. MULVANEY. Right.

Mr. COMEY. And the law was exactly the same?

Mr. MULVANEY. Right.

Mr. COMEY. Yeah. The result would be the same.

Mr. MULVANEY. And I guess under the theory that if the law is to be equally applied to everybody, that if a White House staffer does the exact same thing for the exact same purpose and exposes the exact same risks, that there will be no criminal action against that person. There could be, as you've mentioned, administrative penalties. There are no administrative penalties, as I understand it, by the way, against the President. Correct?

Mr. COMEY. I don't think so. But I'm not a——

Mr. MULVANEY. I don't think there are either. I don't think you can take away the President's top security clearance. And I'm pretty sure you can't fire the President because we've tried. Not only would a staffer not have any criminal charges brought against him, but I suppose a summer intern could do the exact same thing under the theory that we're going to apply the law equally regardless of who the people are. My question to you is this: And it's not a legal question. I guess it's a commonsense, ordinary question that folks are asking me. From a national security standpoint, somebody who used to lecture on that, does that bother you?

Mr. COMEY. The mishandling of classified information bothers me no matter what circumstance it occurs in. Because it has national security implications.

Mr. MULVANEY. Does it bother you that the precedent that you are setting today may well lead to a circumstance where our top secret information continues to be exposed to our potential enemies?

Mr. COMEY. No, in this sense. The precedent that I'm setting today is my absolute best effort to treat people fairly without regard to who they are. If that continues to be the record of the FBI

and the Justice Department, that's what it should be. The rest of the implications in your question are beyond that. They're important, but they're not for the FBI to answer. We should aspire to be apolitical, facts and the law, treat Joe the same as Sally as Secretary so-and-so. That's my goal.

Mr. MULVANEY. If you had come to a different decision—by the way, I tend to agree with everything you've just said. If you had come to a different decision, do you think that would have a different precedential value that would keep our information more safe?

Mr. COMEY. If we decided to recommend criminal charges here?

Mr. MULVANEY. Yes, sir.

Mr. COMEY. I don't know. That's a good question. I don't know. I could argue it both ways. I guess I'm a lawyer, I can argue everything both ways. But I could argue that both ways.

Mr. MULVANEY. Thank you, Director Comey. Thank you, Mr. Chairman.

Chairman CHAFFETZ. Thank the gentleman. Now recognize the gentleman from Arizona, Mr. Gosar, for 5 minutes.

Mr. GOSAR. Thank you, Mr. Chairman. Thank you, Mr. Comey, for being here. My colleague alluded to Bryan Pagliano, the IT adviser. And were you made aware of the deal of immunity with him?

Mr. COMEY. I am aware.

Mr. GOSAR. Now that Attorney General Lynch has stated that there will be no charges, there's many that suspect that he failed to answer questions in his congressional deposition, that he had something to hide. Why did your investigators at the DOJ decide it was necessary to offer Mr. Pagliano immunity?

Mr. COMEY. As I said in response to the earlier question, I need to be more thoughtful about what I say about an immunity deal in public. It may be totally fine. I just don't want to screw up because we're doing this so quickly. In general, I can answer, because I've done it many times as a prosecutor. You make a grant of immunity in order to get information that you don't think you could get otherwise.

Mr. GOSAR. But you know that there may be something there in hindsight, right? You're looking ahead because of the pertinent information this person possesses.

Mr. COMEY. Right. You believe they have relevant information to the investigation.

Mr. GOSAR. So did the investigators draft an interview report known as a 302 with Mr. Pagliano?

Mr. COMEY. Yes.

Mr. GOSAR. Given the importance of this case, will you commit to voluntarily disclosing the 302s for review of Bryan Pagliano and other witnesses interviewed as part of your investigation?

Mr. COMEY. I'll commit to giving you everything I can possibly give you under the law, and to doing it as quickly as possible. That said, that means I got to go back and sort it out. For example, the 302 of Secretary Clinton is classified at the TS/SCI level. So we got to sort through all that. But we'll do it quickly.

Mr. GOSAR. Yeah. I know you've done this, because you've done this for Lois Lerner and other cases. So we would expect that.

Now, Director Comey, Hillary Clinton testified before Congress and told the American people multiple times that she never emailed any classified information to anyone on her private email servers. Your investigation revealed 110 of Clinton's emails, and 52 email chains confined classified information. Clinton told the American people, and I quote, "The laws and regulations in effect when I was Secretary of State allowed me to use my email for work. This is undisputed," end of quote. Your investigation revealed that that also wasn't true.

Clinton claimed she turned over all her work-related emails. Your investigation revealed that this wasn't also true. Clinton claimed that there was no security breaches and her private servers had numerous safeguards. Your investigation revealed eight email chains on Clinton's private servers containing top secret information. And that is was possible, quote, "hostile actors gained access to sensitive information." Further, multiple people she emailed with regularity were hacked by hostile actors and her private servers were less secure than a Gmail account, making a security breach all the more likely.

Director Comey, it's a Federal crime, as you know, to mishandle classified information in a grossly negligent way. And you stated Clinton and her colleagues were extremely careless. Clinton has publicly stated she was well aware of the classification requirements, yet she broke the law anyway. Multiple people have been prosecuted for less. And there is a growing trend of abuses in senior level employees. The only difference between her and others is her total resistance to acknowledge her irresponsible behavior that jeopardized our national security and the American people.

I think you should have recommended Clinton be prosecuted under section 793 or section 1024 of Title 18. If not, who? If not now, when? Your recommendation deprived the American people of the opportunity for justice in this matter. There shouldn't be double standards for the Clintons, and they shouldn't be above the law. With that, I'm going to yield the rest of my time to the gentleman from South Carolina, Mr. Gowdy.

Mr. GOWDY. Thank you, Dr. Gosar. Director Comey, I want to go back to the issue of intent for just a second. We can disagree on whether or not it's an element of the offense. Let's assume, for the sake of argument, that you're right and I'm wrong, and that it is an element of the offense. Secretary Clinton said that she was, quote, "Well aware of classification requirements." Those are her words, not mine and not yours. So if she were, quote, "well aware of classification requirements," how did that impact your analysis of her intent. Because I've heard you this morning describe her as being less than sophisticated. She disagrees with that.

Mr. COMEY. Well, I was talking about technical sophistication. The question is—I would hope everybody who works in the government is aware of classification requirements. The question then is if you mishandle classified information, when you did that thing, did you know you were doing something that was unlawful. That's the intent question.

Mr. GOWDY. Well, you and I are going to have to get together some other time and discuss all the people we prosecuted who were unaware that they were breaking the law. There are lots of really

dumb defendants out there who don't know that what they're doing is against the law. But let's go with what you say.

Mr. COMEY. I disagree. You may have prosecuted a lot of those folks. I did not prosecute a lot of those folks——

Mr. GOWDY. Well, I was a gutter prosecutor and you were a white collar prosecutor. Trust me. There are lots of people who don't know you can't kill other people. Let me ask you this: On the issue of intent, you say it was convenience. Okay? You're a really smart lawyer. If it were convenience, Director, she wouldn't have waited 2 years to return the documents. And she wouldn't have deleted them 4 years after they were created. So you can't really believe that her intent was convenience when she never turned them over until Congress started asking for them. Could you?

Mr. COMEY. You know, my focus, and I hope I made this clear.My focus was on what was the thinking around the classified information. I mean, it's relevant why the system was set up and the thinking there. But she didn't—I don't understand her to be saying—well, I think I've said it already. But that's my focus.

Mr. GOWDY. So I know I'm out of time, but it just strikes me you are reading a specific intent element into a gross negligence statute. Not even general intent.

Chairman CHAFFETZ. The gentleman's time——

Mr. GOWDY. A specific intent——

Chairman CHAFFETZ. The gentleman's time has expired.

Mr. COMEY. Sorry.

Chairman CHAFFETZ. The Director can answer.

Mr. COMEY. I enjoy talking with him. The question you got to ask is so why is it that the Department of Justice, since 1917, has not used that gross negligence statute but charging it once in an espionage case. And whether their decision was smart or not, that is the record of fairness. And so you have to decide, do I treat this person against that record? And if I do, is that a fair thing to do, even if you're not worried about the constitutionality of it? And my judgment is no reasonable prosecutor would do that. That would be celebrity hunting. That would be treating this person differently than John Doe.

Chairman CHAFFETZ. Director, I want to follow up on that. Why did you do what you did? You know, my interpretation of what the FBI is supposed to be doing is come to a determination of the facts. And then turn it over to a prosecutor. You were a prosecutor. But you're not a prosecutor now.

Mr. COMEY. Right.

Chairman CHAFFETZ. It is unprecedented that an FBI Director gave the type of press conference that he did and took a position that an unreasonable prosecutor would only take this case forward. Why did you do that?

Mr. COMEY. Yeah. It's a great question. The—everything I did would have been done privately in the normal course. We have great conversations between the FBI and prosecutors. We make recommendations. We argue back and forth. What I decided to do was offer transparency to the American people about the whys of that what I was going to do because I thought that was very, very important for their confidence in the system of justice. And within that, their confidence in the FBI. And I was very concerned if I

didn't show that transparency, that in that lack of transparency people could say, Gees. What's going on here? Something—you know, something seems squirrely here. And so I said I will do something unprecedented because I think this is an unprecedented situation.

Now, the next Director who is criminally investigating one of the two candidates for President may find him or herself bound by my precedent. Okay. So if that happens in the next 100 years they'll have to deal with what I did. So I decided it was worth doing.

Chairman CHAFFETZ. Mr. Cummings.

Mr. CUMMINGS. Mr. Director, I have just one question. You know, I've been sitting here listening to this. And I really—this is something that bothered me in the Lois Lerner case, and it bothers me in this case. And I'm just wondering your opinion. Mrs. Lawrence had talked about this, the chilling effect of your having to come here and justify your decisions. And I know that you've been really nice, and you just explained why you did what you did, and I'm glad you're doing it. But, you know, do you at all, and, I mean, taking off—I'm just talking about here you've got people making decisions and then being pulled here in the Congress to then say, okay, to be questioned about the decisions. At what point—or do you even think about it becoming a chilling effect? Because most people, you know, when their decision's made, don't get this kind of opportunity, as you well know. There are no statements. You know, they either get indicted or they're not.

So I noted you see this as a special case. And I wonder whether you agree with Mrs. Lawrence that we may be just going down a slippery slope. That's all I want to ask.

Mr. COMEY. And my honest answer is I don't think so. As I—when I talked to the chairman, I agreed to come because I think the American people care deeply about this. There's all kind of folks watching this at home or being told, Well, lots of other cases were prosecuted and she wasn't. I want them to know that's not true.And so I want to have this conversation. And I actually welcome the opportunity. Look, it's a pain. I've had to go to the bathroom for about an hour, but it is really——

Chairman CHAFFETZ. Don't worry. We're halfway done. So——

Mr. COMEY. It is really important to do. Because this is an unprecedented situation. Transparency is the absolute best thing for me and for democracy.

And I realize, Mr. Chairman, my folks told me I screwed up one fact that I should fix. I was misremembering. In the Petraeus case, we didn't find the notebooks in the attic, we found it in his desk. So I wanted to make sure I was fair to him about that.

But I really don't think so. I don't think it has a chilling effect. Again, if there's another presidential candidate being investigated by the FBI, maybe they'll be bound by this. Lord willing, it's not going to happen again. Certainly I have 2,619 days left in this job. I won't happen on my term. But if does, I won't be chilled.

Chairman CHAFFETZ. Thank the gentleman. If we need a humanitarian break, just give me the cue, but——

Mr. COMEY. No. I feel like we're almost done, though.

Chairman CHAFFETZ. We're on the right trajectory, yes.

But we would like to recognize the gentleman from Alabama, Mr. Palmer, for 5 minutes.

Mr. PALMER. Thank you, Mr. Chairman. Director Comey, your statement on Tuesday indicated that Secretary Clinton and her colleagues send and received emails marked classified on an unsecured private email server that may or may not have been hacked by a foreign power. Are you aware that teenage hackers hacked the personal email accounts of CIA Director John Brennan, the Director of U.S. National Intelligence, James Clapper, and FBI Deputy Director Mark Giuliano?

Mr. COMEY. I am intensely aware. They didn't hack in the way we normally think of it, but that they, by trickery, got access to their accounts.

Mr. PALMER. The point I want to make is that these were personal—commercially protected personal email accounts that contained no classified information. Yet Mrs. Clinton used her personal email, not a commercial account, on a server in her basement without even this basic protection, and transmitted classified information through that account. If teenagers in England were able to hack the personal email accounts of the Director of the CIA, the Director of U.S. National Intelligence, and the Deputy Director Of the FBI, does it concern you that sophisticated hackers or hackers working for foreign interests never attempted—I mean, does it seem reasonable that they never attempted, or were never successful in hacking Mrs. Clinton's personal email accounts or one of her devices?

Mr. COMEY. No. It concerns me a great deal. And that's why we spent so much time to see if we could figure out—see fingerprints of that.

Mr. PALMER. Well, you said in your statement regarding your recommendation not to prosecute, "To be clear, this is not to suggest that in similar circumstances, a person who engaged in this activity would face no consequences. To the contrary, these individuals are often subject to security or administrative sanctions, but that is not what we're deciding here." Do you stand by that?

Mr. COMEY. Yes.

Mr. PALMER. Okay. I thought you would. You also said you could not prove intent. I don't want to—I want to touch on a couple things here. One, a reasonable person would not have compromised classified information by keeping that information on inadequately secure private devices. In other words, such a person would be viewed as unreasonable and unsuitable for any position in our government that included any responsibility for handling and protecting classified information. Would you agree?

Mr. COMEY. I would agree it would be negligent. I can't prejudge a suitability determination, but it would definitely be stared at very hard.

Mr. PALMER. Well, let me tell you why I bring this up. I sat here next to Mr. Hurd, who served our country valiantly. Put his life on the line. And I don't know if you could sense the passion and intensity of his questions, because he knows people whose lives are on the line right now. And in regard to his questions, if someone, a U.S. intelligence agent had their mission compromised, or worse, had been killed or injured or captured because of the carelessness

of someone responsible for protecting classified information, would intent matter at that point?

Mr. COMEY. In deciding whether to prosecute the person? Of course. But—yeah. That's the answer. Of course it would. It would—the matter would be deadly serious. But the legal standards would be the same.

Mr. PALMER. Well, what we're dealing with in this hearing is not the lack of due diligence in handling routine government data or information, but the lack of due diligence by Secretary Clinton and her carelessness in handling classified information that could have compromised American national security, and as Mr. Hurd pointed out, the missions and personal safety of our intelligence agents. That troubles me greatly.

And I think the issue here—and I do respect you. I have spoken in your defense many times, at this point, to my detriment. But I do believe that your answers are honest and factual. But based on your answers regarding Mrs. Clinton's use of the email, and based on what we know, it seems to me that she is stunningly incompetent in her understanding of the basic technology of email, and stunningly incompetent in handling classified information. I mean, you should never associate the Secretary of State and classified information with the word "careless." It doesn't matter. I mean, we have to exercise the utmost due diligence. All of us in this committee do in handling this. You do in prosecuting cases. And I see that in what you're trying to do.

I just think we need to leave here with this understanding, that there's more to this story than we know. If a foreign hacker got into this, I can assure you that they know what was in those emails that were deleted. They read them all. They know what is in the emails that we never received.

Mr. Chairman, I yield back.

Chairman CHAFFETZ. I thank the gentleman. We'll now go to the gentleman from Wisconsin, Mr. Grothman, for 5 minutes.

Mr. GROTHMAN. Thank you. Thanks for coming on over to the Rayburn Building. As I understand it, your testimony today, is that you have not brought criminal charges against Hillary Clinton, in part, because you feel you can't prove guilt beyond a reasonable doubt, and in part, because she didn't understand the laws with regard to emails and servers and that sort of thing.

Question for you. When she erased these emails—or no, I digress for a second. You, however, did say that if somebody did this under you there would be consequences. If somebody did exactly what Mrs. Clinton did, but was one of your lieutenants or you think one of the lieutenants under the CIA or some other agency that deals with top secret documents, what would you do to those underlings?

Mr. COMEY. I would make sure that they were adjudicated through a security disciplinary proceeding to figure out what are all the circumstances and then what punishment, discipline is appropriate. That could range from being terminated, to being reprimanded, and then a whole spectrum in between, suspension, loss of clearance. It's a bunch of different options.

Mr. GROTHMAN. Okay. But tomorrow, say one of your top two or three lieutenants you find out that they've had this separate server out there and they're keeping secret documents, you know, flipping

them around. Do you think they should be fired? Not criminally charged, but fired?

Mr. COMEY. Yeah. I don't think it's appropriate to say. I think it should go—we have a very robust process. There ought to be a very intense suitability review of that person. Maybe there's something we're missing that would mitigate the punishment we would impose. But it would have to do through our system.

Mr. GROTHMAN. Okay. Next question. Just for the listening audience here, at first when I hear about erasing emails, I think it's like, you know, on my own phone where I might erase an auto insurance solicitation. The erasures here, however, were not just Mrs. Clinton pressing delete. Were they? There was a much greater effort made to make sure that these emails would never be recovered. Do you want to comment on what was done to erase the emails?

Mr. COMEY. I think what you're referring to is after her lawyers—her lawyers say, although I'm not able to verify this, there were 60,000 or so left at the end of 2014. They went through them in a way I described in my statement 2 days ago. And then they produced the ones that were work-related, and then they erased from their system the ones that were not work-related. That was done using technical tools basically to remove them from the servers to wipe them way.

Mr. GROTHMAN. Okay. So in other words, the effort was not just Mrs. Clinton or somebody went delete, delete, delete. They went above and beyond that so that your top technical efforts could not—technical experts could not get back at these emails, correct?

Mr. COMEY. Right. Not fully. We were able to by going——

Mr. GROTHMAN. You recovered a few.

Mr. COMEY. Yeah. We could go through the lawyers' laptops and see some traces, but not fully—not fully recover them.

Mr. GROTHMAN. Okay. Now, the information that I have, and you can correct me if I'm wrong, implies that these erasures were done in December of 2014 after the Benghazi scandal broke, after there were questions about the Clinton Foundation. Did you ever come across why she allowed these emails to sit out there, even for years after she stopped being Secretary of State but all of a sudden as these other scandals began to bubble up she felt, or her lawyers felt, that she had to erase them?

Mr. COMEY. Yeah. I think the way the process worked is she had emails that were just on her system. She actually had deleted some, I think, over time, as an ordinary user would. And then the State Department contacted her and other former Secretaries and said, We have a gap in our records. We need you to look and see if you have emails and give them back. She then tasked her lawyers to engage in this review process of that 60-some thousand and make that cut. And then was asked by her lawyers at the end, Do you want us to keep the personal emails? And she said, I have no use for them anymore. It's then that they issued the direction that the technical people delete them.

Mr. GROTHMAN. Do you think Mrs. Clinton knew that the technical people were erasing these emails so that even your top technical experts could recover them?

Mr. COMEY. Based on my sense now of her technical sophistication, I don't think so.

Mr. GROTHMAN. You don't think the lawyers told her that that's what they were doing, erasing all these emails that everybody on this committee wanted to look at?

Mr. COMEY. Yeah. And I'm sure we've asked this and——

Mr. GROTHMAN. What type of lawyer wouldn't tell their client they were doing that? But——

Mr. COMEY. I don't think—I think our evidence—our investigation is they did not, that they asked her, Do you want to keep them, and they said no, and they said, Wipe them away.

Mr. GROTHMAN. Okay. Now, as I understand it, the goal was just to erase personal emails, but you've recovered emails that wouldn't be considered personal emails at all.

Mr. COMEY. Correct.

Mr. GROTHMAN. Okay. I know that you didn't recover them, but based upon the emails that you recovered, presumably her lawyers or somebody was going well beyond personal emails, is it possible we'll never be able to recover emails that dealt with the Clinton Foundation or dealt with the Benghazi scandal? Is it possible, because of what her lawyers did, that they were erasing things that were incriminating, maybe involving items that you yourself were not particularly investigating, but that these have now been destroyed forever?

Mr. COMEY. I guess it's possible. As I said in my statement on Tuesday, we did not find evidence to indicate that they did the erasure to conceal things of any sort. But it's possible, as I said on Tuesday, that there are work-related emails that were in the batch that were deleted.

Mr. GROTHMAN. I'm sorry. When you go to this length to make sure you can never recover the emails that are erased, wouldn't you think the intent is to make sure nobody ever looks at them again? Why would—otherwise, would you just go——

Chairman CHAFFETZ. I thank the gentleman. We'll give the Director time if he wants to respond.

Mr. COMEY. Sure. You know, I guess it's a bit circular. You delete because you want to delete, but that—what I mean is we didn't find any evidence of evil intent, an intent to obstruct justice there.

Mr. GROTHMAN. You wouldn't have been able to——

Chairman CHAFFETZ. I thank——

Mr. GROTHMAN. —because you don't know what was deleted, but——

Chairman CHAFFETZ. I thank the gentleman.

We'll now recognize Mr. Russell of Oklahoma for 5 minutes.

Mr. RUSSELL. Thank you, Mr. Chairman.

Director Comey, thank you for your long service and your long suffering. I think we're toward the end of the line here.

I want to state for the record with regard to national security, I sleep a little easier at night knowing that you're at the helm of the FBI. Thank you for your dedicated service and your integrity.

Mr. COMEY. Thank you.

Mr. RUSSELL. You have stated in your statement and also multiple times here that there should be consequences for the mishandling of state secrets. If I held a top secret/SCI in the Bureau—

and I did hold one when I was in the United States Army, in a career of service, I've handled classified information here—but if I held that in the FBI and you discovered that I mishandled state secrets on a private server in my basement, would I be trusted by the Bureau to further handle top secret/SCI information?

Mr. COMEY. Maybe not. You would go immediately through a security process to review whether you should continue working for us, and if you do, what clearances you should retain.

Mr. RUSSELL. If I violated the handling of state secrets in the FBI, would you consider me the best suitable candidate for promotion and higher responsibility?

Mr. COMEY. It would be a serious concern, and we would stare at it very hard in a suitability review.

Mr. RUSSELL. Although you have recommended to the Department of Justice that no criminal charges be brought to bear, are you recommending to the Department of Justice that there be no consequences for the mishandling of state secrets?

Mr. COMEY. No. My recommendation was solely with respect to criminal charges.

Mr. RUSSELL. What would you recommend?

Mr. COMEY. I don't think it's for me to recommend.

Mr. RUSSELL. But you do—you've been very open and even stated why you felt that these were unique sets of circumstances that called for greater transparency. You do make recommendations routinely, as you've stated here today. We're talking top secret/SCI information that's been mishandled. You would take a dim view to that if I were an agent. What consequence—this is what the American people feel exasperated about. There seems to be no consequence.

So in a case like this, if it's not going to be criminal charges recommended, what are the American people to do to hold their officials accountable if maybe they shouldn't be trusted for further promotion and higher responsibility?

Mr. COMEY. And what I meant earlier is that's not a question that the American people should put to the FBI Director. I can answer about the things within my remit, but that—I understand the question, but it's not one for me to answer in my role.

Mr. RUSSELL. Well, I hope it's one that the American people answer in the future, because we do have a choice about those that would mishandle information. And while we're all fallible human beings and we all make mistakes, in a case like this, I mean, for decades of my service in the Army infantry and handling top secret/SCI information and then as a Member of Congress, I mean, we know those responsibilities.

Is it your view and others that have interviewed Mrs. Clinton that she would not have known what those responsibilities were?

Mr. COMEY. No, I think, in a way, you would expect she understood the importance of protecting classified information.

Mr. RUSSELL. Well, I would agree with that. And there has been a breach, and I think that the American people demand a consequence, that they demand an accountability. And I think it's important, to uphold the form of our republican government, that we have a consequence.

And with that, thank you for your appearance here today.

And I would like to yield the remainder of my time to Chairman Chaffetz.

Chairman CHAFFETZ. Thank you. I think, if you yield back, through mutual agreement, Mr. Cummings and I have agreed that I do have about a dozen or so quick follow-up questions. You've been most generous with your time, but I would like to get through these last bit.

Mr. COMEY. Okay.

Chairman CHAFFETZ. And, again, we'll do so with equal time.

How did the Department of Justice—or how did the FBI view the incident in which Hillary Clinton instructed Jake Sullivan to take the markings off of a document that was to be sent to her?

Mr. COMEY. Yeah. We looked at that pretty closely. There was some problem with their secure fax machine. And there's an email in which she says, in substance, take the headers off of it and send it as a nonpaper.

As we've dug into that more deeply, we've come to learn that, at least there's one view of it that is reasonable, that a nonpaper in State Department parlance means a document that contains things we could pass to another government. So essentially, take out anything that's classified and send it to me.

Now, it turned out that didn't happen, because we actually found that the classified fax was then sent, but that's our best understanding of what that was about.

Chairman CHAFFETZ. So this was a classified fax?

Mr. COMEY. Correct.

Chairman CHAFFETZ. So Hillary Clinton sends to Jake Sullivan—let me go back. Jake Sullivan says: They say they had issues sending secure fax. They're working on it. Hillary Clinton sends to Jake Sullivan: If they can't, turn into nonpaper with no identifying heading and send nonsecure.

Mr. COMEY. Yeah.

Chairman CHAFFETZ. So you're telling me it's a classified piece of information, she's taking off the header, and she's instructing them to send it in a nonsecure format.

Mr. COMEY. Right.

Chairman CHAFFETZ. Is that not intent?

Mr. COMEY. Well, that actually caught my attention when I first saw it. And what she explained to us in her interview was, and other witnesses did as well, is what she meant by that is make it into a nonclassified document, that's a what a nonpaper is in their world, and send it to us, because I just—I don't need the classified stuff, I just need the——

Chairman CHAFFETZ. Then why take off the heading? If it's going to be turned into a nonclassified document, why take off the heading?

Mr. COMEY. I assume because it would be nonclassified anymore, so you wouldn't have a classified header on it, I think is what she said during her interview.

Chairman CHAFFETZ. So she wanted to be technically correct? Is that what you're saying? This is your——

Mr. COMEY. No. I think what she said during the interview is: I was telling him, in essence, send me an unclassified document, take the header off, turn it into a nonpaper. Which is a term I'd

never heard before, but I'm told by people I credit that in diplomatic circles, that means something we could pass to another government.

Chairman CHAFFETZ. You are very generous in your accepting of that.

Let me ask you, Director, did any uncleared individuals receive any classified information over Hillary Clinton's server?

Mr. COMEY. Did any uncleared people receive classified information? I don't think any of the correspondents on the classified emails were uncleared people. These were all people with clearances working, doing State Department business on the unclass system.

Chairman CHAFFETZ. Did Mr. Pagliano have the requisite security clearance?

Mr. COMEY. As I sit here today, I can't remember. He was not a participant on the classified email exchanges, though.

Chairman CHAFFETZ. He was running the server. He set up the server.

Mr. COMEY. That's a different question. Well, I'm sorry. I misunderstood your question, then.

Yeah. There's no doubt that uncleared people had access to the server, because even after Pagliano, there were others who maintained the server who were private sector folks.

Chairman CHAFFETZ. So there are hundreds of classified documents on these servers. How many people without a security clearance had access to that server?

Mr. COMEY. I don't know the exact number as I sit here. It's probably more than 2, less than 10.

Chairman CHAFFETZ. And I appreciate your willingness to follow up with this.

Did Secretary Clinton's attorneys have the security clearances needed?

Mr. COMEY. They did not.

Chairman CHAFFETZ. Does that concern you?

Mr. COMEY. Oh, yeah. Sure.

Chairman CHAFFETZ. Is there any consequence to an attorney rifling through Secretary Clinton's, Hillary Clinton's emails without a security clearance?

Mr. COMEY. Well, not necessarily criminal consequences, but there's a great deal of concern about an uncleared person, not subject to the requirements we talked about in the read-in documents, potentially having access. That's why it's very, very important for us to recover everything we can back from attorneys.

Chairman CHAFFETZ. So what's the consequence? I mean, here Hillary Clinton gave direction to her attorneys without a security clearance to go through documents that were classified.

Mr. COMEY. I think that's what happened in fact. Whether that was the direction is a question I can't answer sitting here.

Chairman CHAFFETZ. You're parsing that one a little bit for me.

Mr. COMEY. No, no. You were just asking me. I don't—I don't know——

Chairman CHAFFETZ. What's the consequence? They don't work for the government. We can't fire them.

Mr. COMEY. Right.

Chairman CHAFFETZ. So is there no criminal prosecution of those attorneys? Should they lose their bar license? What's the consequence to them?

Mr. COMEY. Well, if they acted with criminal intent or acted with some mal-intent.

Chairman CHAFFETZ. What you're telling us is it doesn't matter if you have a security clearance or not, because I may be innocent enough, hey, I'm just an attorney, I like the Secretary, I'm trying to help Hillary Clinton, I'm not trying to give it to the Chinese or the Russians, I'm just trying to help her. So there's no intent? It doesn't matter if these people have security clearances?

Mr. COMEY. Of course it matters. That's why I said——

Chairman CHAFFETZ. But there's no consequence, Director. There's no consequence.

Mr. COMEY. Well, I don't know what consequence you'd have in mind. Very——

Chairman CHAFFETZ. Prosecute them.

Mr. COMEY. An attorney for receiving from his client information that ends up being classified?

Chairman CHAFFETZ. I asked you at the very beginning, does Hillary Clinton—is there a reasonable expectation that Hillary Clinton would send and receive hourly, if not daily, classified information? That's reasonable to think that the Secretary of State would get classified information at every moment. She is not the head of Fish and Wildlife.

So the idea that she would turn over her emails, her system, her server to, what it sounds like, up to 10 people without security clearances, and there's no consequence. So why not do it again?

Mr. COMEY. Well, that's a question I don't think you should put to me. You're asking—I'm talking about my criminal investigation.

Chairman CHAFFETZ. But how can that—there's no intent there? Does she not understand that these people don't have security clearances?

Mr. COMEY. Surely she understands at least some of them don't have security clearances.

Chairman CHAFFETZ. So she understands they don't have security clearances and it's reasonable to think she's going to be getting classified information. Is that not intent, to provide a noncleared person access to classified information?

Mr. COMEY. You're mixing it up, though. I don't think it's reasonable to assume—mixing me up, sorry, it's not your fault—that someone who is maintaining your server is reading your emails. In fact, I don't think that's the case here.

There's a separate thing, which is when she's engaging counsel to comply with the State Department's requests, are her lawyers then exposed to information that may be on there that's classified.

Chairman CHAFFETZ. Did they see any classified information? Did Hillary Clinton's attorneys, without security clearances, see classified information?

Mr. COMEY. As I sit here, I don't know the answer to that.

Chairman CHAFFETZ. It has to be yes, Director. You came across 110, and they said they went through all of them.

Mr. COMEY. Well, they didn't read them all, they just looked at headers.

Chairman CHAFFETZ. So their excuse is, "We saw the emails, but we didn't read them"?

Mr. COMEY. No, I think I said this in my statement on Tuesday, they sorted the emails by using headers and search terms to try and find work-related emails. We read them all.

Chairman CHAFFETZ. I know that you read them all. Do you think it's reasonable or unreasonable to think that her attorneys, under her direction, did or did not read those emails? Because there were—let me go back to this. Yes or no, were there or were there not classified emails that her, that Hillary Clinton's attorneys read?

Mr. COMEY. I don't know whether they read them at the time.

Chairman CHAFFETZ. Did Hillary Clinton give noncleared people access to classified information?

Mr. COMEY. Yes. Yes.

Chairman CHAFFETZ. What do you think her intent was?

Mr. COMEY. I think then it was to get good legal representation and to make the production to the State Department. I think it would be a very tall order in that circumstance, I don't see the evidence there to make a case that she was acting with criminal intent in her engagement with her lawyers.

Chairman CHAFFETZ. And I guess I read criminal intent as the idea that you allow somebody without a security clearance access to classified information. Everybody knows that, Director. Everybody knows that.

I've gone way past my time. Let me recognize Mr. Cummings for an equal amount of time.

Mr. CUMMINGS. Director, thank you for your patience.

I want to clear up some things. I want to make sure I understand exactly what you testified to on the issue of whether Secretary Clinton sent or received emails that were marked as classified.

On Tuesday, you stated, and I quote: "Only a very small number of the emails containing classified information bore markings"—and I emphasize, bore markings—"indicating the presence of classified information," end of quote. Republicans have pounced on this statement as evidence that Secretary Clinton lied. But today we learned some significant new facts, and I hope the press listens to this.

First, you clarified that you were talking about only 3 emails out of 30,000 your office reviewed. Is that right?

Mr. COMEY. Three, yes.

Mr. CUMMINGS. Three out of 30,000. Is that right?

Mr. COMEY. Yes. At least 30,000.

Mr. CUMMINGS. At least 30,000.

Second, you confirmed that these three emails were not properly marked as classified at the time based on Federal guidelines and manuals, they did not have a classification header, they did not list the original classifier, the agency, office of origin, reason for classification, or date for declassification. Instead, these emails included only a single, quote, "C," parenthesis, end parenthesis, and then end of quotation mark, for confidential on one paragraph lower down in the text. Is that right?

Mr. COMEY. Correct.

Mr. CUMMINGS. Third, you testified that based on these facts, it would have been a, quote, "reasonable inference" for Secretary Clinton to, quote, "immediately," end of quote, conclude that these emails were not, in fact, classified. So that was also critical new information.

But there's one more critical fact, that these emails were not in fact—and that is this, Director, and to the press—these emails were not, in fact, classified. The State Department explained to us yesterday, they reported that these emails are not classified and that including the little C on these emails was a result of a human error. The bottom line is that those little C's should not have been on those documents because they were not in fact classified.

When Representative Watson Coleman asked you a few minutes ago about this, you testified that you had not been informed. And I understand that, I'm not beating up on you, I promise you. But can you tell us why, Director Comey, because I want—you know, because the Republicans are pouncing and saying that the Secretary lied, and so I want to make sure that we're clear on this.

Can you tell us why, Director Comey, did you consult—and we're just curious—did you consult with the State Department about these 3 emails out of the more than 30,000, or did this just not come up? What happened there?

Mr. COMEY. Yeah. I'm not remembering for sure while I'm here. I'm highly confident we consulted with them and got their view on it. I don't know about what happened yesterday, maybe that their view has changed or they found things out that we didn't know. But I'm highly confident we consulted with them about it.

Mr. CUMMINGS. So this is totally different than what we understood yesterday. Today we learned that these emails were not in fact classified. They should not have been included—they should have not included those stray markings, they were not properly marked as classified, and the Director of the FBI believes it was reasonable for Secretary Clinton to assume that these documents were not classified.

Chairman, you raised a question about whether Secretary Clinton's attorneys had security clearances. It's my understanding that they did. We can double-check that, but that is my understanding. We'll double-check that.

Going on, let me move to the next topic. You explained on Tuesday that you were providing, quote, "an update on the FBI's investigation of Secretary Clinton's use of a personal email system during her time as Secretary of State." You explained that you received a referral on this matter from the inspector general of the intelligence community on July 6, 2016. Is that right.

Mr. COMEY. Yes.

Mr. CUMMINGS. Today, tens of thousands of Secretary Clinton's emails are publicly available on the State Department's Web site. And our staff have been reviewing the emails that were retroactively determined to include classified information.

Based on this review, it appears that these emails included more than 1,000 individuals who sent or received the information that is now redacted as classified. Let me make that clear. About 1,000 people sent or received the same information that was contained in

Secretary Clinton's emails and retroactively classified. Were you aware of that?

Mr. COMEY. No. The number doesn't surprise me, though.

Mr. CUMMINGS. Why not?

Mr. COMEY. Because this was—they were doing the business of the State Department on this email system. So I don't know how many thousands of people work at the State Department, but it doesn't surprise me there would be lots of people on these chains.

Mr. CUMMINGS. And would you agree that we need—that something needs to be done with regard to this classification stuff, because things are classified, then they're not classified, then they are retroactively classified. I mean, does that go into your consideration when looking at a case like this?

Mr. COMEY. Yeah. I don't pay much attention to the up-classified stuff, because we're focused on intent. So if someone classifies it later, it's impossible that you formed intent around that, because it wasn't classified at the time. I know that's a process. I wasn't familiar with it before this investigation, but I don't spend a lot of time focused on it in the course of a criminal investigation.

Mr. CUMMINGS. I understand. We also reviewed who these people are, and they include a host of very experienced career diplomats with many years of experience. So let me ask you this. When you received this referral from the inspector general about Secretary Clinton's emails, did you also receive any referrals for any of the other 1,000 people who sent and received those emails? Did you?

Mr. COMEY. No.

Mr. CUMMINGS. I understand——

Mr. COMEY. Well, I should stop there. Within the scope of our investigation was a group of people closer to the Secretary. We looked at their conduct. I forget what the number is, four or five of them. But then the hundreds of others who may have been on the chains were not the subjects of the investigation.

Mr. CUMMINGS. Okay. I think I have 30 more seconds.

I understand that Secretary Clinton is the only one running for President, but it does not make sense that she was singled out for a referral to the FBI. Do you agree with that?

Mr. COMEY. No, I don't—I don't think I agree with that.

Mr. CUMMINGS. Okay. So you—so you—let's go back to Colin Powell. Do you think you ought to look at his situation? Or Condoleezza Rice?

Mr. COMEY. Well, there's been no referral on them. I know only sort of at a superficial level their circumstances. This case strikes me as very different from those and not an inappropriate referral from the inspector general.

Mr. CUMMINGS. Very well.

Chairman CHAFFETZ. I thank the gentleman.

Who was Hillary Clinton emailing that was hacked?

Mr. COMEY. Yeah. I don't want to say in an open forum. We can get you that information, but I don't want to—again, I don't want to give any hostile adversaries insight into who—what we figured out.

Chairman CHAFFETZ. Fair enough.

Mr. COMEY. So I know the names.

Chairman CHAFFETZ. Understood.

Mr. COMEY. Yeah.

Chairman CHAFFETZ. Was there any evidence of Hillary Clinton attempting to avoid compliance with the Freedom of Information Act?

Mr. COMEY. That was not the subject of our criminal investigation, so I can't answer that sitting here.

Chairman CHAFFETZ. It's a violation of law, is it not?

Mr. COMEY. Yes. My understanding is there are civil statutes that apply to that. I don't know of——

Chairman CHAFFETZ. Let's put the boundaries on this a little bit, what you didn't look at. You didn't look at whether or not there was an intention or the reality of noncompliance with the Freedom of Information Act?

Mr. COMEY. Correct.

Chairman CHAFFETZ. You did not look at testimony that Hillary Clinton gave in the United States Congress, both the House and the Senate?

Mr. COMEY. To see whether it was perjurious in some respect?

Chairman CHAFFETZ. Yes.

Mr. COMEY. No, we did not.

Chairman CHAFFETZ. Did you review and look at those transcripts as to the intent of your recommendation?

Mr. COMEY. I'm sure my folks did. I did not.

Chairman CHAFFETZ. So—okay. And this is an important point, because I think those of us in Congress, knowing that you got a criminal referral from an inspector general, thought that you were also looking at whether or not Hillary Clinton had provided false testimony, which is a crime, to the Congress, but you didn't look at that.

Mr. COMEY. Correct. As I said, I'm confident my folks looked at the substance of the statements trying to understand the circumstances around the entire situation.

Chairman CHAFFETZ. Can you confirm that? I just want to make——

Mr. COMEY. Yeah, we'll confirm that. And also, again, maybe I'm missing this, but I don't think we got a referral from congressional committees, a perjury referral.

Chairman CHAFFETZ. No. It was the inspector general that initiated this.

Mr. COMEY. Yeah.

Chairman CHAFFETZ. Did the—the fact that Hillary Clinton refused to be interviewed by the inspector general, what did that say to you about intent?

Mr. COMEY. Not, at least for our criminal investigation, not particularly germane.

Chairman CHAFFETZ. Are you familiar—you're familiar—there's a Web site. I mean, lots of government agencies have Web sites. The State Department has a Web site, state.gov, and they have a YouTube site. Videos that are uploaded to a YouTube site, would those be considered Federal records?

Mr. COMEY. I don't know.

Chairman CHAFFETZ. So they're paid for by Federal dollars, they're maintained by Federal employees. Would that not be a Federal record?

Mr. COMEY. Yeah, I just don't know. I'm sure there's an expert who could answer that in 2 seconds, but I'm not that expert.

Chairman CHAFFETZ. Okay. We've kept you here a long time. I want to follow up on that.

Is the FBI still investigating Hillary Clinton's aides?

Mr. COMEY. No is the answer. The Department of Justice declined on all of those who were subjects communicating with her through that email system.

Chairman CHAFFETZ. What recommendations did you make about her aides?

Mr. COMEY. Same. Same. We didn't recommend that anybody be prosecuted on those facts.

Chairman CHAFFETZ. And if you can help us understand who precisely had been ruled out for prosecution, that would be——

Mr. COMEY. Sure.

Chairman CHAFFETZ. Did you look at the Clinton Foundation?

Mr. COMEY. I'm not going to comment on the existence or nonexistence of any other investigations.

Chairman CHAFFETZ. Was the Clinton Foundation tied into this investigation?

Mr. COMEY. I'm not going to answer that.

Chairman CHAFFETZ. The server that was set up in her home was originally set up by, you said, former President Bill Clinton.

Mr. COMEY. Correct.

Chairman CHAFFETZ. Do you know who paid for that?

Mr. COMEY. I don't, sitting here.

Chairman CHAFFETZ. Okay. I'll allow some equal time now for my colleague and friend, Mr. Cummings.

Mr. CUMMINGS. I'm going to yield 2 minutes to—of my 3.43—to Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Director. We're talking about hacking. And so on this committee we're very much interested in cybersecurity and we review a lot of the major hacks that are going on. So just recently, and I would say in the last 18 months, we've had a major hack, February of 2016, at the Department of Homeland Security and the FBI. We had a hacking group, the SITE Intelligence Group, reported that a group called Crackers With Attitude had hacked 9,000 employees' data from the Department of Homeland Security, including names, email addresses, locations, telephone numbers; also 20,000 FBI workers.

We had another hack—direct evidence, obviously, of those—another hack at OPM of 4.2 million current and former Federal Government employees. Their information had been stolen, including Social Security numbers, which were not redacted.

We had IRS in May 2015, millions—no, I'm sorry, 200,000 attempted and 100,000 were successful. We had—the State Department announced a breach of its computer systems after an infiltration forced the agency to temporarily shut down its classification system. We had the United States Postal Service, 800,000 postal employees, 2.9 million customers.

The White House, The Washington Post reported back in—this is back in 2014—that the White House computer was hacked. The National Oceanic and Atmospheric Administration. I'm on another committee for Financial Service. We had Verizon. UCLA Health

Systems, thousands and thousands and thousands of employees. Anthem HealthCare. Sony Pictures. Staples. Home Depot. JPMorgan. It gets into the millions. Community Health Systems. Target. TJX.

So all these we have direct evidence, millions and millions and millions of people, their accounts being hacked. Any direct evidence that Hillary Clinton's emails were hacked?

Mr. COMEY. No.

Mr. LYNCH. Okay. I have no further questions. I yield back.

Mr. CUMMINGS. Mr. Director, we are about at the end. I'm going to do a concluding statement and then I think the chairman will.

I want to, first of all, I want to go back to something that Mrs. Watson Coleman said a little earlier. As an African American man in this country, 66 years old, moving towards the twilight of my life, we cannot allow Black men to continue to be slaughtered.

This morning I woke up to my wife literally crying watching the tape of this guy, Alton Sterling, in Baton Rouge. And then she looked at the one, Philando Castile, near Minneapolis. And I hope you watched them. There's something wrong with this picture.

And don't get me wrong. I am all for, I've supported police, I am a lawyer, and I know how important police are, and I know there's so many great folks.

But, Mr. Director, if you do nothing else in your 2,000-plus days left, you have got to help us get ahold of this issue. It is so painful, I can't even begin to tell you.

And so I don't want—I've been fortunate in my life. I've been very fortunate that I have not been harmed by the police. But I've been stopped 50 million times.

Now, with regard to this hearing, I want to thank you again. You know, as I listened to you, you said something that I will never forget, and for some reason it gave me a chill. You said there are two things that are most important to me, two things. You said: My family and my reputation. My family and my reputation.

And I don't know whether your family's watching this, but I hope that they are as proud of you as I am, because you are the epitome of what a public servant is all about, sacrificing over and over and over again, trying to do the right thing, sometimes coming under ridicule, but yet still doing the right thing. And so I hope that they are proud of you.

The second thing is that no matter what has happened in this hearing, I hope that you know that your reputation is still intact.

And so I conclude by summarizing that I think some of our—of some of our key findings today. First, the Director testified that his entire team of 15 to 20 FBI investigators unanimously agreed on the recommendation not to prosecute Secretary Clinton.

Second, Director Comey made crystal clear that Republican claims and some of the talking heads' claims of bias are completely false. He testified that he would treat John Doe the same way he would treat Hillary Clinton, that he was very forceful on that point.

Third, on the claim that Secretary Clinton sent or received emails that were marked as classified, that claim has now been significantly undercut. Those documents were not classified and those markings were not proper.

Finally, Republicans have repeatedly cried foul about a double standard when it comes to Secretary Clinton's emails, but Director Comey testified that the real double standard would have been to prosecute her with this completely inadequate evidence.

Again, Director, I thank you, but I thank somebody else. I thank—and having practiced law for many years and having dealt with the FBI on many cases, I want to thank the people who work with you. Because it's not just—it's not just—this is not just about you.

Mr. COMEY. No.

Mr. CUMMINGS. This is not just about Secretary Clinton. When we are addressing you, there are a whole cadre of people who give their blood, their sweat, and their tears to protect us as Americans. And I just want to thank them, because sometimes I think they are forgotten, unseen, unnoticed, unappreciated, and unapplauded. But today I applaud them and I thank you.

Thank you very much, and I yield back.

Chairman CHAFFETZ. And I thank the gentleman.

And I concur with the idea that every FBI agent I have ever met has just been above reproach, and they make us proud. And they work hard, they put their lives on the line, they serve overseas, they serve domestically. Can't thank them enough for what they do, and I hope that is part of the message that we carry back.

I cannot thank you personally enough, you on a personal level, for your accessibility, your ability to get on the phone with me the same day that you make your announcement, and then in rapid fire when I said to you, "What day is best, we're going to have to do this, so which day is best for you?" and you said Thursday, and here we are and doing it. I can't thank you enough.

I wish all of the government employees would have that attitude and approach, I really do, and I can't thank you enough. I look forward to working with you and your staff as we move forward in getting this documentation, things that you can't share publicly, and others.

It is the intention of the committee to—I had told Mr. Cummings here that we would come back after votes. Votes have been pushed back now a bit. So what I'd like to do is to go into recess for 5 minutes and then we will start with our second panel.

The committee stands in recess till 5 minutes from now.

Thank you again, Director Comey.

[Recess.]

Chairman CHAFFETZ. The Oversight and Government Reform Committee will reconvene and we will now recognize our second panel of witnesses.

I'm pleased to welcome the Honorable Steve Linick, inspector general of the United States Department of State.

Mr. Linick, it is our understanding that you are accompanied by Ms. Jennifer Costello, assistant inspector general for the Office of Evaluations and Special Projects, whose expertise may be needed during questioning. So we will also ask that she be sworn in during this time too.

We also welcome the Honorable Charles McCullough, III, inspector general of the intelligence community at the Office of the Director of National Intelligence.

We thank you for being here. We thank you for your patience. It has been a long afternoon. But you've done some exceptionally significant and important work, and we want to hear it and understand it and digest it and ask questions about it.

So pursuant to committee rules, all witnesses are to be sworn before they testify. And as I said, we will also swear in Ms. Costello. If you will please rise and raise your right hands.

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.

Let the record reflect that all three of the witnesses did answer in the affirmative.

Inspector General Linick and Inspector General McCullough, you are both welcome to make oral remarks. We'll be very generous with the time. And your entire written statement and extraneous materials will be entered into the record as you so wish.

But let's now go to Mr. Linick and recognize him.

STATEMENTS OF MR. STEVE LINICK, MS. JENNIFER COSTELLO, AND MR. I. CHARLES MCCULLOUGH, III.

Mr. LINICK. Thank you, Chairman Chaffetz. I'm pleased to be here to testify about our report on records management and cybersecurity at the Department of State. I have no opening statements, and therefore am prepared to answer any questions the committee has about the report and any other matters.

Chairman CHAFFETZ. Thank you, Mr. Linick.

Mr. McCullough, we'll now recognize you for as much time as you'd like.

Mr. MCCULLOUGH. Thank you, Chairman Chaffetz. It's——

Chairman CHAFFETZ. If you could both bring those microphones, and it's a little uncomfortable, but bring them right up there. There we go. Thank you.

Mr. MCCULLOUGH. It's a pleasure to be here, and I'm here—I don't have an opening statement either, so in the interests of time, I'm here to answer your questions, and I'm very happy to be here for you.

Chairman CHAFFETZ. Thank you.

I'll now recognize myself first.

I need you to summarize your findings as to what is happening and not happening with classified information. And, Mr. McCullough, my understanding is a referral was given that kicked off this whole process. Why did you make that referral? What was it that you were seeing that you think warranted an investigation?

Mr. MCCULLOUGH. We were—Chairman, we were assisting—I had been asked to assist IG Linick in a review of classification issues and other issues at the State Department. He requested my office to help because of our expertise with classification matters. And during our assistance with his particular review he was doing, we reviewed 300 documents that had already been released in the FOIA process for former Secretary Clinton's emails.

We saw some classified material, one classified document that had been released that wasn't properly redacted. My inspectors noticed a second document that was classified but was properly re-

dacted. So we knew that in this sample of 300 that had already been published, that there were classified documents in this set of emails.

So also during our review, looking at essentially the internal controls of the email processing at the State Department, again, the role that we played was to look at the controls to determine whether or not the controls were sufficient to spot intelligence community equities in classified information.

So we had talked to some people there and were hearing from—we heard from senior management officials that there were—they had perused the documents, and they were under the impression, one in particular, that there was a good deal of classified information in these documents yet to be processed, these 30,000 documents.

They also commented to us that they didn't feel as though they had the personnel there, that there was a deficiency with the personnel in terms of having the appropriate number of people, appropriately cleared people, people with the appropriate expertise to review these documents.

So I was looking at that. So we have—we have documents that are already published, already processed through a FOIA. One was not properly redacted and it was classified. And I'm being told by the State Department information management people that they have concerns that there's a good deal of classified information in this set of documents.

And on top of that, I was advised by Mr. Linick's office that this whole set of emails was present on a thumb drive in Secretary Clinton's attorney's office. We knew nothing about the clearances for counsel or for the law firm. And I was also advised that this set of documents previously resided on a private server, which at that point in time was with a private company.

So as an IG, I was facing a situation where I had classified information, it appeared to me, outside the care, custody, and control of the U.S. Government.

In the intelligence community what you do when that happens is you tell the security component of the agency who owns that information. In this case, I told the agencies who owned the information, I also told the ODNI's security component, the NCSC, and I was advised to go directly to the FBI with a referral with respect to my referral to them.

Chairman CHAFFETZ. So these emails, which are supposedly all of Hillary Clinton's emails, they were sitting in a secure or nonsecure facility at her attorney's office?

Mr. MCCULLOUGH. I don't know anything about the security of the facility at the attorney's office. I think—I had heard at that point in time that there was a safe there, and I think that it was represented——

Chairman CHAFFETZ. But it's not a cleared—not cleared by the United States Government?

Mr. MCCULLOUGH. Not to my knowledge.

Chairman CHAFFETZ. Mr. Linick, what was your finding here?

Mr. LINICK. Well, we were not involved in any of the classification determinations. I mean, our role in this was to look at the

FOIA process. We were asked jointly to look at the FOIA process, whether improvements could be made.

And we made a number of recommendations to the Department to make sure that classified information wasn't inadvertently released in the context of doing the review for FOIA. That was our role in this.

Chairman CHAFFETZ. Hillary Clinton had this convenient email arrangement with herself. Have you ever seen anything like that? Were there people that expressed concerns about that? And what happened when these people expressed concerns?

Mr. LINICK. Well, as we reported in our evaluation report, we did interview a couple of individuals who were in the Office of the Secretary, the computer division, SES/IRM, who said that they approached the then-director of that particular office and expressed concerns both about the server and about whether or not her emails were being properly preserved under the Federal Records Act.

And that individual, the director of SES/IRM, informed those individuals that it had been approved by Legal and not to mention it again.

Chairman CHAFFETZ. What does that mean, "not mention it again"? How did you read that?

Mr. LINICK. You know, I can only report—I can only report what the witnesses told us. We were not able to interview the individual——

Chairman CHAFFETZ. Why not?

Mr. LINICK. I'm sorry, I didn't hear the question.

Chairman CHAFFETZ. Why not? Why didn't you interview him?

Mr. LINICK. Well, we asked to interview him, but he declined to interview with us. So we were not able to get the benefit of his perspective on it. So I'm really unable to interpret what that means, other than just present the facts.

Chairman CHAFFETZ. And were you able to interview Hillary Clinton?

Mr. LINICK. We were not.

Chairman CHAFFETZ. Why not?

Mr. LINICK. Well, we asked to interview Secretary Clinton. We interviewed all of the Secretaries. We looked at five Secretaries of State, going back to Madeleine Albright. And, through counsel, she declined to meet with us.

Chairman CHAFFETZ. Did she indicate a reason why she would refuse to meet with the inspector general?

Mr. LINICK. Her counsel informed our staff that she had—that all of the information about the email was on the FAQ sheet published by her campaign.

Chairman CHAFFETZ. So they directed you to the campaign?

Mr. LINICK. To the FAQ sheet.

Chairman CHAFFETZ. At the campaign?

Mr. LINICK. On the Web site, yes.

Chairman CHAFFETZ. The campaign Web site?

Mr. LINICK. I will have to check that. I'm not sure exactly what Web site it was.

Chairman CHAFFETZ. Well, it's an important point, so please check that.

Mr. LINICK. Okay.

Chairman CHAFFETZ. I have gone over my time.

Let me recognize the gentleman from Massachusetts for 7 minutes in equal time, Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman.

The chairman asked—I want to follow up on that question. The chairman asked, have you ever seen anything like this before? And I think, in the fullness of your response, I would say you have.

As you indicated, you investigated, you reviewed the records of five Secretaries of State. And here is part of your report. It says here that your report identified more than 90 department employees under Secretary Powell and Secretary Rice who used personal email accounts for official business.

And I will quote your report. The report says exactly this. It says, "OIG reviewed the Department email accounts of senior department employees who served on the immediate staffs of Secretary Powell and Secretary Rice between 2001 and 2008. Within these accounts, OIG identified more than 90 department employees who periodically used personal email accounts to conduct official business, though OIG could not quantity the frequency of this use."

So I know this is sort of the second part of this hearing, but that would have been good information to have at the first one.

Also, Inspector General Linick, in May, you issued a report on the management of email records by the Secretaries of State, and your review found that Secretary Powell used a personal email account for official business.

As a matter of fact, in his book, he lays it out. I'm not going to repeat it again, but there's an interesting section here where, you know, he'd get a little frustrated with the State Department system, and he installed a laptop computer on a private line and just started emailing folks. And, again, Secretary Powell has later admitted to deleting all of his emails.

So we got 55,000 emails from Hillary Clinton. How many did we get from Secretary Powell?

Mr. LINICK. I'm not aware of any from Secretary Powell.

Mr. LYNCH. That would be zero.

Mr. LINICK. I believe that's the case.

Mr. LYNCH. Yeah. Okay.

Mr. LINICK. Yes, he did use an aol.com account to transmit email.

Mr. LYNCH. Now, this is the—now, get this. So Secretary Powell is testifying before the United Nations Security Council, telling them they got—that there are weapons of mass destruction and we need to go into Iraq. At that time, he is using a personal email system. And he has deleted everything that he had in that file, so we have nothing. And Hillary Clinton is getting investigated.

You know, it just—let me ask you, have you followed up with that and tried to get any information from Secretary Powell?

Mr. LINICK. Well, we haven't. The Department, though, has asked for information from Secretary Powell, and I don't believe they have received it yet. But you will have to ask the Department about that.

Mr. LYNCH. When did they—do you have any knowledge of when they asked?

Mr. LINICK. You know, I'd have to—it's in our report, the exact date. I don't have it off the top of my head.

Mr. LYNCH. I do. October 21, 2015.

Mr. LINICK. Perfect.

Mr. LYNCH. The State Department sent Secretary Powell a letter requesting that he contact his email provider, AOL, to determine whether any of his emails could still be retrieved. Is that right?

Mr. LINICK. That's right.

Mr. LYNCH. Okay.

And, in your report, you note that, as of May 2016, the Department has not received a response from Secretary Powell or his representative. Is that still correct?

Mr. LINICK. To the best of my knowledge, that's correct.

Mr. LYNCH. Okay. So we got nothing there. What are we doing about that?

Mr. LINICK. I mean, it's up to the Department to get that information pursuant to NARA regulations. They are on the hook to recover records that are lost from the State Department, and, through that letter, they're trying to fulfill that obligation.

Mr. LYNCH. So there's a huge gap.

We got the goose egg from Condoleezza Rice too. She gave us nothing, in terms of emails. So we have 8 years of silence from the Secretaries of State.

Mr. LINICK. Well, the difference with—we don't—Condoleezza Rice, we believe, wasn't using email to conduct State Department business.

Mr. LYNCH. But her staff were.

Mr. LINICK. Yes.

Mr. LYNCH. She's got a bunch of staffers——

Mr. LINICK. Yes.

Mr. LYNCH. And she served in 2001. This was not 1901. So there were emails. She acts like there were no emails in 2001. There were. We just don't have any, not from her.

Mr. LINICK. We did find that her staff——

Mr. LYNCH. I just think there's a double standard going on here. People have talked about a double standard all day. How come these folks gave us the goose egg? We got zero, We got silence for 8 years from our Secretaries of State, and no one is going after them. They don't get subpoenaed up here. I haven't seen them at these hearings.

Chairman CHAFFETZ. Will the gentleman yield?

Mr. LYNCH. The gentleman will yield, yeah, sure.

Chairman CHAFFETZ. The inspector general was able to interview them and talked to them, and they did look at them.

Mr. LYNCH. And they got nothing. They got the—they got the, you know, "Talk to the hand." That's what they got. They got zero.

Chairman CHAFFETZ. Would the gentleman yield?

No, he said that she did not use email.

Mr. LYNCH. They just told—but they never subpoenaed or anything.

Chairman CHAFFETZ. But if you ask Mr. Linick what happened with her aides, I'd like him to answer that question.

Mr. LINICK. So we did talk to Secretaries Rice and Powell and all the other Secretaries. Secretary Rice told us that she didn't use email——

Mr. LYNCH. And you just take that at face value?

Mr. LINICK. Well, we actually tested that. We looked at archives. We didn't find—I mean, we tried to corroborate that. We did not find any evidence that she used——

Mr. LYNCH. What about her immediate staff?

Mr. LINICK. Well, we did conclude that her immediate staff used email to conduct official business.

Mr. LYNCH. Yeah.

Mr. LINICK. So, we did.

Mr. LYNCH. Okay. So, you know, that's interesting. Do we have their emails?

Mr. LINICK. I'd have to check on that. I do know that we, in the course of our work, we bumped into a number of emails that—classified emails that staff sent to personal accounts. And we did write up a memo describing that and providing that to the Department and asking the Department to take appropriate action and make sure any of the archives—you know, the archives didn't have classified email in them.

So we did take—same thing with Secretary Powell when we found the two classified emails that were sent to him.

Mr. LYNCH. Okay.

Mr. McCullough, what do you think about this?

Mr. MCCULLOUGH. With regard to?

Mr. LYNCH. The lack of response by Secretary Powell, 4 years, and then getting zero from Condoleezza Rice as well.

Mr. MCCULLOUGH. My office's role here was extraordinarily narrow. When we came in, IG Linick's office was doing this review. It was limited to the past five Secretaries. We don't have the resources. The tasking, I believe, from Congress——

Mr. LYNCH. We just spent $7 million investigating Secretary Clinton. We don't have the resources to, you know, to——

Mr. MCCULLOUGH. I'm talking about my office. The tasking from Congress was to determine whether classified information—one of the taskings that I believe Steve received was to determine whether classified information had traversed nongovernmental systems at the State Department. His office had scoped that down to the five past Secretaries.

When I came in, we thought it was the easiest thing and, quite frankly, we thought it would be the fastest thing to do, since they already had 30,000 documents they were processing for a FOIA, to determine whether or not they had sufficient internal controls in place to spot, identify classified information, identify classified equities.

Mr. LYNCH. Can we subpoena AOL and just say, you know, this was a private account that the Secretary of State during a very important part of our country's history—and we want those emails, go get them, rather than just waiting for—and, look, I have great admiration for Secretary Powell. I do. But, still, that's information, in fairness, that we should have.

Mr. MCCULLOUGH. I'm trying to explain that our—my office's role and my role in the review was narrowly tailored to determine

whether or not classified information—we didn't have—my office doesn't have the resources to determine, with the thousands of employees at the State Department, who was trafficking in classified information on personal systems and who was not.

He already had 30,000 documents right there that were going over that——

Mr. LYNCH. You mean Secretary Clinton's documents?

Mr. MCCULLOUGH. That's correct—that were going through a FOIA process. So, from an IG perspective—and it was more efficient for us—we thought we would look at the processes being used by the FOIA managers at the State Department. And we made recommendations to them that——

Mr. LYNCH. Did you recommend that we go after Secretary Powell?

Mr. MCCULLOUGH. No. The recommendations we made were—first of all, they asked us, can you please give us—these are the people who were actually doing the review. They felt as though they didn't have sufficient expertise there to spot intelligence equities. And so we recommended that they include intelligence people for this type of FOIA review, this particular FOIA review.

We also recommended that they get on—they were doing this review on a Secret-level system, a SIPRNet-level system, and because we had been told by some of the State officials that they thought there was a good deal of classified information in the emails, we recommended that they perform this processing on a Top Secret/SCI-level system, a JWICS-level system.

Mr. LYNCH. But that went all over—that went completely around Secretary Powell's information, because he was giving us nothing. They had only Secretary Clinton's stuff, so they—this review of five Secretaries of State was heavily focused on Secretary Clinton because of the complete absence of any other information.

Mr. MCCULLOUGH. I would have to defer to IG Linick with respect to any of the other Secretaries in terms of the availability of emails on personal systems.

Mr. LYNCH. Okay.

I'll yield back. I'm way over time. Thank you, Mr. Chairman.

Chairman CHAFFETZ. Thank you.

I now recognize the gentleman from South Carolina, Mr. Gowdy, for 5 minutes.

Mr. GOWDY. Thank you, Mr. Chairman.

Inspector General Linick, did you desire to interview Secretary Clinton as part of your investigation?

Mr. LINICK. Yes, we did.

Mr. GOWDY. And were you able to do so?

Mr. LINICK. No, we were not.

Mr. GOWDY. And how was it communicated to you that you were not going to be able to do so?

Mr. LINICK. Through her counsel. David Kendall had sent a letter to one of the team leaders on the report.

Mr. GOWDY. Is that letter available for Congress to inspect?

Mr. LINICK. You know, I'll go back and check, but I'll have to get back to you on that. I mean, it certainly exists. Whether if it's legal to provide it to you, sure.

Mr. GOWDY. Well, let's do this then. Let's fast-forward and let's assume that you were able to interview her. Why did you seek to interview her? And what questions, specifically, would you have asked?

Mr. LINICK. Well, we were—the focus of our report was not about classified information. The focus of our report was how the Department over the past 20 years addressed records preservation and cybersecurity.

And, you know, we were looking at—we were looking at whether or not—there was a rule the Department issued in 2005 requiring that employees use departmental systems. She used a nondepartmental system, her server, to conduct official government business. And we wanted to ask her questions about that—whether she had approval, who approved it, and so forth.

We also—so we wanted to get her perspective on those issues, among others.

Mr. GOWDY. So let me see if I have this right. The inspector general for the State Department wanted to interview a former Secretary of State.

Mr. LINICK. That's correct.

Mr. GOWDY. And that request was declined.

Mr. LINICK. Yes.

Mr. GOWDY. Well, at first blush, it sounds like your question was a reasonable one. You want to make sure that the information is safeguarded and protected and archived consistent with law. So I wonder why you weren't able to interview her. Were you given a reason?

Mr. LINICK. Just the reason that I articulated before. Other than that, I would be speculating.

Mr. GOWDY. What other questions—and if you need to ask any of the wonderful folks with you—what other questions would you have sought to ask the former Secretary of State?

Mr. LINICK. Well, we also looked at records preservation. And the rules required a certain—that she print and file her emails and that she, you know, make sure that they're part of the agency recordkeeping system. We wanted—we would've asked her about that.

We would've asked her about some of the attempts to hack her system, at least as expressed by her—some of her staff, which we have identified in our report. We probably would've asked her about that.

So those are the kinds of things, her state of mind and so forth.

Mr. GOWDY. I don't think you were in the room for Director Comey's testimony, and I don't know whether or not you had access to it in the back.

Are you familiar with his testimony that convenience was one of the intentions the former Secretary had in having this unusual email arrangement with herself?

Mr. LINICK. No, I don't recall that. But I did watch parts of the testimony.

Mr. GOWDY. All right. He did cite convenience as one of the factors.

Do you know when her emails were returned to the State Department?

Mr. LINICK. They were returned 21 months after she left the Department.

Mr. GOWDY. What was going on the second month after she left that made it inconvenient to return them then?

Mr. LINICK. I wouldn't be able to comment on that.

Mr. GOWDY. How about the fourth month?

Mr. LINICK. Again, I just don't know.

Mr. GOWDY. How about the 1-year anniversary?

Mr. LINICK. Same answer.

Mr. GOWDY. Do you know what possibly could have inspired her to begin searching for those records?

Mr. LINICK. Well, she did receive a request from the Department to return records in accordance with their obligations under the Federal Records Act, and there are regulations.

Mr. GOWDY. But that obligation didn't manifest itself 21 months later. That obligation was present the day she left office.

Mr. LINICK. And one of our findings was, along with Secretary Powell, that both of them failed to surrender their records, their personal records containing government business when they left the Department, thus depriving the Department of having those records as part of the agency recordkeeping system.

Mr. GOWDY. And I assume you probably would've asked former Secretary had you had an opportunity to do so why it took 21 months to return public records.

And just so there's no—I mean, nobody likes Congress. I get that. We're not sympathetic. But there are FOIA requests that would've been received by the State Department during that time period, right?

Mr. LINICK. Possibly.

Mr. GOWDY. How would those FOIA requests have been responded to and complied with if they didn't even have the records?

Mr. LINICK. Well, sir, as we identified in our previous report on FOIA, it would've been difficult if the records are not part of the agency recordkeeping system to respond to FOIA.

Mr. GOWDY. I'm out of time, but I know the chairman will give me one more question since he's given a lot more than one more question to other folks.

I want you to assume an absurd hypothetical, that the Secretary of State has exclusive use of personal email and that she is corresponding with someone who also uses personal email. Are you with me?

Mr. LINICK. I'm with you.

Mr. GOWDY. How in the world is the State Department ever going to capture that email?

Mr. LINICK. It would be—and this is something we addressed in our FOIA report. It would be—it would be difficult because——

Mr. GOWDY. It'd be a challenge, wouldn't it?

Mr. LINICK. It would, because only records under the agency's control are subject to FOIA. So, in other words, the Department wouldn't be able to reach in, necessarily, to a private account. So it——

Mr. GOWDY. Well, you wouldn't even know about it, would you? If it's personal-to-personal, how would you know about it?

Mr. LINICK. You wouldn't know about it.

Mr. GOWDY. All right.

Well, I'm barely out of time. I thank the chairman.

Chairman CHAFFETZ. I thank the gentleman.

I will now recognize Mr. Cummings for 7 minutes.

Mr. CUMMINGS. Inspector General Linick and Inspector General McCullough, on March 9, 2016, seven committee ranking members of the United States Congress from the House and the Senate sent you a letter. I signed this letter, along with the ranking members of both the Senate and the House Intelligence Committees, the House Foreign Affairs Committee, the Senate Foreign Relations Committee, and the House Armed Services Committee, and the Senate Judiciary Committee.

Are you both familiar with the letter?

Mr. MCCULLOUGH. Yes, sir.

Mr. CUMMINGS. Are you, Mr. Linick?

Mr. LINICK. Yes, I am.

Mr. CUMMINGS. The letter asked you 13 questions. To date, neither of you has answered one single one of those questions. Why is that?

Mr. MCCULLOUGH. We have responded to the letter, and, in the response to the letter, that has led to several individual Member meetings, and we have offered Member meetings to all the Members who had concerns so that we could address them. And the Member meetings I have had directly addressed those questions. And so, again, I would re-extend that offer to you, Ranking Member Cummings.

Mr. CUMMINGS. Well, let me, let me, let me—on May 16, 2016, Mr. McCullough, you provided a response that was written in such a way that it was overclassified, at the Secret level.

Was it really necessary to classify your response that way? And why did you write a response that could be publicly—why didn't you just do one that could be publicly available?

Mr. MCCULLOUGH. It wasn't overclassified, Ranking Member Cummings. There was a lot of concern by Members who did not have access to certain of the emails. And I wanted to make sure that anyone receiving and reading that letter would understand that, if I was coming to brief, I wouldn't be able to brief on the one set of emails that are ORCON with one of the agencies.

Mr. CUMMINGS. All right.

Now, Mr. Linick, you responded on May 25, 2016. You had a short letter too.

Mr. LINICK. I did.

Mr. CUMMINGS. Wow. Like Mr. McCullough's letter, it failed to answer any of the specific questions from the ranking members.

You both received followup letters, again posing the same 13 questions. Neither of you responded to those letters.

And so I guess your answer is the same. Did you all talk to each other about how you all were going to coordinate and not respond to Members of Congress, ranking members at that?

Mr. LINICK. Well, the underlying issue in those letters was accusing our office of bias. And I think we responded in our letter that we conduct ourselves with the highest integrity, and I could vouch for my staff. We are obviously focused on where the facts lead,

we're independent, and we've worked very competently on our reports.

And I think our recent report, the evaluation on records preservation and cybersecurity, speaks for itself. No one has contested or challenged our findings or recommendations. And, in fact, the State Department has accepted the findings and recommendations.

And we explained that in the letter. We explained that we have had bipartisan contacts with the Congress. So——

Mr. CUMMINGS. Well, let me ask you some questions, because I'm going to run out of time.

Other than through official press statements, have you or anyone in your office, with the knowledge of the office, provided any information regarding the review of Secretary of State Clinton's emails to the news media?

Mr. LINICK. Well, we, like every other IG office, have a press office. And when we get press inquiries, we respond to them. We respond to them appropriately. We would never——

Mr. CUMMINGS. So the answer is yes.

Mr. LINICK. —we would never release—well, of course, just like every other IG office. If someone asks about our findings or is misinterpreting, you know, what we're doing, we'll respond to it.

But we have never released any confidential information or have been inappropriate.

Mr. CUMMINGS. Okay.

Have you or your offices given any information, written or oral, regarding the review to the Republican congressional Members or staff that your offices have not made available simultaneously to the Democratic congressional Members or staff?

Mr. LINICK. No. We are bipartisan, always.

Mr. MCCULLOUGH. We've been bipartisan, bicameral——

Mr. LINICK. Absolutely.

Mr. MCCULLOUGH. —at every step with our congressional notifications.

I believe there was a blip on one occasion. It was unintentional, where one side—and I think there was a briefing where the Members or the staffers had requested the other side not be there. We briefed one side, and then offered the exact same briefing to the other.

But, otherwise, we've made every attempt to be bipartisan and bicameral with all of our reporting and all of our briefings. We've done a number of briefings.

Mr. CUMMINGS. The letter says, and I quote—this is the same letter that we sent you. It says, "Last week, a potential whistleblower in the office of the State Department inspector general publicly accused the office of having an anti-Clinton bias."

What are the policies and procedures for employees of your offices to report concerns regarding ongoing investigations, including concerns of bias within your offices?

Mr. Linick?

Mr. LINICK. Well we're—if there are any issues about conflicts of interest, we would—I mean, as a matter of—as a matter of course, we would take action if there was an issue.

But let me just say that I've been—prior to my having become an IG for the last 6 years, I was a career prosecutor for 16 years.

And the principles of integrity and honesty are of utmost importance to me and to my work.

So, you know, these allegations are entirely unfounded. Our work speaks for itself. And we will follow the facts wherever they lead, and partisan politics has no bearing on what we're doing.

Mr. CUMMINGS. Well, this committee has a reputation for going after people who interfere with whistleblowers. And that's why I have to ask you. This was a whistleblower who——

Mr. LINICK. An anonymous whistleblower.

Mr. CUMMINGS. Well, he publicly accused the office.

Mr. LINICK. It was anonymous. We have no idea who or what. But these are unfounded allegations. This was before our report was issued. I think our report speaks for itself.

Mr. CUMMINGS. Let me ask you this—did you have a response to that, Mr. McCullough?

Mr. MCCULLOUGH. I would echo——

Mr. CUMMINGS. And do it briefly, because I've got one more question.

Mr. MCCULLOUGH. I would echo IG Linick's response.

Mr. CUMMINGS. Tell me something. What happens when you all disagree on things that should be classified?

One of the things that bothers me about this whole thing is this retroactive classification. I mean, people on this committee may have committed a crime—I'm just telling you—by releasing things that were made retroactively classified. I mean, how do we deal with that? What can we do to try to clear that up?

And what happens when you all disagree with each other?

Mr. MCCULLOUGH. So in terms of when our departments or whether when we disagree as IGs?

Mr. CUMMINGS. Yeah, I mean—yeah, when you disagree as IGs. In other words—in other words, your departments—one of your departments says there is something that should be classified, the other one says it shouldn't, didn't deserve that kind of classification. I mean, what happens then? Is there an arbitrator or whatever? Because this stuff leads to crimes, as you well know.

Mr. LINICK. Well, we don't make classification determinations. We don't——

Mr. CUMMINGS. Well, what can we do to help with that?

Mr. MCCULLOUGH. So, as IGs, we don't make classification determinations.

Mr. CUMMINGS. Right.

Mr. MCCULLOUGH. You're talking about when a department disagrees with another department.

Mr. CUMMINGS. Yes.

Mr. MCCULLOUGH. That happened in this case. So you had the State Department—and I did hear Director Comey's testimony with respect to this up-classification. And that was relative—despite my years in the Federal Government, that was a relatively new term to me. I think that is a fairly common occurrence, a fairly common occurrence in the State Department.

What I can say is that the emails that we reported to Congress in the congressional notification, we focused on those. Those were not up-classified, sir. Those were classified when they were sent and when they were received. So we were focusing on those.

Now, if there's—there is a disagreement, and I think what you're getting to is there was this parallel reporting issue where I believe there was an email or two, the State Department thought that they had received it from a different source. What I can tell you there is the agency that we dealt with and facilitated the classification on that, that's one of the agencies who completed declarations for us. And they disagreed with the supposition that the information came from a parallel source. They believe that that information—they are the information owner for that information.

Some of it was very specific. I can't get into why it was their information in an open forum here. But some of the information was specific enough to tell where it would've come from.

Mr. CUMMINGS. Are you all going to answer the 13 questions?

Mr. MCCULLOUGH. I think we'll get together—if you're not satisfied with where we are right now——

Mr. CUMMINGS. No, I'm not satisfied. I'm not.

Mr. MCCULLOUGH. —we will come and brief you in person, if you like, or——

Mr. CUMMINGS. Yes, I would.

Mr. MCCULLOUGH. —I will get together—yes, sir.

Mr. CUMMINGS. Thank you. I appreciate it.

Mr. MCCULLOUGH. Okay.

Chairman CHAFFETZ. And just as we recognize Mr. Meadows, I think what the committee should look at, in a bipartisan way—if we do it right, we do it together and do it united and do it unanimous if we can. I am very intrigued by what Senator Patrick Moynihan did about 20 years ago. Because, in a bipartisan way, they issued a report about classification. And it was done so—and, basically, the synopsis was: Everything is overclassified, and if everything is classified, then nothing is classified.

And I do agree and concur with the gentleman from Maryland here, my friend, that the consistency, the human error, the problems that this creates, with the mass amount of data and information and the millions of people that have classified clearance, it does create a problem. And I think a bipartisan commission, something similar to what Senator Moynihan spearheaded 20-plus—20 years ago or so, is something that we should look at.

Mr. CUMMINGS. That's a good idea, Mr. Chairman.

Chairman CHAFFETZ. I'd ask unanimous consent to enter into the record the two inspector general reports that are under discussion today.

Without objection, so ordered.

Chairman CHAFFETZ. We'll now recognize the gentleman from North Carolina, Mr. Meadows.

Mr. MEADOWS. Thank you, Mr. Chairman.

Mr. Linick, let me come to you, and feel free to have Ms. Costello jump in if she can illuminate the answer better.

On March of 2015, Secretary Clinton publicly said, and I quote, "I opted for convenience to use my personal email account, which was allowed by the State Department," close quote. She went further to say, "The laws and regulations in effect when I was Secretary of State allowed me to use my email for work. That is undisputed," close quote.

Are those accurate statements?

Mr. LINICK. Well, I'm—I hesitate to comment on public statements, but I will say that our report shows that——

Mr. MEADOWS. Well, we're in a public forum now, and, obviously, a lot's been said about it. Are those accurate or not?

Mr. LINICK. Well, I can tell you our report said that she didn't have approval from senior officials at the Department, and we don't believe it was permitted, both under the rules and none of the officials, the senior officials who were there at the time, gave her approval or were even aware that she had a server, according to them.

Mr. MEADOWS. So let me see if I can digest that long answer into a very short, concise statement. It is not an accurate statement.

Mr. LINICK. Again, she didn't have approval. So——

Mr. MEADOWS. Okay.

So, Ms. Costello, would she have required approval in order to be able to use a personal email, according to regulations? Would she have required that kind of approval?

Chairman CHAFFETZ. Ms. Costello, we have to—I need you to bring your chair up and sit next to Mr. Linick, if you would, because we need to be able to capture that for our recording purposes.

She was sworn.

Ms. COSTELLO. I was.

Chairman CHAFFETZ. Yes.

Ms. COSTELLO. Can you hear me?

Chairman CHAFFETZ. Yes.

Ms. COSTELLO. Okay.

So, in order to exclusively use personal email for official business, Secretary Clinton would have required approval.

The reason we know this is because the officials we interviewed at the Department, both in the Office of Diplomatic Security and the Office of Information Resource Management, told us that. And in telling us that, they were relying on a department policy that was put in place in 2005, which says that day-to-day operations must be conducted—I'm paraphrasing, but must be conducted on authorized information systems.

And so the implication there is any exclusive use would be a day-to-day operation and shouldn't occur without approval.

Mr. MEADOWS. So that created a red flag for your investigative team.

Ms. COSTELLO. As we reviewed the policies that were in place by the Department, yes. It was something that we considered very carefully in evaluating the evidence that we obtained.

Mr. MEADOWS. So her statement that this is undisputed would not be accurate. So I won't make you make a reference to the rest of it, but obviously it's disputed if we're disputing it here today.

Ms. COSTELLO. I would say that, in relying on the interviews that we conducted with the officials at the Department who would be the people responsible for implementing these policies, the answer is, yes, it's disputed.

Mr. MEADOWS. So they would dispute it.

Ms. COSTELLO. They did.

Mr. MEADOWS. Okay. And they did, all right, for the record.

So let me go on a little bit further. Because who—so you mentioned who had the obligation. I guess, how difficult would it be to comply with the law, the Federal Records Act, if you are using your personal email account? What would you have to do?

Ms. COSTELLO. Well, I want to draw a distinction here, because what we were just talking about were the cybersecurity provisions at the Department, and now we've switched a little bit——

Mr. MEADOWS. But to Federal records, wouldn't she have had to have printed out those emails and kept those to be in full compliance with the regulation?

Ms. COSTELLO. Yes. During her tenure, folks in the Office of the Secretary, in order to comply with email records preservation and management policies at the Department, needed to print and file those emails. Now, you can——

Mr. MEADOWS. So, out of the 30,000 emails that we've had testimony earlier today, how many printed copies of emails—of her emails did you find?

Ms. COSTELLO. I don't know. But I can say that we did find, as we reviewed other folks' emails and hard-copy files, we did find some examples of Secretary——

Mr. MEADOWS. So in more than a thousand printed?

Ms. COSTELLO. I'm sorry, I can't hazard a guess on that. I really don't know.

Mr. MEADOWS. All right. So can we get copies of all those printed emails through FOIA or through subpoena?

Mr. LINICK. Well, those—those emails——

Mr. MEADOWS. Because that's the whole reason for the Federal Records Act, is so it would be—so you're suggesting that there is a universe of printed-out emails that we can find.

Ms. COSTELLO. To the extent that other folks who Secretary Clinton emailed did go ahead and print and file——

Mr. MEADOWS. Oh, so you're saying she didn't print any of them out.

Ms. COSTELLO. Right, but they do exist.

Mr. MEADOWS. Oh, okay. That's a big difference. So she made no printed copies in order to comply with the law. That was somebody else perhaps printing it out and she happens to be communicating with them.

Ms. COSTELLO. Correct. And I'm sorry if I wasn't clear before.

Mr. MEADOWS. Okay. No, that's good.

Ms. COSTELLO. What——

Mr. MEADOWS. I'm out of time.

Ms. COSTELLO. —I'm saying is that they exist in the Department. A few here and there do.

Mr. MEADOWS. All right.

I will yield back. Thank you, Mr. Chairman.

Chairman CHAFFETZ. Thank you.

And I think the point that certainly Mr. Gowdy was making is, if those emails on a private server were mailed to somebody else who is not involved in the government, then there is no printed-out copy as required.

We'll now go to Mr. Walberg of Michigan.

Mr. WALBERG. I thank the chairman.

And thanks to the panel for being here.

Mr. McCullough, what is the significance of special access programs?

Mr. MCCULLOUGH. It is the highest level of sensitivity in terms of classification information in the Federal Government.

Mr. WALBERG. The highest level, so beyond classified, Secret——

Mr. MCCULLOUGH. It's the most sensitive information the government has, sir.

Mr. WALBERG. How does that classification then relate to the other categories classified as information such as Confidential, Secret, and Top Secret? In other words, why is it determined to be the most sensitive?

Mr. MCCULLOUGH. So you have several levels of confidentiality classification in the Federal Government. You're starting with Confidential. That's the parenthesis, C, close parenthesis. That's the lowest level of classification. You go up there from the—to the Secret level, and then you go to the Top Secret level.

And then each of those levels may have handling caveats that are trigraphs, such as ORCON, SCI, and what you're asking about is SAP. So the SAP information would be characterized as the most sensitive—among the most sensitive information that we have in the government in terms of classification.

Now, you classify things based upon the relative likelihood of damage to the national security if the information happens to be released. That's an assessment that each person makes in OCA. That's an original classifying authority. They make that assessment when they do classify something. I'm talking about original classification.

Mr. WALBERG. Okay.

Mr. MCCULLOUGH. Now, derivative classification, you're just taking it straight from the OCA's classification and carrying it over. You don't question whether or not the OCA was correct in calling it Secret, SI; you bring it over.

Mr. WALBERG. Okay.

On January 19, 2016, you wrote to the chairman of the Senate Intelligence Committee—or Intelligence and Foreign Relations Committees, saying that the State Department subsequently announced later, as a result of that letter, that it would withhold seven email chains because they referenced materials on special access programs.

In your letter, you said you had not received a declaration from a second intelligence community element as of that time. Did you ever receive one?

Mr. MCCULLOUGH. Yes, sir. That intel element provided their declaration—I believe two declarations directly to the Congress via their own IG, via their agency IG.

Mr. WALBERG. Is it your experience that senior government officials are often unaware of the significance of special access program designations?

Mr. MCCULLOUGH. No, sir. That's not my experience.

Mr. WALBERG. So it's a normal and expected understanding——

Mr. MCCULLOUGH. Absolutely.

Mr. WALBERG. —that senior officials should have.

Mr. MCCULLOUGH. Absolutely.

Mr. WALBERG. Let me ask both of you then, have either of you in your careers ever seen a situation before where special access program information was discussed over unclassified systems?

Mr. MCCULLOUGH. No. I can't recall—I've had a fairly extensive career in the IG world. I was an FBI agent for 10 years, I was the head of investigations at the NSA for 8, and I have been the IC IG for about 5. I can't recall a situation where I have come across this particular situation, no.

Mr. WALBERG. Mr. Linick?

Mr. LINICK. Well, I haven't, but I haven't been in this—I haven't really been working in this space, in terms of, you know, I don't have a lot of opportunity to assess whether others are disclosing special access information. But I haven't seen it in my career.

Mr. WALBERG. What repercussions, Mr. McCullough, come from——

Mr. MCCULLOUGH. Well—and I'll just qualify my answer. That's not to say it hasn't happened. We do get—in the intel community, when you're dealing with intel information every day, especially for the agencies we call the big six, the purely intel agencies, we have employees who are dealing with only classified information all the time, and so there are issues we run into.

And in terms of the consequence for that, I couldn't prejudge what a consequence would be in terms of a security process or an administrative—a misconduct process. But it certainly would be something where the security elements for the intelligence agencies would look at readjudicating the clearance, and it would be a significant factor in the readjudication.

But it's a case-by-case basis for these types of things. There are a lot of factors involved.

Mr. WALBERG. But there would be repercussions, undoubtedly, as a result of——

Mr. MCCULLOUGH. Yes. There would be consequences, yes.

Mr. WALBERG. Okay. Thank you.

Chairman CHAFFETZ. I thank the gentleman.

Mr. WALBERG. I yield back.

Chairman CHAFFETZ. I'd ask unanimous consent to enter into the record a series of memoranda from both the Department of State inspector general and the ODNI inspector general.

And, without objection, so ordered.

Chairman CHAFFETZ. We'll now recognize the gentleman from Georgia, Mr. Carter, for 5 minutes.

Mr. CARTER. Thank you, Mr. Chairman.

And thank you, gentlemen, for being here.

Mr. Linick, in May of 2016, you submitted a report on the Secretary of State's email records management. And you referred to two separate incidents in 2011 in which then-Secretary Clinton's private email server was targeted in hacking attack attempts.

In January of 2011, there were two instances where a non-State Department employee notified Clinton's deputy chief of staff that he had to shut down her server because he believed someone was trying to hack in. The next day, then-Secretary Clinton's deputy chief of staff for operations, Huma Abedin, told senior staff not to email sensitive information over Clinton's server.

Is that true?

Mr. LINICK. That's what we reported, and that's contained in the documents we reviewed.

Mr. CARTER. Okay.

On May 13, 2011, after two of Secretary Clinton's immediate staff discussed Clinton's concern that someone was hacking into her email after she received a suspicious link, Secretary Clinton received another email with a suspicious link from an under secretary. She replied to the email directly, asking if the under secretary had really sent that email, since she was worried about opening it.

Is this best practices? Is this the way you're supposed to—you know, I'm no expert on the Internet or anything, but my kids always told me, no, don't open it.

Mr. LINICK. Well, I can't speak to what's best practices in that community. I mean, I think I probably would——

Mr. CARTER. But is that the way you should respond to a suspicious email, especially after you've already had staff warning you that someone may be hacking into it and that you're concerned that it's being hacked into?

Mr. LINICK. Well, what we reported is that, under State Department rules, you're supposed to report when you believe you've been hacked. And that was where they fell short. They didn't report those.

Mr. CARTER. So they did not report. Even though Ms. Clinton believed that she was being attempted to be hacked into, she did not follow State Department rules and report it.

Mr. LINICK. That's correct.

Mr. CARTER. This is Hillary Clinton we're talking about, the Secretary of State?

Mr. LINICK. That's right.

Mr. CARTER. That's the one? Okay. I just want to make sure.

By responding to that email, do you think that Secretary Clinton may have allowed an attacker to—a hacker to gain access to her emails?

Mr. LINICK. I really would have no knowledge and ability to answer that question, whether she may have allowed an attacker. Obviously, it's a risk. And that's why it's required to be reported, because of the risk. It's a risk.

Mr. CARTER. I was about to say, that's why we have the policy in place.

Mr. LINICK. It's a risk.

Mr. CARTER. Sure, it's a risk.

Mr. LINICK. Yeah.

Mr. CARTER. And I guess that's where we get the "extremely careless," whatever it was.

Anyway, Mr. Linick, at any time during your investigation, did you see evidence—and this is important. Please hang with me here, okay? At any time during your investigation, did you see evidence of Clinton's staff knowing that her server, the server, was unsecure yet they still sent sensitive information over it?

Mr. LINICK. I'm not able to say that. We know from the records—we were not able to interview a number of folks, but we know from email records that there was discussions about the server. Whether

they knew it was secure or unsecure, I don't have any evidence about that.

Mr. CARTER. No evidence about it.

Mr. Linick, if Hillary Clinton's private email server was as secure as she has time and again assured us that it was, saying it was safe and secure, then why would her staff be so concerned?

I mean, you stated in your report, her staff showed a concern, don't use—don't open this email, don't use this, because we think you're being hacked into. Yet we have been told by her that it was perfectly safe and secure. Isn't that true?

Mr. LINICK. We weren't able to interview her staff, so I'm not able to comment on what they were thinking at the time.

Mr. CARTER. You know, I think, Mr. Linick, that it's pretty clear that the Secretary actively jeopardized the network and national security, as well. I think any rational person would understand that this is what happened.

I hope that you'll continue to investigate this. And I hope that you will report back to Congress any information that you might get.

Mr. Chairman, I'll yield back.

Chairman CHAFFETZ. I thank the gentleman.

We'll now recognize the gentleman from Wisconsin, Mr. Grothman, for 5 minutes.

Mr. GROTHMAN. Yeah, I'd like to follow up a little bit more on these emails, okay?

I mean, you guys were investigating the Benghazi thing. A subpoena was issued for the Benghazi documents. Could that have included documents that were emails that she sent or received on her private server?

Mr. LINICK. We didn't investigate Benghazi.

Mr. GROTHMAN. Oh, I'm sorry, I'm sorry.

Mr. MCCULLOUGH. Yeah, we weren't involved in Benghazi either.

Mr. GROTHMAN. Right, right, right. But do you believe on her private email there could have been documents related to Benghazi?

Mr. LINICK. I would be speculating. I don't have an answer for that.

Mr. GROTHMAN. Is it possible? It's her private email.

Mr. LINICK. Again, that wasn't part—I——

Mr. GROTHMAN. Okay. Let me put it this way.

Mr. LINICK. I don't know.

Mr. GROTHMAN. With regard to freedom of information, you have determined that there is no question that she had work emails on her private server, right?

Mr. LINICK. Yes, that's true.

Mr. GROTHMAN. That's incontrovertible, okay? If she had work emails on there, whatever they were about—might have been about Benghazi, might have been about the Clinton Foundation and, you know, whatever's going on there that maybe wasn't right—how long was she supposed to hold on to the emails, the work emails, after she left her office?

Mr. LINICK. Well, as we stated in our report, the rules require that she surrender official records upon her departure. The same rules applied to Powell, as well. And so, at that time, when she left

the Department, those emails should've gone back into the agency recordkeeping system.

Mr. GROTHMAN. Okay. She didn't surrender them. But if she would've surrendered them, how long would they have held on though those emails, work-related emails related to the Secretary of State? Let's say she did the right thing. She leaves office on whatever it was, January of 2013; how long would those emails be held by the government?

Mr. LINICK. Well, that—I don't know the answer to that question. That's unclear. I mean, one of the things in our report was—we stated is that they didn't do such a great job preserving emails at that time. And so their systems that were in place weren't——

Mr. GROTHMAN. Give——

Mr. LINICK. So I don't have an answer to that question, because it's not clear to me how long they would've been preserved.

Mr. GROTHMAN. I'll ask you both, because I think the answer should be obvious.

Maybe the departments weren't doing the right things, but if you get a freedom-of-information request, say, for something that happened 2 years ago, these agencies are supposed to have it, right? Are you guys subject to freedom of information?

Mr. LINICK. Oh, sure. They're supposed to maintain——

Mr. MCCULLOUGH. Right.

Mr. GROTHMAN. Right. So if I ask you guys a freedom-of-information request on something you guys were doing 2–1/2 years ago, you'd be able to pull that up for me, couldn't you?

Mr. LINICK. Well, again, so long as the record is——

Mr. GROTHMAN. You should be able to——

Mr. LINICK. —in the agency's possession.

Mr. GROTHMAN. —right? Assuming somebody didn't screw up.

Mr. LINICK. Some records are disposed of—I mean, there are timeframes. But——

Mr. GROTHMAN. Minutiae. But most things, you would be able to find things that you worked on 2–1/2 years ago, right?

Mr. LINICK. You would hope.

Mr. GROTHMAN. Otherwise, why even have a Freedom of Information Act?

Okay. I guess what I'm getting to, not only did she not turn them over, as you're saying she should have—correct?—but if she wasn't going to turn them over, wouldn't it have more prudent to hold on to them?

Mr. LINICK. I'm not sure I follow you. What——

Mr. GROTHMAN. Okay. If I want to know something that was going on in the Secretary of State's office in 2012 and I made a freedom-of-information request, the first thing they would do is look at the records that they are holding on to, right?

And if Mrs. Clinton did not turn over the records as she was supposed to under law, we might contact her and say, "Hey, Mrs. Clinton, we have a freedom of information request here. Do you have any records dealing with the year 2012?" Right? Isn't that what you think would happen?

Mr. LINICK. I don't know. I mean, possibly.

Mr. GROTHMAN. Kind of frustrating here.

Do you think it was right for her to dispose of these records? This is when she was still Secretary of State. Would it have been right for her to erase work-related emails?

Mr. LINICK. Well, if they count as Federal records, she's supposed to make them part of an agency recordkeeping system.

Mr. GROTHMAN. Right.

Mr. LINICK. That's clear.

Mr. GROTHMAN. Right.

Mr. LINICK. So, if she didn't turn over records that are part of the agency recordkeeping system, then she would be violating State Department rules requiring her to do so.

Mr. GROTHMAN. And if she would've, they would still be available, unlike being erased by her lawyers, right?

Mr. LINICK. So I don't——

Mr. GROTHMAN. Assuming somebody didn't screw up in the State Department.

Mr. LINICK. Well, I don't know if they would've been maintained because we found systemic issues with records preservation. So it's—I can't tell you for sure——

Mr. GROTHMAN. They should've been maintained. I'll put it that way.

Mr. LINICK. Absolutely.

Mr. GROTHMAN. Absolutely. So, absolutely, if somebody makes an open-records request, be it about the Clinton Foundation, be it about Benghazi, whatever, in the year 2014, the State Department should've been able to say, here are the emails related to that, right?

Mr. LINICK. Sure.

Mr. GROTHMAN. Absolutely. And they didn't and couldn't because they were erased by Secretary Clinton.

Mr. LINICK. I don't know if they were erased, but the bottom line is there were, you know, 50,000 pages——

Mr. GROTHMAN. Well, we heard——

Mr. LINICK. —of emails that were not returned to the Department.

Mr. GROTHMAN. We heard when the FBI testified that tens of thousands of emails were erased. So I think we can assume—and some of those they were able to retrieve; we know they were work-related.

So I guess that's the point, was something wrong done there. To erase work-related emails so, as a result, a freedom-of-information request cannot be fulfilled, is there something wrong with that, very wrong with that?

Mr. LINICK. Well, again, in they're agency records, they should be part of the agency recordkeeping system.

Mr. GROTHMAN. In other words, work-related emails.

Mr. LINICK. Well, they'd have to fall within the definition of an agency record, which is anything that documents the, you know, deliberations, the agency transactions, those kinds of things, not personal matters or not logistical matters.

Mr. GROTHMAN. Right. Work-related.

Mr. LINICK. Work-related. Correct.

Mr. GROTHMAN. So when the FBI testifies, as they did, like, an hour ago, that they found work-related emails that had been

erased, there was something clearly wrong there, because those emails should've been available in case somebody was making a freedom-of-information request.

Mr. LINICK. They should have been surrendered to the Department when she left.

Mr. GROTHMAN. Surrendered, and they should have been available.

Mr. LINICK. Right.

Mr. GROTHMAN. Thank you.

Chairman CHAFFETZ. I thank the gentleman.

A couple quick more questions, and then we're getting near the end here.

Ms. Costello, electronic records fall under—electronic records fall under the jurisdiction of the Federal Records Act, correct?

Ms. COSTELLO. Yes, they do.

Chairman CHAFFETZ. Mr. Linick, do you believe—I'm going to ask you both questions, so go ahead and stay.

Does this include—so electronic records fall under the jurisdiction of the Federal Records Act, right, Mr. Linick?

Mr. LINICK. So long as they contain work-related materials, yes.

Chairman CHAFFETZ. Does this include video?

Mr. LINICK. Well, if you're—if you're asking about the videotape, the separate issue, I mean, that's something we're looking at, and we're really not able to comment on it at this time. I mean, that's an ongoing matter, whether videos are records. But we're looking at that issue.

Chairman CHAFFETZ. Let's get—is this relating to the 8 minutes——

Mr. LINICK. Right.

Chairman CHAFFETZ. —of deleted videos?

Mr. LINICK. Right.

Chairman CHAFFETZ. So the inspector general is doing an investigation.

Mr. LINICK. Well, we're looking—where we've done it—we've started a preliminary review, and we're looking into that matter at this point. We have not opened a full-blown investigation, but we are looking to see, sort of, what the issues are, and we have interviewed some people.

Chairman CHAFFETZ. Well, we also have jurisdiction, and we would like to know. So my question is, if the electronic record is video, is it treated differently than if it's text?

Mr. LINICK. I'm not able to answer that question. I mean, that's beyond the scope——

Chairman CHAFFETZ. Why not?

Mr. LINICK. Because I just—I don't have an answer for you. Again, we're sort of in the middle of looking at those issues. It's not part of the report that we issued.

Chairman CHAFFETZ. Right.

Mr. LINICK. And I can only talk about what my work supports. But I wouldn't want to venture a guess if——

Chairman CHAFFETZ. So if the personnel are paid by the Federal Government, the hardware is paid by the Federal Government, the software is paid for by the Federal Government, if somebody were

to tamper with that information, is that a violation of the Federal Records Act?

Mr. LINICK. I mean, a Federal record can be contained on any medium. So, potentially, it could be a record, potentially. In the case you're talking about, there's a transcript and a video, and it's unclear which is the Federal record, so that's why I'm hesitating here. But a Federal record can be on any—it could be on a napkin.

Chairman CHAFFETZ. Could they both be?

Mr. LINICK. Again, I'm not—I'm not sure, and I don't want to guess——

Chairman CHAFFETZ. When will you give us that answer?

Mr. LINICK. Well, we're working on it. So we'll——

Chairman CHAFFETZ. No, but I want to know what's reasonable to know when you're going to get back to us on an answer on that.

Mr. LINICK. You know, I will talk with my staff who's doing that work and get back to you and let you know sort of where we are.

Chairman CHAFFETZ. You'll get back to me when?

Mr. LINICK. I'm happy to get back to you as soon as I get back to the office and let you know you know sort of what's going on.

Chairman CHAFFETZ. By the end of the week? Is that fair?

Mr. LINICK. Sure.

Chairman CHAFFETZ. That's tomorrow.

Mr. LINICK. Sure.

Chairman CHAFFETZ. That would be most helpful.

And I do think—it's a very—it's affecting the Federal record, and I think you need to look very closely at that. It's something we're looking at, and we need your input and your professionalism in saying—to me, it's pretty clear. These are all records, whether they're video, transcript. There may be photos. Certainly, if you are involved in law enforcement, the more of that you have, the better the situation.

And we do this differently than most countries. We do preserve records, and we do allow the public to access this information because they paid for it. It's their government. That's what the Freedom of Information Act is all about. And when things are there and then deleted on purpose, then there's a cloud of mystery that needs to be rectified. And I look forward to hearing back from you.

The emails, the classified Hillary Clinton emails, can you provide us those classified emails?

Mr. LINICK. Well, we didn't look at the classified emails. So that wasn't part of our review. I mean, maybe Mr. McCullough can answer that question. I'm——

Chairman CHAFFETZ. Mr. McCullough?

Mr. MCCULLOUGH. Certainly, I can provide you what—and I believe we have provided Congress with everything that we had. We can certainly—it's over in Senate security. We provided it to SSCI, I believe, and HPSCI also.

Chairman CHAFFETZ. Can you provide this committee in a secure format the classified emails?

Mr. MCCULLOUGH. I can to a certain extent. I cannot provide a certain segment of—because the agency that owns the information for these emails has limited the distribution on those. So they're characterizing them as ORCON. So we have——

Chairman CHAFFETZ. Explain what "ORCON" is.

Mr. MCCULLOUGH. Originator control. So I can't—I can't give them to even Congress without getting the agency's permission to provide them. So they have been provided——

Chairman CHAFFETZ. Which agency?

Mr. MCCULLOUGH. I can't say that here in an open hearing, sir.

Chairman CHAFFETZ. So you can't even tell me which agency won't allow us, as Members of Congress, to see something that Hillary Clinton allowed somebody without a security clearance in a nonprotected format to see? That's correct?

Mr. MCCULLOUGH. This is the segment of emails—this is why my letter back to Ranking Member Cummings had to be classified, because people would like to see this segment of emails. And this has been an issue not just with you and your committee but with several Members at this point.

So we have gone back to the agency that is involved several times, and I can—we can certainly do that again and ask permission.

Chairman CHAFFETZ. Can you generally tell me, is it because they are so sensitive about signals intelligence? Human intelligence? What——

Mr. MCCULLOUGH. We shouldn't get into the content of these emails in an open hearing.

Chairman CHAFFETZ. Okay. I don't want to violate that, but the concern is it has already been violated, and it was violated by Hillary Clinton. And it was her choice. She set it up, and she created this problem, and she created this mess. We shouldn't have to go through this, but she did that.

Mr. MCCULLOUGH. This is the—this is the segment of emails that I had to have people in my office read in to particular programs to even see these emails. We didn't possess the required clearances and compartments.

Chairman CHAFFETZ. So even the inspector general for ODNI didn't have the requisite security clearance.

Mr. MCCULLOUGH. That's right. That's correct. They'd have to get read-ins for them.

Chairman CHAFFETZ. Wow, wow, wow, wow. Unbelievable. What a mess.

I'll yield back. The gentleman from Maryland, Mr. Cummings.

Mr. CUMMINGS. A while back, and it has been a good while, when we had the stimulus program, back in 2009, I guess, Mr. Devaney, who was, I think, in charge of it, he said something I'll never forget. He said—you know, we were talking about how do you control the money and make sure that nobody does anything wrong. He said: I'd rather do things upfront so that people never commit an offense than to have them commit an offense and then they're in trouble.

And I'm trying to figure out—I've got to tell you, this whole thing of classification really bothers me, and it bothers me because I think it's so unfair. I think, I mean, somebody is going to classify something later on, you all just—I mean, your offices—I mean, well, Intelligence and State disagree.

As a matter of fact, I was looking at something where there was a disagreement between State and the Intelligence a while back,

and Senator Corker had sent a letter, wrote a letter to the State Department about one of these disputes last year.

And the State Department responded in September, and I quote: "Your letter focused on an email chain that someone within the intelligence community claims should have been redacted as secret. Our experience is that this process may in some instances result in the IC wrongly assuming that information in the emails originated with the IC, when it may instead have been based upon other sources, given the wide range of context maintained by State Department officials," end of quote.

So, you know, I just—I'm wondering what your offices can do, if anything, it may be out of your jurisdiction, but going back to what Mr. Devaney said back then, is how do we make sure that people are not stepping into violations that they don't even know. I mean, am I missing something?

I mean, and this is serious stuff, man. You've got the FBI Director, the Department of Justice, and people can't even agree. I'm not saying you should agree. But when you tell me—and I'm going to harp on this because I saw it in the Benghazi Committee. You know, you say I'm going to—you committed a crime or you did something wrong when something was upgraded later. What's that about? Can you all help me?

Mr. MCCULLOUGH. There are a couple of issues in there, Mr. Cummings. The first, in terms of the "upgraded later," again, the emails we were concerned about were not those that were upgraded. I believe that's—it's not just—it's not unique to the State Department, but that seems to be a fairly common—when the State Department is processing a FOIA, they upgrade things before they're released.

And so that's one subset, one bucket of emails, and that's separate from the emails we're talking about, it's separate from the emails, I believe, Director Comey is talking about when he says there were 110. I believe that those were classified when they were created and sent and received. So those weren't about being upgraded.

I think—I've heard the term used "retroactive classification." Whatever you want to call it, that is being done with some emails. But the emails that were the concern, I believe, in this case, were the emails that were classified when they were born essentially, when they were created.

Mr. CUMMINGS. But they aren't marked, right?

Mr. MCCULLOUGH. Other than those that you discussed with Director Comey earlier.

Mr. CUMMINGS. Three, three, three, three.

Mr. MCCULLOUGH. Right. I know of none that were marked that we looked at.

Mr. CUMMINGS. See, that's—that's what—that's part of what I'm talking about.

Mr. MCCULLOUGH. Right.

Mr. CUMMINGS. They've got it all out in the press, oh, Hillary Clinton lied because she—and then we come to find out there were three that had markings of a "C," and it was the wrong marking. So basically, 3 out of 30,000-plus. You see how——

Mr. MCCULLOUGH. But to your question about what can we do about over classification, of course, in the intelligence world transparency and classification and secrecy tend to be competing equities. There are civil liberties, protections, offices, and privacy officers.

We have done as IGs over the past several years reports under the Reducing Over-Classification Act. Each IG would have done one of those for their department or agency. And the IGs now, I think, if they haven't finished yet, will be in the process of doing a statutory follow-up—this was mandated from Congress—on reducing over-classification. So each IG is doing a review of its department or agency having to do with overclassification.

Mr. CUMMINGS. Well, I want to—I want to—I hope that the IG bill helps you all, I hope that helps, because we worked very hard on that bill, because we want you all to be effective and efficient. And, again, I want to thank you and your staffs for your service. We really appreciate all that you all do.

Thank you very much, and thank you for being here.

Mr. MCCULLOUGH. Thank you.

Mr. LINICK. Thank you.

Mr. CUMMINGS. And I'm going to follow up on my 13 questions. All right?

Mr. MCCULLOUGH. Yes, sir. We'll be there to brief you in person.

Mr. CUMMINGS. I'm looking forward to it.

Mr. MCCULLOUGH. Yes, sir. Thank you.

Chairman CHAFFETZ. I now recognize the gentleman from Massachusetts, Mr. Lynch.

Mr. LYNCH. Thank you.

I too want to thank you for your service and your willingness to help the committee.

Just in closing, after all this, you know, the long investigation of Secretary Clinton, are we approaching—I mean, technology now has allowed us to have full-spectrum surveillance of people in government, so that every word, every thought, every conversation, it's gone beyond just capturing official records.

But, you know, it's actually—I think we're at a point where it has a chilling effect, where you can't even have normal discourse anymore. You've got to leave your office and have a conversation in the hallway, and you've got to make sure that other person leaves their cell phone aside.

I just think it's driving a lot of conversations underground. And, you know, I realize we're on the Oversight Committee and we want to make sure that we have a certain level of transparency, but I also think that, you know, I think a lot of people in government will think twice.

First of all, people will think twice about serving in government, and then people in government will take great pains to make sure that their thoughts, the open discourse, are not ever recorded because you're going to have a committee like this subpoenaing you and getting every single phone call you ever made and every email you ever made.

It's not good. It's not—this is not a good result. And, you know, I know inquiring minds want to know, but it just makes it very difficult for a government to function and it makes—and it has an im-

plication for the public too, because, you know, people call up—we've exempted ourselves, by the way, Congress, for good reason.

But, you know, the public has to interact with us. And so those phone calls, those emails back and forth, people petitioning their government, that's all subject to surveillance as well. You know, I just think we've reached the tipping point here, and I'm just curious if you think about that at all.

Mr. MCCULLOUGH. Yes, sir. One aspect and one area where we think about that has to do so with whistleblower communications. So as IGs, we deal with the public a lot also. Many of them are current or former government employees or contractors, and so we have, over the past couple of years, had to balance that out too, the need for security, the need for counterintelligence, which is sacrosanct. We have to protect secrets.

On the other hand, we have to have people feel comfortable as whistleblowers to come to an IG and make a complaint about a law, rule, or regulation.

So I share your concern there, and that is something—I chair the Intelligence Community Inspectors General Forum. It's all 17 intel agencies. And it's something that our forum has had a lot of discussion about, frankly.

But we feel as though we've at this point struck a manageable, livable balance with the agencies and management so that people can feel comfortable coming to an IG and complaining to us without fear of their communications being used against them. And if they are, then we have reprisal statutes.

Mr. LYNCH. Yeah.

Mr. MCCULLOUGH. And as Mr. Cummings said, this act is going to help strengthen us also, and so we investigate reprisal when that does happen.

Mr. LYNCH. No, I mean, you see it in the pushback. State Department has a, you know, a culture where, you know, all these people—going back to Condoleezza Rice and Secretary Powell, Secretary Clinton—people using private communication devices, that's all to get out from underneath this, you know, constant surveillance.

So I don't know. At some point we've got to just try to strike that right balance. Sometimes it's difficult.

I yield back.

Chairman CHAFFETZ. I thank the gentleman.

I want to thank our witnesses here today. I want to thank the inspector general community in general. You've got a lot of good men and women who poured their heart and soul in a lot of their work, you know. My biggest fear is that we don't read it, digest it, and then act on it. But we're committed to doing that as much as possible.

Your looking under the hood, your recommendations, your findings, they're pivotal for us to do our jobs here in Congress, and I just want to thank those men and women. I hope you carry that message back to each of your organizations.

I also want to personally thank the three of you for spinning on a dime and being here so swiftly. We did do this around the FBI Director's availability. When I spoke with him on the phone on Tuesday, I asked him which day would be most convenient and he

said Thursday. So that's why we ended up on Thursday, and we all spun around that and you did as well. And so I thank you for the swift manner in which you made yourselves available and the interaction you have had with the committee.

I do want to make sure we follow up on Mr. Cummings' questions and requests. And I do, Mr. Linick, really, and Ms. Costello, want to make sure that we get that information about electronic records as it relates to videos and those types of things.

Chairman CHAFFETZ. Again, I thank you for being here. It has been a good, long day, but fruitful and important work. The committee stands adjourned.

[Whereupon, at 4:04 p.m., the committee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

UNCLASSIFIED U.S. Department of State Case No. F-2015-05069 Doc No. C05833712 Date: 11/05/2015

RELEASE IN PART
B7(C),B6

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between **Hillary Rodham Clinton** and the United States.
(Name - Printed or Typed)

REVIEW AUTHORITY: Barbara Nielsen, Senior Reviewer

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in the Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods, and is classified or is in process of a classification determination under the standards of Executive Order 12958 or other Executive Order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved access to it, and I understand these procedures. I understand that I may be required to sign subsequent Agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be SCI. I further understand that I am obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.

4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to be subjected to security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to disclosing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation with, or showing it to, anyone who is not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.

5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 sets forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon it, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.

6. I have been advised that any breach of this Agreement may result in my termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys fees incurred by the United States Government may be assessed against me if I lose such action.

8. I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code.

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me access to SCI, I understand that all conditions and obligations imposed on me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

FORM 7-97 4414 (EF) (Replaces Form 4355 which is obsolete and will not be used)

UNCLASSIFIED U.S. Department of State Case No. F-2015-05069 Doc No. C05833712 Date: 11/05/2015

11. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798 and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 12958, as amended, so that I may read them at this time, if I so choose.

12. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

13. These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations rights or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosures to Congress by members of the Military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosure of illegality, waste, fraud, abuse, or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.)(governing disclosures that could expose confidential Government agents), and the statutes which protect agent disclosure which may compromise national security, including Section 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

14. This Agreement shall be interpreted under and in conformance with the law of the United States.

15. I make this Agreement without any mental reservation or purpose of evasion.

HR Clinton — Signature — 22 January 2009 — Date

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

WITNESS and ACCEPTANCE: [redacted] — 22 January 2009 — Date

B6
B7(C)

SECURITY BRIEFING / DEBRIEFING ACKNOWLEDGMENT

SI G TK HCS

(Special Access Programs by Initials Only)

[redacted] — SSN (See Notice Below)

Hillary Rodham Clinton — Printed or Typed Name

S — Organization

B6

BRIEF DATE: 22 January 2009

I hereby acknowledge that I was briefed on the above SCI Special Access Program(s):

HR Clinton

Signature of Individual Briefed

DEBRIEF DATE:

Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on the above SCI Special Access Program(s):

Signature of Individual Debriefed

I certify that the briefing presented by me on the above date was in accordance with the relevant SCI procedures.

[redacted] — Signature of Briefing/Debriefing Officer

[redacted] — SSN (See Notice Below)

[redacted] — Printed or Typed Name

DS/IE/SSO State — Organization (Name and Address)

B6
B7(C)
B6
B7(C)

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations.

FORM 11-00 4414 (EF)

Page 2 of 2

UNCLASSIFIED U.S. Department of State Case No. F-2015-05069 Doc No. C05833708 Date: 11/05/2015

RELEASE IN PART
B7(C),B6

REVIEW AUTHORITY:
Barbara Nielsen, Senior Reviewer

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN Hillary Rodham Clinton AND THE UNITED STATES
(Name of Individual – Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Section 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in the Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse)

NSN 7540-01-280-5499
Previous edition not usable

STANDARD FORM 312 (Rev. 1-00)
Prescribed by NARA/ISOO
32 CFR 2003 E.O. 12958

UNCLASSIFIED U.S. Department of State Case No. F-2015-05069 Doc No. C05833708 Date: 11/05/2015

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958, Section 7211 of Title 5, United States code (governing disclosures to Congress); Section 1034 of Title 10, United States code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United State Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE (mm-dd-yyyy)	SOCIAL SECURITY NUMBER (See Notice below)
HR Clinton	22-01-2009	

B6

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)

Department of State
2201 C Street NW
Washington, DC 20520

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE (mm-dd-yyyy) 01-22-2009	SIGNATURE	DATE (mm-dd-yyyy)
NAME AND ADDRESS (Type or print) Department of State 2201 C Street NW Washington, DC 20520		NAME AND ADDRESS (Type or print)	

B6
B7(C)

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE (mm-dd-yyyy)

NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (Rev. 1-00)

Richard W. Painter
S. Walter Richey Professor of Corporate Law
University of Minnesota Law School

July 6, 2016

To the Members of the U.S. House Committee on Oversight and Government Reform:

I write to you about FBI Director James Comey, who I understand has been called to testify before your Committee. I understand that the testimony will concern his recommendation that the Justice Department not pursue criminal charges in connection with former Secretary of State Hillary Clinton's use of a private email server for official government business, including some classified information.

I have known Mr. Comey since we served together in the Administration of President George W. Bush. Mr. Comey is a man of the utmost integrity and he was uniquely suited for the role of United States Attorney and then Deputy Attorney General. He called the shots as he saw them without regard to political affiliation or friendship. He relentlessly prosecuted lawbreakers and refrained from prosecuting when it was not warranted by the evidence.

Throughout the FBIs recent investigation of Secretary Clinton's email server, I have been convinced that Mr. Comey would supervise the investigation with impartiality and strict adherence to the law as well as prosecutorial precedent. Although I am aware of very few prosecutions for carelessness in handling classified information, as opposed to intentional disclosure, I knew that Mr. Comey would recommend prosecution in any and all circumstances where it was warranted. I cannot think of someone better suited to handle such a politically sensitive investigation.

Now that the investigation is concluded, I sincerely hope that your Committee will give Mr. Comey the courtesy of allowing him – once again -- to explain the rationale for his recommendations. Although your Committee is entitled to ask him questions about any alleged impropriety in the course of the investigation, I cannot imagine that there has been any. I also ask that your Committee treat Mr. Comey with the respect that he deserves.

Finally, I urge all Members of the United States Congress to desist from interfering in specific prosecutorial decisions, particularly those involving political allies and opponents. During my tenure in the White House there were very unfortunate allegations that powerful senators sought politically motivated firings of United States Attorneys. Whether or not such allegations were true, it is imperative that Members of the Senate or House never again conduct themselves in a manner where such interference could be suspected. It is also imperative that the Executive Branch do everything possible to assure the independence of federal law enforcement. Mr. Comey's leadership of the FBI and his supervision of this highly sensitive investigation have been a step in the right direction. We should all be proud of his service to our Country.

Respectfully,

/s/

Richard W. Painter

OIG HIGHLIGHTS

View Report

What OIG Reviewed

As part of ongoing efforts to respond to requests from the current Secretary of State and several Members of Congress, the Office of Inspector General (OIG) evaluated efforts undertaken by the Department of State (Department) to ensure that records are properly produced in response to Freedom of Information Act (FOIA) requests involving past and current Secretaries of State. This report addresses (1) the Department's compliance with FOIA statutory and regulatory requirements and (2) the effectiveness of the processes used by the Office of the Secretary's Executive Secretariat (S/ES) to respond to FOIA requests.

What OIG Recommends

OIG recommends that the Bureau of Administration identify personnel needed to improve the timeliness of FOIA responses and to quickly acquire those resources.

OIG recommends further that the Department develop a quality assurance plan to identify and address vulnerabilities in the FOIA process.

OIG also makes two recommendations to S/ES to ensure that its FOIA searches are complete and accurate.

Based on the Department's responses to a draft of this report, OIG considers all of these recommendations to be resolved, pending further action.

January 2016
OFFICE OF EVALUATIONS AND SPECIAL PROJECTS

Evaluation of the Department of State's FOIA Processes for Requests Involving the Office of the Secretary

What OIG Found

S/ES is responsible for coordinating searches for FOIA requests for records held by the Office of the Secretary. When a FOIA request of that nature is received by the Department, the Office of Information Programs and Services (IPS) within the Bureau of Administration notifies S/ES. S/ES reports its findings to IPS, which then communicates with the FOIA requester.

OIG's past and current work demonstrates that Department leadership has not played a meaningful role in overseeing or reviewing the quality of FOIA responses. The searches performed by S/ES do not consistently meet statutory and regulatory requirements for completeness and rarely meet requirements for timeliness. S/ES currently searches Department email accounts only if a FOIA request mentions emails or asks for "all records," or if S/ES is requested to do so during the course of litigation. However, FOIA and Department guidance require searching email accounts when relevant records are likely maintained in these accounts. In addition, although FOIA requires agencies to respond to requests within 20 working days, some requests involving the Office of the Secretary have taken more than 500 days to process. These delays are due, in part, to the Department's insufficient provision of personnel to IPS to handle its caseload.

These problems are compounded by the fact that S/ES FOIA responses are sometimes inaccurate. Officials in IPS and attorneys for the Department identified instances in which S/ES reported that records did not exist, even though it was later revealed that such records did exist. Procedural weaknesses in S/ES FOIA processes appear to be contributing to these deficiencies. For example, S/ES management is not monitoring search results for accuracy, and IPS has limited ability to conduct oversight. S/ES also lacks written policies and procedures for responding to FOIA requests. Finally, staff in S/ES and other components in the Office of the Secretary have not taken training offered by IPS to better understand their FOIA responsibilities.

In September 2015, the Department appointed a Transparency Coordinator to improve the Department's FOIA process, among other things.

~~SENSITIVE BUT UNCLASSIFIED~~

OIG

Office of Inspector General

U.S. Department of State • Broadcasting Board of Governors

ESP-16-01 | Office of Evaluations and Special Projects | January 2016

Evaluation of the Department of State's FOIA Processes for Requests Involving the Office of the Secretary

~~**IMPORTANT NOTICE:** This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

~~SENSITIVE BUT UNCLASSIFIED~~

CONTENTS

OBJECTIVES AND METHODOLOGY 1

BACKGROUND 2

THE DEPARTMENT DOES NOT CONSISTENTLY MEET FOIA LEGAL AND REGULATORY REQUIREMENTS 6

- Statutory Deadlines for Processing Requests Are Not Met 6
- S/ES Does Not Routinely Follow Requirements To Search Email 8

PROCEDURAL WEAKNESSES CONTRIBUTE TO DEFICIENT FOIA SEARCHES AND RESPONSES 10

- Current S/ES FOIA Processes Are Inadequate 10
- S/ES FOIA Searches and Responses Are Sometimes Inaccurate and Incomplete 13

RECOMMENDATIONS 16

APPENDIX A: MANAGEMENT RESPONSES 18

ABBREVIATIONS 24

OIG EVALUATIONS AND SPECIAL PROJECTS TEAM 25

OBJECTIVES AND METHODOLOGY

In April 2015, the Office of Inspector General (OIG) initiated an evaluation to address concerns identified during recent audits and inspections[1] and to respond to requests from the current Secretary of State and several Members of Congress involving a variety of issues, including the use of non-Departmental systems[2] to conduct official business, records preservation requirements, and Freedom of Information Act (FOIA) compliance. This report, which is one of several documenting OIG's findings in these areas, addresses efforts undertaken by the Department of State (Department) to ensure that government records are properly produced in response to FOIA requests involving past and current Secretaries of State. Specifically, this report assesses (1) the Department's compliance with FOIA statutory and regulatory requirements and (2) the effectiveness of the processes used by the Office of the Secretary, Executive Secretariat (S/ES), to respond to FOIA requests. OIG has already issued findings related to one aspect of the FOIA process used to review and release 55,000 pages of emails that former Secretary of State Hillary Rodham Clinton provided to the Department in December 2014.[3] OIG will report separately on issues associated with the use of non-Departmental systems to conduct official business and records preservation requirements.

In planning this work, OIG drew on FOIA, and related regulations and guidance issued by the Department, and *Standards for Internal Control in the Federal Government*.[4] To gain an understanding of the Department's FOIA processes, controls, and policies and procedures, OIG interviewed the Under Secretary for Management, the Assistant Secretary for the Bureau of

[1] OIG has identified the following issues: inconsistencies across the Department in identifying and preserving records, hacking incidents and other issues affecting the security of Department electronic communication, delays and other problems related to processing FOIA requests, and concerns about an Ambassador's use of private email to conduct official business. *See* OIG, *Review of State Messaging and Archive Retrieval Toolset and Record Email* (ISP-I-15-15, March 2015); OIG, *Audit of the Department of State Information Security Program* (AUD-IT-15-17, October 2014); OIG, *Management Alert: OIG Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program* (AUD-IT-14-04, November 2013); OIG, *Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services* (ISP-I-12-54, September 2012); and OIG, *Inspection of Embassy Nairobi, Kenya* (ISP-I-12-38A, August 2012).

[2] For purposes of this work, OIG uses the term "non-Departmental systems" to mean hardware and software that is not owned, provided, monitored, or certified by the Department of State.

[3] OIG, *Potential Issues Identified by the Office of the Inspector General of the Intelligence Community Concerning the Department of State's Process for the Review of Former Secretary Clinton's Emails under the Freedom of Information Act* (ESP-15-04, July 17, 2015). This report made four recommendations to strengthen the Department's review of records prior to release: (1) requesting staff support from intelligence community FOIA offices to assist in the identification of IC equities, (2) facilitating a review of records by IC FOIA officials to ensure that the Department's Classified Network is appropriate for storage of FOIA material, (3) seeking classification expertise from the interagency to act as a final arbiter if there is a question regarding potentially classified material, and (4) incorporating the Department of Justice into the FOIA process to ensure the legal sufficiency review of the FOIA exemptions and redactions. In response, the Department agreed with recommendations 1 and 4, but did not agree with recommendations 2 and 3.

[4] Government Accountability Office (GAO), *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014).

Administration (A), and various officials in the Office of Global Information Services (A/GIS) and S/ES. In addition, OIG reviewed the Department's annual FOIA reports and obtained and analyzed a list of all FOIA requests tasked to the Office of the Secretary from 1996 to 2015. OIG also consulted with the National Archives and Records Administration's Office of Government Information Services and reviewed the FOIA procedures of other Federal agencies. OIG conducted this work in accordance with quality standards for evaluations as set forth by the Council of the Inspectors General on Integrity and Efficiency.

BACKGROUND

Enacted in 1966, FOIA provides that any person has a right, enforceable in court, to obtain access to Federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of the Act's exemptions or exclusions.[5] The Act defines "record" broadly and covers "any information that would be an agency record subject to the requirements of [FOIA] when maintained by an agency in any format, including an electronic format."[6]

Upon receipt of a request for records, the agency is required to determine whether to comply and to notify the requester of its determination and the justification for it within 20 working days.[7] The notification of an adverse determination could be a denial of the request in whole or in part based on the statutory exemptions or a determination that no such records exist. The exemptions include, for example, classified information, privileged communications, and law enforcement information.[8]

In an adverse determination, the agency must notify the requester that he or she has a right to appeal the determination to the head of the agency. An administrative appeal shall be decided within 20 working days.[9] If the appeal is not favorable, the requester may then file a complaint in Federal district court to enjoin the agency from withholding agency records and to order the

[5] FOIA, 5 U.S.C. § 552. If an exemption applies, the agency must notify the requester that a record exists but is exempt from disclosure. If an exclusion applies, the agency may notify the requester that no responsive records subject to FOIA exist. Exclusions relate to the existence of an ongoing criminal investigation, the names of informants, and classified foreign intelligence or counterintelligence or international terrorism records.

[6] 5 U.S.C. § 552(f)(2)(A).

[7] 5 U.S.C. § 552(a)(6)(A)(i). In unusual circumstances, the time limit for responding to a request or an appeal may be extended by up to ten working days. 5 U.S.C. § 552(a)(6)(B).

[8] 5 U.S.C. § 552(b).The nine exemptions are (1) information that is classified to protect national security, (2) information related solely to the internal personnel rules and practices of an agency, (3) information that is prohibited from disclosure by another Federal law, (4) trade secrets or commercial or financial information that is confidential or privileged, (5) privileged communications within or between agencies, (6) information that if disclosed would unwarrantedly invade another individual's personal privacy, (7) certain information compiled for law enforcement purposes, (8) information that concerns the supervision of financial institutions, and (9) geological information on wells.

[9] 5 U.S.C. § 552(a)(6)(A). This includes a determination that no responsive records exist.

production of any agency records the requester believes the agency improperly withheld.[10] In addition, a requester who receives no response within 20 days has a right to file a complaint in district court immediately.[11]

At the Department, the *Foreign Affairs Manual* (FAM) designates the Office of Information Programs and Services (IPS) as responsible for the Department's compliance with FOIA.[12] IPS is a part of the Office of Global Information Services, a subcomponent of the Bureau of Administration. The FAM also designates the Assistant Secretary for Administration as the Chief FOIA Officer, responsible for Department-wide FOIA compliance.[13] The Assistant Secretary for Administration reports to the Under Secretary for Management.[14]

IPS administers the Department's Information Access Program, which includes administering all requests for FOIA records. IPS coordinates, tracks, and reports on responses to all FOIA requests for Department records—including administrative appeals made in connection with such requests—and is supposed to ensure that responses are timely, accurate, and complete.[15] The Department's FOIA regulations specify that FOIA requests be sent to IPS.[16] The request must reasonably describe the records sought, should be specific, and should include all pertinent details about the request, including the subject, timeframe, any individuals involved, and reasons why the Department is believed to have records on the subject of the request.[17]

Once a FOIA request is received, IPS logs it into the case-tracking system—the Freedom of Information Document Management System (FREEDOMS)—and acknowledges the request. IPS then determines which Department bureaus, offices, or overseas posts would possess the requested records and sends a search/review request transmittal (Form DS-1748) to each office FOIA coordinator. The form requires each office to provide information on the files searched and their location, the search terms used, and the time period searched, among other information.

In 2010, the Department issued guidance to offices that describes in general terms how a search is to take place.

> Offices must undertake searches that are reasonably calculated to uncover all relevant materials. Unless otherwise noted in a given request, offices should conduct a search for records in any form, including paper records, email

[10] 5 U.S.C. § 552(a)(4)(B). As an alternative to litigation, a requester may request mediation with the agency, which is conducted by the Office of Government Information Services in the National Archives and Records Administration. 5 U.S.C. § 552(h)(3).

[11] 5 U.S.C. § 552 (a)(6)(C)(i).

[12] 1 FAM 214.2.

[13] 1 FAM 211.2(ee). Executive Order 13392 requires the designation of a Chief FOIA Officer.

[14] 1 FAM 211.2(a)

[15] U.S. Department of State, *FOIA Guidance For State Department Employees* (2010), at 3.

[16] 22 C.F.R. § 171.5(a).

[17] 22 C.F.R. § 171.5(c).

> (including email in personal folders and attachments to email), and other electronic records on servers, on workstations, or in Department databases. Offices do not, however, need to search where there is no reasonable possibility of finding responsive records.[18]

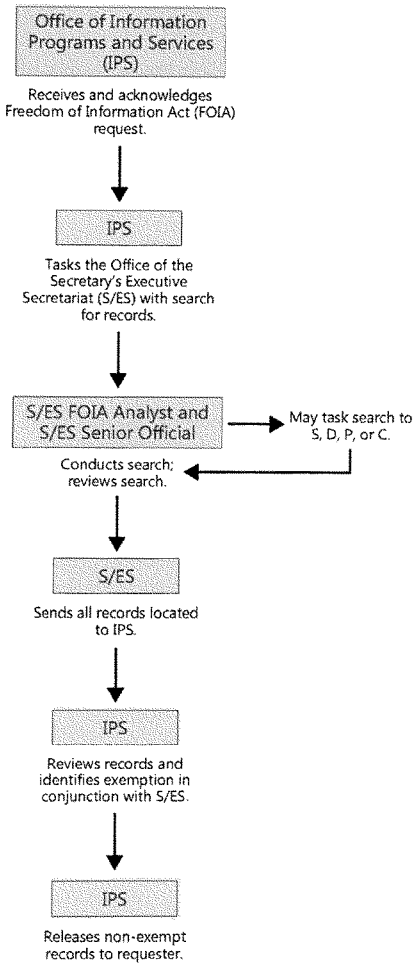
Once the search office returns responsive records to IPS, IPS determines their relevance to the request and whether any part of them may be released to the requester or whether they are subject to one of FOIA's exemptions.[19] IPS then prepares the formal response to the requester and includes any responsive records that are subject to release. If a requester files an administrative appeal of an adverse determination, it is adjudicated by the Appeals Review Panel, consisting of retired Foreign Service Officers.[20]

[18] *FOIA Guidance For State Department Employees,* at 8.

[19] Certain offices, including the Bureau of Diplomatic Security and the Office of Medical Services, are referred to as "decentralized offices" and review their own documents for exemptions. However, these offices must still forward a copy of their response to the request to IPS.

[20] 22 C.F.R. § 171.52.

Figure 1: FOIA Process for Requests Involving the Office of the Secretary



As shown in Figure 1, when a FOIA request involves documents produced by a Secretary of State or other officials in the Office of the Secretary (S), the two Deputy Secretaries of State (D), the Under Secretary for Political Affairs (P), or the Counselor of the Department (C), IPS tasks S/ES with performing a search for relevant documents. S/ES is responsible for the coordination of material presented to the Secretary, Deputy Secretary, and Under Secretaries; the implementation of decisions made by these officials; and the Department's relations with the White House, National Security Council, and other Cabinet agencies.[21] S/ES employs one FOIA Analyst, who reports to the GS-14 Deputy Director of Correspondence, Records, & Staffing (Deputy Director).[22] The Deputy Director serves as the S/ES FOIA coordinator and reports to the Director of Secretariat Staff.

According to information provided by S/ES, the FOIA Analyst searches for relevant documents in several databases or tasks the relevant office (S, D, P, or C) with performing the search. After the search is completed, the Deputy Director conducts a review of the FOIA Analyst's search and the records identified. Finally, all identified records are sent to IPS for processing, along with a signed form DS-1748 identifying the databases searched and the time expended in conducting the search. If the request is in litigation or if legal guidance is sought regarding the search, an attorney from the Office of the Legal Adviser (L) may review the proposed response before it is released to the requester.

[21] 1 FAM 022.2.

[22] A second S/ES employee occasionally assists with FOIA searches in addition to his regular duties.

In September 2015, Secretary of State John Kerry named a former career Senior Foreign Service Officer as the Department's Transparency Coordinator. The Transparency Coordinator will lead the Department's efforts to meet the President's *Managing Government Records* directive, respond to OIG's recommendations, and work with other agencies and the private sector to explore best practices and new technologies. Secretary Kerry also tasked the Transparency Coordinator with improving the efficiency of the Department's systems for responding to FOIA and congressional requests.

THE DEPARTMENT DOES NOT CONSISTENTLY MEET FOIA LEGAL AND REGULATORY REQUIREMENTS

Statutory Deadlines for Processing Requests Are Not Met

FOIA requires agencies to respond to FOIA requests within 20 working days. However, the Department rarely meets this statutory deadline, even for simple requests. Although few agencies are able to meet the 20-day deadline for complex requests,[23] overall compliance is much greater across the Federal Government than at the Department. In FY 2014, the average processing time for simple requests across the Federal Government was 20.5 days, and the Government-wide average for complex requests was slightly less than 119 days.[24] In contrast, the Department took four and one-half times as long—an average of 91 days to process simple requests and almost 535 days to process complex requests.[25]

The Department has been particularly late in meeting FOIA's timelines for requests involving the Office of the Secretary. Table 1, which is based on IPS data provided to OIG, shows the processing time for FOIA requests that were tasked to S/ES and involved the current and past

[23] The Department of Justice, which is required by FOIA to develop reporting and performance guidelines, defines a complex request as one that involves a high volume of material or requires additional steps to process, such as the need to search for records in multiple locations. An example of a simple request is a single individual's visa record. An example of a complex request is one for all records relating to the attacks on U.S. diplomatic facilities in Benghazi, Libya, which covers multiple bureaus and offices of the Department. *See* U.S. Department of Justice, *Guide to the Freedom of Information Act* (2009).

[24] U.S. Department of Justice, *Summary of Annual FOIA Reports For Fiscal Year 2014*, pp. 12–14.

[25] U.S. Department of State, *Freedom of Information Act Annual Report, Fiscal Year 2014*, p. 28. In its 2015 analysis of the performance of the 15 Federal agencies that consistently receive the most FOIA requests, the Center for Effective Government rated the Department as the lowest scoring agency by far. Its analysis demonstrated that the Department processed only 17 percent of the FOIA requests it received in 2013. Center for Effective Government, *Making the Grade: Access to Information Scorecard 2015* (March 2015), p. 2. The Department's Chief FOIA Officer attributed these delays to (1) a large increase in requests and (2) an increase in complex requests. The Department's requests have increased in recent years; however, this increase in requests exists across the Federal Government and is not unique to the Department.

four Secretaries of State.[26] Only 14 of the 417 FOIA requests were completed within the statutory timeframe. Fifty-five of the requests took more than 500 days to process. The majority of the requests, 243 of 417, are still pending; several of these pending requests were received years ago. For example, 10 of the 23 pending requests relating to former Secretary of State Colin Powell are at least 5 years old.

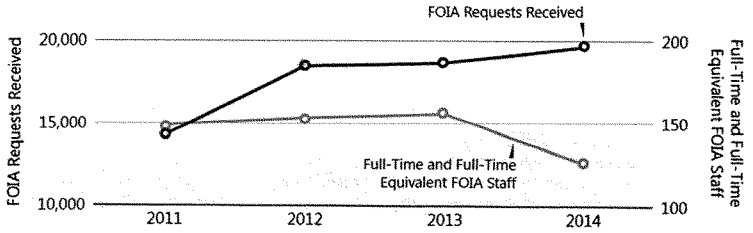
Table 1: Processing Time for FOIA Requests Related to Recent Secretaries of State

	Requests Completed Within Listed Times					
Secretary	Up to 20 Days	21–100 Days	101–500 Days	500+ Days	Still Pending	Total Number of FOIA Requests
Albright	1	0	2	4	2	**9**
Powell	8	4	37	27	23	**99**
Rice	1	3	7	9	20	**40**
Clinton	3	19	27	14	177	**240**
Kerry	1	2	4	1	21	**29**
Total	**14**	**28**	**77**	**55**	**243**	**417**

Source: OIG analysis of IPS data, as of June 2015.

In 2012, OIG reported that one of the key reasons for the timeliness problem was that a relatively small number of IPS staff were processing the heavy volume of Department-wide requests.[27] Since then, as shown in Figure 2, FOIA requests have increased, yet the Department has allocated fewer employees to handle them. According to IPS, some of these employees have been assigned hundreds of requests each and face severe challenges in properly managing their caseloads.

Figure 2: IPS Staff Devoted to Processing Department-wide FOIA Requests



Source: OIG Analysis of IPS data.

[26] S/ES told OIG that its statistics differ from IPS data, but agreed to work with IPS to reconcile the inconsistencies. The FOIA process has several steps, and IPS often tasks multiple offices with responding to requests. Thus, the delays noted in this chart could have occurred at multiple steps in the process and are not necessarily attributable to S/ES search delays.

[27] OIG, *Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services* (ISP-I-12-54, September 2012). GAO also stressed the importance of redirecting or acquiring resources to clear backlogs in a 2012 report on FOIA compliance across the Government. *See* GAO, *Freedom of Information Act: Additional Actions Can Strengthen Agency Efforts to Improve Management* (GAO-12-828, July 2012).

Furthermore, approximately one-third of IPS staff have been assigned to work on one FOIA case in litigation, *Leopold v. Department of State*, in which the court ordered a rolling production of the approximately 55,000 pages of former Secretary Clinton's emails that she provided to the Department in December 2014, while other FOIA work is understaffed.[28]

In each of the past 3 years, IPS has attempted to address this issue by requesting additional personnel to meet the rising caseload, including its most recent request to the Bureau of Administration for 27 additional staff, which it estimated would result in a 10-percent reduction in the FOIA backlog. However, the Department has not provided any additional permanent personnel.

In late September 2015, the Under Secretary for Management decided to detail staff already within the Department to IPS. However, little progress has been made to date to resolve the personnel shortage. On September 2, 2015, the Department solicited expressions of interest from current and retired Department employees in a 9 to 12 month detail to IPS. As of the beginning of November, 7 temporary employees had started work.

S/ES Does Not Routinely Follow Requirements To Search Email

As a general rule, an agency must undertake a FOIA search that is "reasonably calculated to uncover all relevant documents."[29] Since 1997, FOIA has specified that agencies must make a reasonable effort to search for requested documents in electronic form or format, except when such efforts would "significantly interfere" with the operation of an agency's information system.[30] In 2010, the Department issued more explicit requirements for FOIA compliance:

> Unless otherwise noted in a given request, offices should conduct a search for records in any form, including paper records, email (including email in personal folders and attachments to email), and other electronic records on servers, on workstations, or in Department databases.[31]

In addition to searching paper records, S/ES typically searches for relevant documents in several electronic databases, including classified files, the Department's cable and telegram systems, the Secretariat Tracking and Retrieval System (STARS), and EVEREST (which replaced STARS).[32] None

[28] The Department anticipates completing the court-ordered production in January 2016.

[29] *Weisberg v. U.S. Dep't of Justice*, 705 F.2d 1344, 1351 (D.C.Cir. 1983).

[30] 5 U.S.C. § 552(a)(3)(C)).

[31] *FOIA Guidance For State Department Employees*, at 8.

[32] According to information provided by S/ES, EVEREST is a web-based application that provides the Secretary of State and other senior Department principals the ability to receive foreign policy memoranda and correspondence from Department bureaus and offices electronically, as well as task and track the paperless submission of most memoranda. Correspondence and memoranda can include internal and external letters, action memos, information memos, briefing checklists, and telephone talking points, as well as documents received from other agencies. Incoming documents are uploaded (in their native format) by originating offices into EVEREST, submitted to the Executive Secretary for review, and forwarded electronically to the relevant Department principal. EVEREST replaced

of these databases are intended to archive email files. STARS and EVEREST are systems used to route foreign policy memoranda and other documents to the Office of the Secretary. S/ES rarely searched electronic email accounts prior to 2011 and still does not consistently search these accounts, even when relevant records are likely to be uncovered through such a search. For example, S/ES has not searched email accounts for requests seeking all "correspondence" between the Secretary of State and another party. The FOIA Analyst described the decision to search email accounts to be a discretionary one that is only exercised periodically.

According to the Deputy Director's explanation of current practices, S/ES initiates a search of email accounts only if a FOIA request mentions emails or explicitly refers to "all records." S/ES will also search email if it is requested to do so by an L attorney during the course of litigation arising over FOIA issues. If a FOIA request specifically asks for emails of a current employee, the FOIA Analyst tasks S, D, P, or C with searching for the records but does not review the search methodology or approve the results. It appears that current S, D, P, and C employees search through their own email accounts for responsive records.[33] If the FOIA request specifically asks for emails of a former employee, the FOIA Analyst requests the applicable stored electronic file from the S/ES Office of Information Resources Management (S/ES-IRM), the office that handles information technology for the Office of the Secretary.[34] S/ES-IRM reported to OIG that it has maintained files numbering in the thousands for selected senior officials[35] dating back at least as far as Secretary Powell's tenure, though OIG has determined that many of these are not easily accessible.[36] Moreover, as the Deputy Director noted, searching these files is difficult because searches are limited to those that can be undertaken using Microsoft Outlook.[37]

FOIA neither authorizes nor requires agencies to search for Federal records in personal email accounts maintained on private servers or through commercial providers (for example, Gmail, Yahoo, and Hotmail).[38] Furthermore, the FOIA Analyst has no way to independently locate Federal records from such accounts unless employees take steps to preserve official emails in

---

STARS on January 1, 2015, and serves as a permanent, searchable record for the Secretary of State and other senior Department principals memoranda. STARS is a legacy system that was designed to manage the flow of foreign policy memoranda and correspondence both to and from the Secretary of State and other senior Department principals. Incoming and outgoing documents were scanned into STARS, manually indexed (through use of a brief abstract summarizing the substance of the document and identifying document-specific key words), and stored as document images. Searches are limited to retrieval of material based on index terms attached to the document; the document images themselves cannot be searched using text-based search methods. New entries into STARS ended January 1, 2015, but it continues to be used to locate and retrieve documents.

[33] OIG did not evaluate the practices used by S, D, P, and C.

[34] S/ES-IRM stores the files in Personal Storage Table (.pst) files, a format used to store copies of email messages, calendar events, and other items within Microsoft software.

[35] S/ES-IRM does not maintain an index or inventory of these files.

[36] In 2015, the Department began permanently retaining the emails of 102 senior officials.

[37] S/ES has begun testing software intended to enhance its ability to search and retrieve email records.

[38] Records subject to FOIA are those that are (1) either created or obtained by an agency and (2) under agency control at the time of the FOIA request. *U.S. Dept. of Justice v. Tax Analysts*, 492 U.S. 136 (1989). *See also Competitive Enter. Inst. v. Office of Sci. and Tech. Policy*, No. 14-765, 2015 WL 967549 (D.D.C. March 3, 2015).

Department recordkeeping systems. OIG will report separately on preservation requirements applicable to past and current Secretaries of State and the Department's efforts to recover Federal records from personal accounts. However, under current law and Department policy, employees who use personal email to conduct official business are required to forward or copy email from a personal account to their respective Department accounts within 20 days.[39] The Deputy Director, who has handled FOIA responsibilities for S/ES since 2006, could not recall any instances of emails from personal accounts being provided to him in response to a search tasked to an S/ES component.[40]

PROCEDURAL WEAKNESSES CONTRIBUTE TO DEFICIENT FOIA SEARCHES AND RESPONSES

Current S/ES FOIA Processes Are Inadequate

Although specific details of processes for handling FOIA requests vary among agencies, the major steps in processing a request are similar across the Federal Government. Recent assessments of the Department's processes revealed poor practices. In 2012, OIG's inspection of A/GIS found, among other deficiencies, that FOIA requests are prone to delay and that IPS lacked a sound process to develop its information systems.[41] A 2015 report by the Center for Effective Government found that, among 15 agencies that receive a large volume of public records requests, the Department ranked last, in part because of increased processing times and outdated regulations.[42] According to the report, the Department was the only agency whose rules do not require staff to notify requesters when processing is delayed, even though this is mandated by law. Furthermore, little attention has been paid to the accuracy and completeness of responses to FOIA requests. The Department has not sent out a notice or memorandum reminding employees of their FOIA responsibilities since March 2009, when former Secretary Clinton sent a message commemorating Freedom of Information Day.

Although OIG focused on procedural weaknesses in the Office of the Secretary for this evaluation, the issues OIG identified have broader implications. *Standards for Internal Control in the Federal Government* stresses that the tone at the top—management's philosophy and operating style—is fundamental to an effective internal control system.[43] OIG's past and current

[39] 44 U.S.C. 2911; Department of State, *A Message from Under Secretary for Management Patrick F. Kennedy regarding State Department Records Responsibilities and Policy*, Announcement No. 2014_10_115, October 17, 2014.

[40] In November 2014, the Department sent a request to former Secretaries of State for any Federal records that were housed on personal email. In March 2015, the Department sent similar requests to several staff members who worked for former Secretary Clinton. The Department has and continues to produce some of the records received from these requests in response to FOIA requests.

[41] OIG, *Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services* (ISP-I-12-54, September 2012).

[42] Center for Effective Government, *Making the Grade: Access to Information Scorecard 2015* (March 2015).

[43] GAO-14-704G, §§ 1.02 to 1.05.

work demonstrates that Department leadership has not played a meaningful role in overseeing or reviewing the quality of FOIA responses. On September 8, 2015, Secretary Kerry announced the appointment of a new Transparency Coordinator, charged with improving document preservation and transparency systems.[44] This is a positive step, but the following areas, in addition to the lack of compliance with legal and regulatory requirements, need immediate attention:

Lack of Written Policies and Procedures: Although other Department components, such as the Bureaus of Diplomatic Security and International Narcotics and Law Enforcement Affairs, have their own written FOIA guidance or standard operating procedures, S/ES does not. S/ES does use guides on how to search its own databases, EVEREST and STARS, but these are not FOIA specific and no criteria for conducting database searches have been developed. The FOIA Analyst for S/ES reported learning how to perform a FOIA search from on-the-job training. *Standards for Internal Control in the Federal Government* emphasizes the importance of documenting policies and procedures to provide a reasonable assurance that activities comply with applicable laws and regulations.[45] Written policies and procedures are also important for continuity because they increase the likelihood that, when organizational changes occur, institutional knowledge is shared with new staff.[46] Other agencies have recommended written policies and procedures as a best practice. For example, the Office of Inspector General for the Environmental Protection Agency recommends that all regional and program offices responsible for FOIA responses adopt written standard operating procedures to ensure quality control.[47] The Office of Inspector General for the Department of Energy has made a similar recommendation, noting, "without formalized policy and procedures, it could be difficult for an individual unfamiliar with the process to take an active role in filling FOIA requests, possibly leading to delays or inefficiencies in responding to requests."[48]

Inconsistent S/ES Monitoring Efforts: *Standards for Internal Control in the Federal Government* also emphasizes the importance of ongoing monitoring that is built into an entity's operations. Other agencies' monitoring activities vary widely. At some agencies, senior attorneys or career members of the Senior Executive Service are responsible for approving FOIA responses; at others, administrative staff handle the entire FOIA search and review process.[49] Nonetheless, standards emphasize that monitoring should include regular management and supervisory

---

[44] U.S. Department of State Press Statement, *Transparency Coordinator* (Sept. 8, 2015), available at http://www.state.gov/secretary/remarks/2015/09/246691.htm.

[45] GAO-14-704G.

[46] *See, e.g.*, GAO, *Social Security Disability: Management Controls Needed to Strengthen Demonstration Projects* (GAO-08-1053, September 2008).

[47] EPA, Office of Inspector General, *EPA Has Improved Its Response to Freedom of Information Act Requests But Further Improvement Is Needed* (09-P-0127, March 2009).

[48] DOE, Office of Inspector General, *Department's Freedom of Information Act Request Process* (OAS-SR-10-03, Sept. 2010).

[49] *See, e.g.*, Nuclear Regulatory Commission, Office of Inspector General, *Evaluation of Involvement of Political Appointees in NRC's FOIA Process* (OIG-15-A-18, August 2015) and Social Security Administration, Office of the Inspector General, *Freedom of Information Act Response Process* (A-03-15-50107, August 2015).

activities, comparisons, reconciliations, and other routine actions.[50] Such actions may include assessing employee performance with FOIA compliance, conducting spot checks, and establishing and reviewing metrics. Performance standards within S/ES for handling FOIA matters are incomplete. In 2012, OIG recommended that the Department place responsibility at all stages of the process and update performance standards, position descriptions, and work commitments to reflect FOIA responsibilities.[51] While the Deputy Director's performance standards have consistently contained multiple references to that individual's responsibilities as FOIA coordinator, the performance standards for the Deputy Director's former supervisors[52] in the Director of Secretariat Staff position have not mentioned FOIA at all.

Other oversight activities have also been inconsistent. The Deputy Director reviews the FOIA Analyst's search and the records identified. However, the past two Directors of Secretariat Staff reported minimal involvement in the FOIA process, other than providing occasional briefings to supervisors on high-profile or sensitive requests. The past two Directors did not review actual FOIA searches and responses, even on a spot-check basis, for quality, timeliness, thoroughness, or consistency. They also did not gather or review any metrics or other tracking information on S/ES FOIA activities. The current Director, who has been in the position since July 2015, told OIG that, while she periodically reviews FOIA responses, depending on the scope and nature of the FOIA request, she does not carry out any spot checks for accuracy. The current Director also reviews status reports that contain basic information on the date of the request and the offices tasked with conducting searches. No one in S/ES reviews the methodology of FOIA searches tasked to the other components in the Office of the Secretary (S, D, P and C).

Limited IPS Review Capability: The FAM designates IPS as responsible for the Department's compliance with FOIA,[53] and Department guidance specifically requires IPS to ensure that responses are timely, accurate, and complete.[54] However, IPS is almost completely dependent on FOIA coordinators in individual bureaus and offices to ensure that search results meet FOIA requirements. IPS does not have the ability to do independent spot checks in part because it does not have access to the unique databases used to conduct the searches, such as the EVEREST system used by the Office of the Secretary. According to IPS, the quality of responses to requests for FOIA searches varies across the Department. For example, IPS reported that the form documenting the search result (Form DS-1748) the FOIA coordinators submit is sometimes missing key information, such as the files searched and the search terms used. If this information is missing or if IPS identifies another inconsistency, it may ask for a search to be redone. IPS reported that its reviewers have at times spent weeks working with FOIA coordinators to obtain complete responses. In some cases, IPS will contact the FOIA coordinator's supervisor or executive-level staff within the office to resolve an issue. IPS's engagement with S/ES has been

[50] GAO-14-704G, at §§ 16.04, 16.05.

[51] The Department agreed with these recommendations but has yet to take action.

[52] The performance standards for the current Director of Secretariat Staff were not yet available for review at the close of OIG's work.

[53] 1 FAM 214.2.

[54] U.S. Department of State, *FOIA Guidance For State Department Employees* (2010).

limited, with its only contact typically being the Deputy Director. IPS also reports that it has contacted L attorneys for assistance when it has had difficulty obtaining complete responses from S/ES. In one case regarding a request for emails, correspondence, memos, internal notes, and other pertinent documents and records relating to a former S staff member, IPS tasked S/ES with a search in November 2013, but S/ES did not complete the search until December 2014 after the involvement of L. One L attorney characterized routine S/ES searches as frequently deficient, except in instances when FOIA litigation has commenced.

Insufficient Training: During OIG's 2012 inspection of A/GIS, IPS reported to OIG that most Department employees are poorly informed about FOIA principles and procedures, as well as about the importance of providing information to the public. IPS has since provided two Department-wide annual training courses on FOIA, recordkeeping, and classification issues. Records maintained by IPS show that no more than two S/ES employees have attended trainings, open houses, or workshops offered by IPS, and no one from S, D, P, or C has attended.[55] In addition to the annual training sessions, IPS has trained specific offices on FOIA at their request. Twelve bureaus, offices, or embassies have requested and completed this training since 2014, but S/ES is not among them.

S/ES FOIA Searches and Responses Are Sometimes Inaccurate and Incomplete

These procedural weaknesses, coupled with the lack of oversight by leadership and failure to routinely search emails, appear to contribute to inaccurate and incomplete responses. L attorneys and officials in IPS recalled several instances when S/ES searches have yielded inaccurate or incomplete results, though they were unable to determine the magnitude of this problem. The attorneys also noted that FOIA requesters have been able to produce evidence of the existence of records responsive to a FOIA request despite the attestation by S/ES that no responsive records existed.[56]

S/ES has not taken any corrective actions to ensure the accuracy and completeness of FOIA searches. *Standards for Internal Control in the Federal Government* notes that management should remediate identified deficiencies in controls and determine appropriate corrective actions on a timely basis.[57] Implementing such corrective actions could protect the Department from sanctions. For example, in litigated cases, incomplete searches by S/ES can expose the Department to financial liability, including attorney fees and other litigation costs.[58] The Department and its leadership could also be subject to contempt citations if they were found to

[55] According to S/ES, the FOIA Analyst also attended workshops at the Department of Justice.

[56] Department attorneys noted that these instances do not necessarily indicate that the search for records was inadequate. Not all documents created by the Department are Federal records. It is also possible that a document existed at one time but was subsequently destroyed either in compliance with the records disposition schedules or because of poor recordkeeping practices.

[57] GAO-14-704G, at §§ 17.01, 17.05.

[58] 5 U.S.C. § 552(a)(4)(E).

have violated rules requiring candor to the court.[59] Although L attorneys are not aware of an instance where such sanctions were imposed, it is not uncommon for courts to order the Department to conduct additional searches or provide additional information explaining the adequacy of the searches conducted.[60]

OIG has been unable to determine the extent of these inaccuracies, but recent examples of incomplete searches and responses to FOIA queries involving the Office of the Secretary include the following:

- In March 2010, the Associated Press (AP) filed a FOIA request for copies of all of former Secretary Clinton's public and private calendars and schedules. IPS tasked S/ES with searching for responsive records. In November 2010, S/ES provided IPS with records that were non-responsive. IPS then contacted the Office of the Secretary directly and also contacted L for guidance. IPS has no record of receiving responses and the FOIA request sat dormant for several years. In August 2013, AP resubmitted its FOIA request and updated it to include a request for all of the calendars from Secretary Clinton's tenure. In June 2014, December 2014, and again in July 2015, S/ES provided IPS with information regarding the location of these records, which had been retired. In March 2015, after failing to receive responses to multiple FOIA requests, AP filed suit against the Department.[61] In a July 2015 court filing, the Department disclosed that it had finally conducted a search and located at least 4,440 paper and electronic records related to Secretary Clinton's calendars and schedules, which were created by various personnel in the Office of the Secretary.

- In December 2012, the nonprofit organization Citizens for Responsibility and Ethics in Washington (CREW) sent a FOIA request to the Department seeking records "sufficient to show the number of email accounts of, or associated with, Secretary Hillary Rodham Clinton, and the extent to which those email accounts are identifiable as those of or associated with Secretary Clinton."[62] On May 10, 2013, IPS replied to CREW, stating that "no records responsive to your request were located."[63] At the time the request was

[59] *See, e.g., Judicial Watch v. Internal Revenue Service*, Civil Action No. 13-1559 (D.D.C.), where contempt of court citations have been threatened against the IRS in a FOIA lawsuit.

[60] *See e.g., Tarzia v. Clinton*, Civil Action No. 1:10-cv-05654-FM (S.D.N.Y. January 30, 2012); *Beltranena v. Clinton*, Civil Action No. 1:09-cv-01457-BJR (D.D.C. March 17, 2011).

[61] *The Associated Press v. U.S Dept. of State*, Civil Action No. 1:15-cv-00345-RJL (D.D.C.).

[62] Later in the letter as part of its request to waive processing fees, CREW stated its belief that the records it was requesting were "likely to contribute to greater public awareness of the extent to which Secretary Clinton, like the administrator of the Environmental Protection Agency (EPA), use[s] email accounts not readily identifiable as her accounts." CREW also noted: "[r]ecently it was reported that [EPA] Administrator Jackson established alias email accounts to conduct official government business, including an account under the name 'Richard Windson' which is not publicly attributable to her. . . Through this FOIA, CREW seeks to learn how widespread this practice is, and to evaluate the extent to which it has led to under-inclusive responses to FOIA, discovery, and congressional requests, and a failure to preserve records in a way that complies with the Federal Records Act."

[63] The response also noted:

received, dozens of senior officials throughout the Department, including members of Secretary Clinton's immediate staff, exchanged emails with the Secretary using the personal accounts she used to conduct official business. OIG found evidence that the Secretary's then-Chief of Staff was informed of the request at the time it was received and subsequently tasked staff to follow up. However, OIG found no evidence to indicate that any of these senior officials reviewed the search results or approved the response to CREW. OIG also found no evidence that the S/ES, L, and IPS staff involved in responding to requests for information, searching for records, or drafting the response had knowledge of the Secretary's email usage. [64] Furthermore, it does not appear that S/ES searched any email records, even though the request clearly encompassed emails. [65]

- In May 2013, the nonprofit organization Judicial Watch filed a FOIA request for records related to the authorization of a former adviser to Secretary Clinton to undertake employment outside the Department. IPS tasked S/ES with performing the search, which returned 23 documents. In August 2013, AP filed a FOIA request seeking the same information, but S/ES only returned five documents for a nearly identical request.

- In May 2014, Judicial Watch filed a FOIA request seeking records related to talking points given to Ambassador to the United Nations Susan Rice concerning the September 11, 2012, attack on the U.S. diplomatic facilities in Benghazi, Libya. In July 2014, Judicial Watch filed suit in district court because the Department had not responded to the request. In September 2014, IPS tasked S/ES with conducting the search. S/ES initially identified five documents but only returned four documents to IPS because it did not view the fifth document, an email, as responsive. IPS provided the four documents to Judicial Watch in November 2014. In June 2015, pursuant to an earlier request, several former officials provided the Department with copies of records that were in their possession. One of these records included the fifth document identified in the September 2014 search by S/ES as part of a longer email chain. S/ES reviewed this

---

It may be helpful for you to know that messages from the Secretary are occasionally transmitted to the Department via email. However, these messages are transmitted from a "dummy" email address that is not capable of receiving replies, rather than from a functioning email account.

[64] On August 11, 2014, the Department produced to the House Select Committee on Benghazi documents related to the 2012 attack on U.S. facilities in Benghazi. The production included a number of emails revealing that Secretary Clinton used a personal email account to conduct official business. OIG discovered four instances, between July and September 2014, in which staff from L, A, or the Bureau of Legislative Affairs reviewed the CREW request and the Department's May 2013 response, but the Department did not amend its response. L and A staff also told OIG that the Department does not customarily revise responses to closed FOIA requests. Nevertheless, during the course of this review, Department staff advised OIG of their belief that the Department's response to CREW was incorrect and that it should have been revised to include the former Secretary's personal email account used to conduct official government business. OIG notes that the issue may have been resolved insofar as the Department is now engaged in the process of publishing on its FOIA website the 55,000 pages of personal emails produced by Secretary Clinton.

[65] According to a February 26, 2013, memorandum to IPS, S/ES stated that its FOIA Analyst spent an hour searching through the Department cable and telegram system and STARS and did not discover any responsive records. The Deputy Director reviewed the search and results, but no other official within S/ES conducted a review.

document and determined that it was in fact responsive to the FOIA request, which the Department disclosed to the court in July 2015.

RECOMMENDATIONS

To ensure that FOIA requests involving the Office of the Secretary generate timely, accurate, and complete searches and responses, OIG has issued the following recommendations to the Bureau of Administration, the Office of the Secretary, and the Department's Transparency Coordinator. Their responses can be found in Appendix A.

Recommendation 1: The Bureau of Administration should identify necessary permanent personnel as part of FOIA workforce planning efforts and quickly acquire those resources so the Department can comply with applicable law and improve the timeliness of FOIA searches and responses.

Management Response: In its November 30, 2015, response, the Bureau of Administration concurred with this recommendation. It noted that its fiscal year 2017 budget request includes funding for two additional permanent positions for FOIA and continued funding of 50 temporary positions (eligible family members and rehired annuitants).

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation showing that these 52 positions have been filled. However, OIG strongly encourages the Bureau of Administration to continue to monitor its staffing levels to determine whether additional permanent personnel are needed to process FOIA requests.

Recommendation 2: The Office of the Secretary, Executive Secretariat, should fully comply with FOIA requirements and Department guidance by (a) searching email records for all FOIA requests in which relevant records are likely maintained in email accounts; and (b) reminding S/ES employees that Federal records contained in personal emails may be subject to FOIA when in the Department's control and should be preserved in the Department's recordkeeping systems.

Management Response: In its November 30, 2015, response, the Executive Secretariat concurred with this recommendation. It noted that its current practice is to search email records for all FOIA requests in which responsive records are likely to be located.

OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives a copy of S/ES FOIA policies and procedures that require a search of email records for all FOIA requests in which relevant records are likely maintained in email accounts and a reminder to S/ES employees that Federal records contained in personal email may be subject to FOIA and must be preserved in the Department's recordkeeping systems.

Recommendation 3: The Office of the Secretary, Executive Secretariat should address weaknesses in its FOIA processes by:

- Developing written policies and procedures for performing FOIA searches addressed to the Office of the Secretary.
- Including FOIA duties as part of the performance standards for the Director of Secretariat Staff.
- Ensuring that executive-level staff members rigorously oversee the FOIA process, to include regular monitoring activities and implementing corrective actions as needed.
- Coordinating FOIA training for all S/ES, Office of the Secretary, Deputy Secretaries, Under Secretary for Political Affairs, and Counselor of the Department staff.

Management Response: In its November 30, 2015, response, the Executive Secretariat concurred with this recommendation. It noted that S/ES is currently drafting FOIA policies and procedures and metrics for timeliness and completeness of FOIA responses. S/ES also noted that the work requirements for the current Director of the Executive Secretariat include FOIA responsibilities and that FOIA training for S/ES staff is in progress.

OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives copies of S/ES FOIA policies and procedures that include monitoring activities and the development of metrics that are reviewed by executive-level staff; a copy of the work requirements for the current Director that include FOIA responsibilities; and FOIA training records for S/ES employees.

Recommendation 4: The Department's Transparency Coordinator should work with IPS to develop a quality assurance plan to identify and address Department-wide vulnerabilities in the FOIA process, including lack of monitoring of FOIA searches and responses, technological challenges, and the sufficiency of staffing and training.

Management Response: In her response, the Transparency Coordinator concurred with this recommendation. She endorsed an accountability framework for the Department that includes processes, roles, standards, and metrics to help ensure that important legal, administrative, evidential, and historical information requirements of the Department are met.

OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives a copy of the quality assurance plan.

APPENDIX A: MANAGEMENT RESPONSES

United States Department of State

Assistant Secretary of State
for Administration
Washington, D.C. 20520

November 30, 2015

UNCLASSIFIED

TO: Inspector General - Steve Linick

FROM: Bureau of Administration - Joyce A. Barr

SUBJECT: Draft report - Review of the Department of State's FOIA Processes for Requests Involving the Office of the Secretary (ESP-16-01 dated November 13, 2015)

The Bureau of Administration thanks the OIG for the opportunity to respond to the subject draft report and provides the following in response to the single recommendation for this bureau's action.

Recommendation 1: The Bureau of Administration should identify necessary permanent personnel as part of the FOIA workforce planning efforts and quickly acquire those resources so the Department can comply with applicable law and improve the timeliness of FOIA searches and responses.

The Bureau of Administration concurs with this recommendation. As the OIG is aware, increasing the number of A/GIS/IPS FOIA staff is one part of the solution for improving Department response time to FOIA cases that are often broad and extremely complex. To date, A Bureau has taken the following steps to increase our FOIA staffing/resources in Fiscal Year 2016 and our request for Fiscal Year 2017.

The A/GIS approved budget request for FY 2016, which includes FOIA, was $13,932,000. The A Bureau recently requested an additional $8.3M for FY 2016 to cover the cost of salaries, support, information technology (IT), and other necessities for 50 new positions dedicated to FOIA operations ("FOIA 50"). Hiring is currently under way for 10 Eligible Family Members (EFMs) and 40 subject matter expert Foreign Service annuitants. A minimum Top Secret

UNCLASSIFIED

clearance is required for each of these positions and hiring eligible family members and annuitants helps to expedite that clearance requirement. The FY 2016 funding level for these activities is subject to the availability of FY 2016 appropriations which are currently pending with Congress.

A Bureau's FY 2017 request to OMB includes two FTE and additional support costs including resources to improve FOIA systems. It is our understanding the OMB pass-back for FY 2017 is expected later this week. If provided, the resources requested for FY 2017 should allow the A Bureau to fund, at least partially, the recurring costs to maintain the FOIA 50 positions in FY 2017 (i.e. salaries, support, IT, etc.).

The A Bureau appreciates the OIG's support of our ongoing efforts to improve the Department's FOIA program.

United States Department of State

Washington, D.C. 20520

November 30, 2015

UNCLASSIFIED

TO: Steve Linick, Inspector General

FROM: MaryKary Carlson, Acting Executive Secretary

SUBJECT: Response to Draft OIG Review of the Department of State's FOIA Processes for Requests Involving the Office of the Secretary

The Executive Secretariat thanks the OIG for the opportunity to respond to this review and values the OIG's study of the Department's FOIA process. The Secretariat has the following specific responses to the recommendations contained in the report.

Recommendation 1: While this recommendation is directed to the A Bureau, the Executive Secretariat notes that it has experienced a commensurate increase in the number of FOIA requests and also needs more staff dedicated to FOIA-related work. S/ES-S is currently in the process of reprogramming one FTE position to work on FOIA. While the growing FOIA workload has affected response times, S/ES-S records do not match the number of pending FOIA requests cited in the draft report. S/ES-S and A/GIS/IPS have agreed to work together to review and reconcile the number of outstanding FOIA cases involving the Office of the Secretary.

Recommendation 2: The Executive Secretariat strongly agrees with the OIG recommendation that it should fully comply with FOIA requirements and Department guidance by searching email records for all FOIA requests in which relevant records are likely maintained in email accounts. This is the current practice of the Executive Secretariat staff (S/ES-S) and is the instruction provided to all offices engaged in FOIA searches involving the Office of the Secretary and comports with the instruction provided to all offices in the Department.

The Executive Secretariat further agrees with the OIG recommendation that S/ES employees should be reminded that Federal records contained in personal emails may be subject to FOIA and should be preserved in the Department's record-keeping systems. All Department employees received this guidance and

instruction from the Under Secretary for Management on October 17, 2014 and it is reiterated to all S/ES and S bureau employees in their check-in, periodic training, and check-out briefings on records management. As instructed in the above-referenced guidance from the Under Secretary for Management, to ensure Federal records contained in personal emails are preserved in the Department's recordkeeping systems, all employees are required to copy or forward any personal message containing a Federal record to their official Department email accounts for appropriate retention and archiving.

Recommendation 3: The Executive Secretariat welcomes the OIG's suggestions for improvement in its FOIA processes and concurs with all four elements of the recommendation. The Executive Secretariat has already taken steps to implement these recommendations, specifically:

1. Written policies and procedures (SOPs) are currently being drafted for all involved in the FOIA search process in the S bureau. These SOPs will be cleared with A/GIS/IPS and others in the Department, as appropriate.
2. The work requirements of the current Director of the Executive Secretariat Staff (S/ES-S) include oversight and management of the FOIA process for S/ES.
3. The Director of the Executive Secretariat Staff oversees all FOIA searches conducted by S/ES-S staff and reviews and approves all responses to A Bureau. S/ES-S management is developing metrics for timeliness of response and completeness of searches.
4. The Acting Executive Secretary and other senior Executive Secretariat managers have recently completed FOIA training conducted by A/GIS, and training sessions are being arranged for staff of the office of the Secretary, the Deputy Secretaries, the Under Secretary for Political Affairs, and the Counselor.

The Secretariat notes (p. 9 of draft report) the OIG comment on the fact that S/ES tasks current S, D, D-MR, P, and C employees to search through their own email accounts for responsive records in FOIA cases. The Executive Secretariat would like to clarify for OIG that this is standard practice Department-wide per guidance from A Bureau. The Executive Secretariat would further like to clarify for OIG that S/ES-S does review the results of all such searches.

Recommendation 4: The Executive Secretariat looks forward to continuing ongoing collaboration with the Transparency Coordinator to improve the FOIA process. In particular, the Secretariat strongly supports the recommendation to focus on technological challenges to conducting successful FOIA searches.

UNCLASSIFIED

TO: Steve Linick, Inspector General

FROM: Janice L. Jacobs, Transparency Coordinator

SUBJECT: Response to Draft OIG Review of the Department of State's FOIA Processes for Requests Involving the Office of the Secretary

I appreciate the work by your Special Projects team to identify needed improvements to processes and procedures related to the Department's handling of requests under the Freedom of Information Act (FOIA). I will take the opportunity in the Quality Assurance Plan (QAP) to address FOIA-related issues (Recommendation 4) within the context of information management within the Department.

As Transparency Coordinator, my overall vision is a 21st century enterprise-wide information management system that advances the Department's goals of increased efficiency, transparency, and accountability. Under this vision, records management is less an independent arm in the information landscape and a more integrated process and functional system within a whole-of-enterprise information and knowledge management environment.

Information is one of the Department's most valuable assets requiring careful management, thoughtful governance and strategic consideration in its use and control. The IG report recommends a stronger focus on information governance, technological challenges and sufficient staffing and training. Specifically, the Department needs an accountability framework that covers the processes, roles, standards, and metrics to help ensure that important legal, administrative, evidential and historical information requirements of the Department are met. Creating this framework is the goal of the QAP I will prepare, in concert with A/GIS/IPS, S/ES and other pertinent offices.

The Department is not alone in dealing with the information management challenges associated with today's fast changing, data-driven world. Many agencies have the same issues: records management/FOIA traditionally have not been a high priority; a new norm of a high volume of requests and litigation cases; staffing and funding shortfalls; outdated technology or technology silos; insufficient records-related internal controls; and insufficient training/education on

the importance of effective management of information/records. Secretary Kerry recognizes these challenges and my appointment was one step towards trying to address these matters holistically.

My plan will address all these issues, again with a view towards finding Department-wide solutions. I will start with a communications strategy that begins to talk about information management in new ways to highlight the important role that all Department employees play in preserving records. This will begin with a message from the top followed up by periodic messages to domestic and overseas employees.

Thank you for the opportunity to provide comments to the report on FOIA-related processes. I look forward to helping to implement your recommendations both on FOIA and on records preservation in general.

ABBREVIATIONS

A	Bureau of Administration
A/GIS	Office of Global Information Services
AP	Associated Press
C	Counselor of the Department
CREW	Citizens for Responsibility and Ethics in Washington
D	Deputy Secretary
Department	Department of State
Deputy Director	S/ES Deputy Director of Correspondence, Records, and Staffing
FAM	*Foreign Affairs Manual*
FOIA	Freedom of Information Act
GAO	Government Accountability Office
IPS	Office of Information Programs and Services
FREEDOMS	Freedom of Information Document Management System
L	Office of the Legal Adviser
OIG	Office of Inspector General
P	Under Secretary for Political Affairs
S	Office of the Secretary
S/ES	Office of the Secretary, Executive Secretariat
S/ES-IRM	S/ES Office of Information Resources Management
STARS	Secretariat Tracking and Retrieval System

OIG EVALUATIONS AND SPECIAL PROJECTS TEAM

Jennifer L. Costello, Team Leader
David Z. Seide, Team Leader

Michael Bosserdet, Office of Inspections
Kelly Minghella, Office of Investigations
Brett Fegley, Office of Inspections
Aaron Leonard, Office of Audits
Robert Lovely, Office of Evaluations and Special Projects
Jeffrey McDermott, Office of Evaluations and Special Projects
Kristene McMinn, Office of Inspections
Eric Myers, Office of Investigations
Phillip Ropella, Office of Audits
Timothy Williams, Office of Inspections

HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926
OIG.state.gov/HOTLINE

If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:

OIGWPEAOmbuds@state.gov

UNCLASSIFIED

OIG

Office of Inspector General

U.S. Department of State • Broadcasting Board of Governors

ESP-16-03 | Office of Evaluations and Special Projects | May 2016

Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements

IMPORTANT NOTICE: This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.

UNCLASSIFIED

ESP-16-03

What OIG Evaluated

As part of ongoing efforts to respond to requests from the current Secretary of State and several Members of Congress, the Office of Inspector General (OIG) reviewed records management requirements and policies regarding the use of non-Departmental communications systems. The scope of this evaluation covers the Office of the Secretary, specifically the tenures of Secretaries of State Madeleine Albright, Colin Powell, Condoleezza Rice, Hillary Clinton, and John Kerry.

This report (1) provides an overview of laws, regulations, and policies related to the management of email records; (2) assesses the effectiveness of electronic records management practices involving the Office of the Secretary; (3) evaluates compliance with records management requirements; and (4) examines information security requirements related to the use of non-Departmental systems.

What OIG Recommends

OIG makes eight recommendations. They include issuing enhanced and more frequent guidance on the permissible use of personal email accounts to conduct official business, amending Departmental policies to provide for administrative penalties for failure to comply with records preservation and cybersecurity requirements, and developing a quality assurance plan to address vulnerabilities in records management and preservation. The Department concurred with all of OIG's recommendations.

UNCLASSIFIED
May 2016
OFFICE OF EVALUATIONS AND SPECIAL PROJECTS

Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements

What OIG Found

The Federal Records Act requires appropriate management and preservation of Federal Government records, regardless of physical form or characteristics, that document the organization, functions, policies, decisions, procedures, and essential transactions of an agency. For the last two decades, both Department of State (Department) policy and Federal regulations have explicitly stated that emails may qualify as Federal records.

As is the case throughout the Federal Government, management weaknesses at the Department have contributed to the loss or removal of email records, particularly records created by the Office of the Secretary. These weaknesses include a limited ability to retrieve email records, inaccessibility of electronic files, failure to comply with requirements for departing employees, and a general lack of oversight.

OIG's ability to evaluate the Office of the Secretary's compliance with policies regarding records preservation and use of non-Departmental communications systems was, at times, hampered by these weaknesses. However, based on its review of records, questionnaires, and interviews, OIG determined that email usage and preservation practices varied across the tenures of the five most recent Secretaries and that, accordingly, compliance with statutory, regulatory, and internal requirements varied as well.

OIG also examined Department cybersecurity regulations and policies that apply to the use of non-Departmental systems to conduct official business. Although there were few such requirements 20 years ago, over time the Department has implemented numerous policies directing the use of authorized systems for day-to-day operations. In assessing these policies, OIG examined the facts and circumstances surrounding three cases where individuals exclusively used non-Departmental systems to conduct official business.

CONTENTS

OBJECTIVES AND METHODOLOGY 1

BACKGROUND 2

PRESERVATION REQUIREMENTS HAVE GENERALLY REMAINED CONSISTENT AS LAWS AND POLICIES RELATED TO THE USE OF EMAILS HAVE EVOLVED 4

MANAGEMENT WEAKNESSES CONTRIBUTE TO LOSS OF EMAIL RECORDS 12

STAFF EMAIL USAGE AND COMPLIANCE WITH RECORDS MANAGEMENT REQUIREMENTS VARY 19

CYBERSECURITY RISKS RESULT FROM THE USE OF NON-DEPARTMENTAL SYSTEMS AND EMAIL ACCOUNTS 26

- Employees Generally Must Use Department Information Systems To Conduct Official Business 27
- Restrictions Apply to the Use of Non-Departmental Systems 28
- The Department Has Issued Numerous Warnings About Cybersecurity Risks 32
- Three Officials Exclusively Used Non-Departmental Systems for Day-to-Day Operations 34

CONCLUSION 42

RECOMMENDATIONS 43

APPENDIX A: RELEVANT LAWS AND POLICIES DURING THE TENURES OF THE FIVE MOST RECENT SECRETARIES OF STATE 47

APPENDIX B: MANAGEMENT RESPONSES 65

ABBREVIATIONS 77

OIG TEAM MEMBERS 79

OBJECTIVES AND METHODOLOGY

In April 2015, the Office of Inspector General (OIG) initiated an evaluation to address concerns identified during recent audits and inspections[1] and to respond to requests from the current Secretary of State and several Members of Congress involving a variety of issues, including the use of non-Departmental systems[2] to conduct official business, records preservation requirements, and Freedom of Information Act (FOIA) compliance. This report, which is the fourth and final to document OIG's findings in these areas,[3] addresses efforts undertaken by the Department of State (Department) to preserve and secure electronic records and communications involving the Office of the Secretary. Specifically, this report (1) provides an overview of laws, regulations, and policies related to the management of email records; (2) assesses the effectiveness of electronic records management practices involving the Office of the Secretary; (3) evaluates staff compliance with records management requirements; and (4) examines information security requirements related to the use of non-Departmental systems.

As part of the current evaluation, OIG reviewed laws, policies, and practices from (and, in some cases, prior to) 1997 through the present, covering the tenures of five Secretaries: Madeleine Albright (January 23, 1997–January 20, 2001); Colin Powell (January 20, 2001–January 26, 2005); Condoleezza Rice (January 26, 2005–January 20, 2009); Hillary Clinton (January 21, 2009–February 1, 2013); and John Kerry (February 1, 2013–Present).

OIG reviewed the requirements of the Federal Records Act[4] and the Federal Information Security Management Act (FISMA)[5] and related regulations; circulars and directives issued by the President, the National Archives and Records Administration (NARA), the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB); applicable

[1] OIG has identified the following issues: inconsistencies across the Department in identifying and preserving records, hacking incidents and other issues affecting the security of Department electronic communication, delays and other processing problems related to FOIA requests, and concerns about an Ambassador's use of private email to conduct official business. *See* OIG, *Review of State Messaging and Archive Retrieval Toolset and Record Email* (ISP-I-15-15, March 2015); OIG, *Audit of the Department of State Information Security Program* (AUD-IT-15-17, October 2014); OIG, *Management Alert: OIG Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program* (AUD-IT-14-03, November 2013); OIG, *Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services* (ISP-I-12-54, September 2012); and OIG, *Inspection of Embassy Nairobi, Kenya* (ISP-I-12-38A, August 2012).

[2] For purposes of this work, OIG uses the term "non-Departmental systems" to mean hardware and software that is not owned, provided, monitored, or certified by the Department of State.

[3] Previous reports include the following: OIG, *Potential Issues Identified by the Office of the Inspector General of the Intelligence Community Concerning the Department of State's Process for the Review of Former Secretary Clinton's Emails under the Freedom of Information Act* (ESP-15-04, July 2015), OIG, *Evaluation of the Department of State's FOIA Processes for Requests Involving the Office of the Secretary* (ESP-16-01, January 2016), and OIG, *Classified Material Discovered in Unclassified Archival Material* (ESP-16-02, March 2016).

[4] 44 U.S.C. chapters 21, 29, 31, and 33.

[5] Pub. L. No. 107-347, title III, 116 Stat. 2946 (2002). In 2014, FISMA was replaced by the Federal Information Security Modernization Act, 44 U.S.C. § 3551 (2014).

Department directives issued in the *Foreign Affairs Manual* (FAM) and the *Foreign Affairs Handbook* (FAH);[6] and guidance and policies in cables and memoranda. Appendix A summarizes the relevant laws and policies that OIG reviewed during this evaluation.

OIG employed a number of strategies to test compliance with email records preservation requirements applicable to each Secretary's tenure, including (1) sending questionnaires to current and former staff of the Office of the Secretary requesting information about email usage and preservation practices; (2) reviewing records and public statements related to email usage; (3) comparing stated practices against applicable laws and policies; and (4) searching available hard-copy and electronic files to identify and analyze email records and assess staff practices. OIG faced a number of challenges in conducting this testing, which will be discussed in greater detail throughout the report.

OIG also interviewed dozens of former and current Department employees, including the Deputy Secretary for Management and Resources (D-MR); the Under Secretary for Management (M); the Assistant Secretary and other staff in the Bureau of Administration (A); and various staff in the Office of the Secretary and its Executive Secretariat (S/ES), the Office of the Legal Adviser (L), the Bureau of Information Resource Management (IRM), and the Bureau of Diplomatic Security (DS). In conjunction with the interviews, OIG reviewed paper and electronic records and documents associated with these offices. OIG also consulted with NARA officials. Finally, OIG interviewed Secretary Kerry and former Secretaries Albright, Powell, and Rice. Through her counsel, Secretary Clinton declined OIG's request for an interview.[7]

OIG conducted this work in accordance with quality standards for evaluations as set forth by the Council of the Inspectors General on Integrity and Efficiency.

BACKGROUND

The Federal Records Act requires the head of each agency to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the

[6] The Department articulates official guidance, including procedures and policies, on matters relating to Department management and personnel in the *Foreign Affairs Manual* and *Handbook*. 2 FAM 1111.1 (July 3, 2013).

[7] In addition to Secretary Clinton, eight former Department employees declined OIG requests for interviews: (1) the Chief of Staff to Secretary Powell (2002-05); (2) the Counselor and Chief of Staff to Secretary Clinton (2009-13); (3) the Deputy Chief of Staff for Policy to Secretary Clinton (2009-11) and the Director of Policy Planning (2011-13); (4) the Deputy Chief of Staff for Operations to Secretary Clinton (2009-13); (5) the Deputy Assistant Secretary for Strategic Communication (2009-13); (6) the Director of the S/ES Office of Information Resources Management (2008-13); (7) a Special Advisor to the Deputy Chief Information Officer (2009-13) who provided technical support for Secretary Clinton's personal email system; and (8) a Senior Advisor to the Department, who supervised responses to Congressional inquiries (2014-15). Two additional individuals did not respond to OIG interview requests: the Deputy Secretary of State for Management and Resources (2011-13) and an individual based in New York who provided technical support for Secretary Clinton's personal email system but who was never employed by the Department.

information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities."[8] Effective records management is critical for ensuring that sufficient documentation of an agency's business is created, that an agency can efficiently locate and retrieve records needed in the daily performance of its mission, and that records of historical significance are identified, preserved, and made available to the public.[9]

Citing its responsibilities under the Federal Records Act, the Department sent letters in October and November 2014 to the representatives of former Secretaries Albright, Powell, Rice, and Clinton requesting that they make available copies of any Federal records in their possession, such as emails sent or received on a personal email account while serving as Secretary of State. In response, Secretary Albright's representative advised that Secretary Albright did not use a Department or personal email account during her tenure, and Secretary Rice's representative advised that Secretary Rice did not use a personal email account to conduct official business.[10] Representatives for Secretaries Powell and Clinton acknowledged that the Secretaries used personal email accounts to conduct official business.

Secretary Powell has publicly stated that, during his tenure as Secretary, he "installed a laptop computer on a private line" and that he used the laptop to send emails via his personal email account to his "principal assistants, individual ambassadors, and foreign minister colleagues."[11] Secretary Powell's representative advised the Department in 2015 that he did not retain those emails or make printed copies.[12] Secretary Powell has also publicly stated that he generally sent emails to his staff via their State Department email addresses but that he personally does not know whether the Department captured those emails on its servers.[13]

Secretary Clinton employed a personal email system to conduct business during her tenure in the United States Senate and her 2008 Presidential campaign. She continued to use personal email throughout her term as Secretary, relying on an account maintained on a private server, predominantly through mobile devices. Throughout Secretary Clinton's tenure, the server was located in her New York residence.[14]

---

[8] 44 U.S.C. § 3101. The FAM assigns these recordkeeping responsibilities to officials within the Bureau of Administration. 1 FAM 214 (May 1, 2009); 1 FAM 214.2 (November 25, 1998); 1 FAM 216.4 (January 17, 1997).

[9] GAO, *National Archives and Records Administration: Oversight and Management Improvements Initiated, but More Action Needed* (GAO-11-15, October 5, 2010).

[10] Letter from Margaret P. Grafeld, Deputy Assistant Secretary for Global Information Systems, Bureau of Administration, U.S. Department of State, to Paul M. Wester, Jr., Chief Records Officer for the U.S. Government, NARA (April 2, 2015) [hereinafter Grafeld Letter].

[11] Colin Powell, *It Worked For Me: In Life and Leadership* 109 (2012).

[12] Grafeld Letter. Secretary Powell did not provide his emails to the Department in any form.

[13] ABC News, *This Week Transcript: Former Secretary of State Colin Powell* (March 5, 2015), available at http://abcnews.go.com/Politics/week-transcript-secretary-state-colin-powell/story?id=29463658.

[14] A March 17, 2009 memorandum prepared by S/ES-IRM staff regarding communications equipment in the Secretary's New York residence identified a server located in the basement.

In December 2014, in response to Department requests, Secretary Clinton produced to the Department from her personal email account approximately 55,000 hard-copy pages, representing approximately 30,000 emails that she believed related to official business. In a letter to the Department, her representative stated that it was the Secretary's practice to email Department officials at their government email accounts on matters pertaining to the conduct of government business. Accordingly, the representative asserted, to the extent that the Department retained records of government email accounts, the Department already had records of the Secretary's email preserved within its recordkeeping systems.[15]

PRESERVATION REQUIREMENTS HAVE GENERALLY REMAINED CONSISTENT AS LAWS AND POLICIES RELATED TO THE USE OF EMAILS HAVE EVOLVED

The requirement to manage and preserve emails containing Federal records has remained consistent since at least 1995, though specific policies and guidance related to retention methods have evolved over time. In general, the Federal Records Act requires appropriate management, including preservation, of records containing adequate and proper documentation of the "organization, functions, policies, decisions, procedures, and essential transactions of the agency."[16] Although emails were not explicitly mentioned in the Federal Records Act or FAM until the mid-1990s, the law has stated since 1943 that a document can constitute a record "regardless of physical form or characteristics."[17]

NARA promulgates regulations providing guidance to agencies on implementation of the Federal Records Act and recordkeeping obligations more generally.[18] Since 1990, the regulations issued by NARA have explained that the medium of the record may be "paper, film, disk, or other physical type or form" and that the method of recording may be "manual, mechanical, photographic, electronic, or any other combination of these or other technologies."[19] These regulations also have stated that a record can be made "by agency personnel in the course of their official duties, regardless of the method(s) or the medium involved."[20] See Appendix A for a compilation of preservation laws and policies that were in effect during the tenures of each Secretary, from Secretary Albright through Secretary Kerry. Figure 1 shows the evolution of management and preservation requirements related to emails containing Federal records.

[15] Letter from Cheryl Mills, cdmills Group, to Patrick F. Kennedy, Under Secretary of State for Management (December 5, 2014).

[16] 44 U.S.C. § 3101.

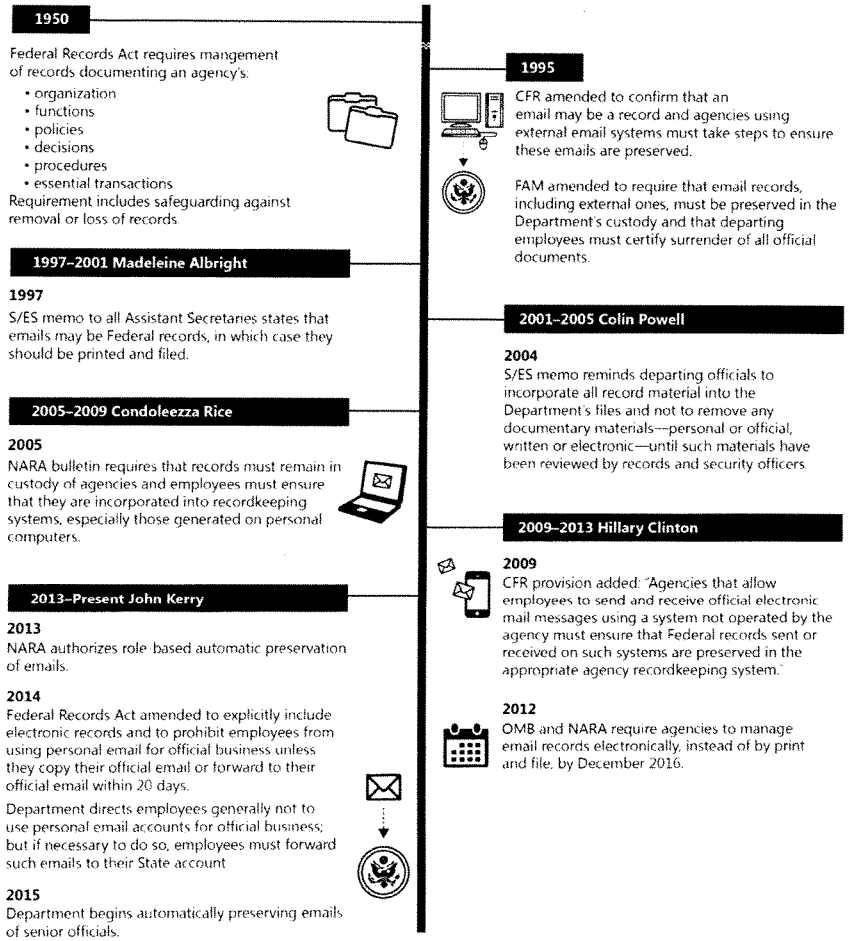
[17] H.R. 2943, Records Disposal Act of 1943, 57 Stat. 380 (July 7, 1943).

[18] 44 U.S.C. § 2904.

[19] 36 C.F.R. § 1222.12(b)(2) (1990).

[20] 36 C.F.R. § 1222.12(b)(3) (1990).

Figure 1: Timeline of Selected Records Management Requirements and Policies



Source: OIG analysis of laws and policies.

Email Records Equivalent to Other Records: In 1995, NARA amended the Code of Federal Regulations to confirm that "messages created or received on electronic mail systems may meet the definition of record."[21] The regulations also referenced the use of electronic communications systems external to the Government, indicating that "agencies with access to external electronic mail systems shall ensure that Federal records sent or received on these systems are preserved in the appropriate recordkeeping system."[22] A recordkeeping system is a manual or electronic system that captures, organizes, and categorizes records to facilitate their preservation, retrieval, use, and disposition.[23] The FAM adopted similar requirements in 1995, by providing in pertinent part that:

> all employees must be aware that some of the variety of the messages being exchanged on email are important to the Department and must be preserved; such messages are considered Federal records under the law.[24]

The FAM also included examples of emails that could constitute Federal records, including those providing key substantive comments on a draft action memorandum, documenting significant Department decisions and commitments reached orally, and conveying information of value on important Department activities.[25] The Department has frequently reminded employees of this requirement, including through a November 2009 announcement to all employees that noted that Federal records can be found in "any media, including email, instant messages, social media, etc."[26] However, the Department believes that the majority of the millions of emails sent to and from Department employees each year are non-permanent records with no long-term value.

In 2014, Congress amended the Federal Records Act explicitly to define Federal records to include "information created, manipulated, communicated, or stored in digital or electronic form."[27]

Methods of Preservation: According to NARA regulations, an agency "must ensure that procedures, directives and other issuances ... include recordkeeping requirements for records in all media, including those records created or received on electronic mail systems."[28] These recordkeeping requirements include identifying specific categories of records to be maintained

---

[21] 36 C.F.R. § 1222.34(e) (1995).

[22] 36 C.F.R. § 1222.24(a)(4) (1995).

[23] 36 C.F.R. § 1220.18 (2009).

[24] 5 FAM 443.1(c) (October 30, 1995).

[25] 5 FAM 443.2(d) (October 30, 1995).

[26] *See, e.g.*, 09 STATE 120561; Department of State, Records Management Responsibilities, Announcement No. 2009_11_125, November 23, 2009.

[27] Presidential and Federal Records Act Amendments of 2014, Pub. L. No: 113-187, 128 Stat. 2003 (November 26, 2014) (amending 44 U.S.C. § 3301(a)).

[28] 36 C.F.R. § 1222.24 (October 2, 2009).

by agency personnel. Such maintenance includes ensuring that complete records are filed or otherwise identified and preserved, records can be readily found when needed, and permanent and temporary records are physically segregated from each other (or, for electronic records, segregable). Guidance issued by both NARA and the Department emphasize that every employee has records management responsibilities and must make and preserve records according to the law and Department policy.[29]

At the Department, compliance with this regulation and preservation of emails that constitute Federal records can be accomplished in one of three ways: print and file; incorporation into the State Messaging and Archive Retrieval Toolset (SMART); or the use of the NARA-approved Capstone program for capturing the emails of designated senior officials. Since 1995, the FAM has instructed employees, "until technology allowing archival capabilities for long-term electronic storage and retrieval of E-mail messages is available and installed," emails warranting preservation as records must be printed out and filed with related Department records.[30] NARA regulations codified in 2009 also specified that agencies must not use an electronic mail system to store the recordkeeping copy of electronic mail messages identified as Federal records unless that system contains specific features.[31] However, according to the Department, its technology has "lagged behind" this mandate.

---

[29] 5 FAM 414.8 (September 17, 2004). The prior version was located in 5 FAM 413.10 (October 30, 1995). *See also*, NARA, Frequently Asked Questions about Records Management in General, available at: http://www.archives.gov/records-mgmt/faqs/general.html#responsibility (January 20, 2001) (stating that "Federal employees are responsible for making and keeping records of their work.").

[30] 5 FAM 443.3 (October 30, 1995). S/ES-IRM reported to OIG that it has preserved email files numbering in the thousands for selected senior officials dating back at least as far as Secretary Powell's administration, although OIG found that these files are maintained in a format that makes them almost impossible to review or use.

[31] 36 C.F.R. § 1236.22 (2009). These required features are specified in 36 C.F.R. § 1236.20(b) as follows:

> (a) General. Agencies must use electronic or paper recordkeeping systems or a combination of those systems, depending on their business needs, for managing their records. Transitory email may be managed as specified in § 1236.22(c).
>
> (b) Electronic recordkeeping. Recordkeeping functionality may be built into the electronic information system or records can be transferred to an electronic recordkeeping repository, such as a DoD-5015.2 STD-certified product. The following functionalities are necessary for electronic recordkeeping:
>
> > (1) Declare records. Assign unique identifiers to records.
> >
> > (2) Capture records. Import records from other sources, manually enter records into the system, or link records to other systems.
> >
> > (3) Organize records. Associate with an approved records schedule and disposition instruction.
> >
> > (4) Maintain records security. Prevent the unauthorized access, modification, or deletion of declared records, and ensure that appropriate audit trails are in place to track use of the records.
> >
> > (5) Manage access and retrieval. Establish the appropriate rights for users to access the records and facilitate the search and retrieval of records.
> >
> > (6) Preserve records. Ensure that all records in the system are retrievable and usable for as long as needed to conduct agency business and to meet NARA-approved dispositions. Agencies must develop procedures to enable the migration of records and their associated metadata to new storage media or formats in order to avoid loss due to media decay or technology obsolescence.

In 2009, IRM introduced SMART throughout the Department, enabling employees to preserve a record copy of emails through their Department email accounts without having to print and file them.[32] However, the Office of the Secretary elected not to use SMART to preserve emails, in part because of concerns that the system would allow overly broad access to sensitive materials. As a result, printing and filing remained the only method by which emails could properly be preserved within the Office of the Secretary in full compliance with existing FAM guidance.

In August 2012, OMB and NARA issued a memorandum requiring agencies to eliminate paper recordkeeping and manage all email records in an electronic format by December 31, 2016.[33] Subsequently, in August 2013, NARA published a bulletin authorizing agencies to use the Capstone approach to manage emails based upon the sender or recipient's role within the agency (rather than the content of the email), which "allows for the capture of records that should be preserved as permanent from the accounts of officials at or near the top of an agency or an organizational subcomponent."[34] In February 2015, S/ES began retaining the emails of senior Department officials within its purview using the Capstone approach, a practice that was broadened to approximately 200 senior officials across the Department in September 2015.[35] However, if an employee is not a senior official under Capstone, he or she would still be responsible for preserving emails in an appropriate agency recordkeeping system, such as through the use of SMART or printing and filing.

Requirements for Email Records in Personal Accounts: As previously stated, documents can qualify as Federal records regardless of the location, method of creation, or the medium involved. Consequently, records management requirements have always applied to emails

---

(7) Execute disposition. Identify and effect the transfer of permanent records to NARA based on approved records schedules. Identify and delete temporary records that are eligible for disposal. Apply records hold or freeze on disposition when required.

(c) Backup systems. System and file backup processes and media do not provide the appropriate recordkeeping functionalities and must not be used as the agency electronic recordkeeping system.

[32] Prior OIG reports have observed that that use of the SMART system to create record emails has varied widely across Department offices. OIG, *Review of State Messaging and Archive Retrieval Toolset and Record Email* (ISP-I-15-15, March 2015) and OIG, *Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services* (ISP-I-12-54, September 2012).

[33] OMB and NARA, *Memorandum for The Heads of Executive Departments and Agencies and Independent Agencies: Managing Government Records Directive* (OMB Memorandum M-12-18) (August 24, 2012).

[34] NARA, *Guidance on a New Approach to Managing Email Records*, Bulletin No. 2013-02 (August 29, 2013), available at https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html.

[35] On January 29, 2015, the Executive Secretary notified the covered officials in the offices of the Secretary (S), the Deputy Secretaries of State (D), the Under Secretary for Political Affairs (P), and the Counselor of the Department (C) that on February 1, 2015, S/ES-IRM would begin permanently retaining all email activity in their State Department accounts. This notice also stated: "You should not use your private email accounts (e.g., Gmail) for official business." Later in 2015, the Under Secretary for Management notified all Assistant Secretaries and equivalents and Principal Deputies that all their email will be permanently stored and indexed beginning September 1, 2015. See *Memorandum To All Assistant Secretaries, Assistant Secretary Equivalents, And Principal Deputies: Email Retention* (July 29, 2015).

exchanged on personal email accounts, provided their content meets the definition of a record. In 2004, NARA issued a bulletin noting that officials and employees "must know how to ensure that records are incorporated into files or electronic recordkeeping systems, especially records that were generated electronically on personal computers." In 2009, NARA amended its regulations explicitly to address official emails on personal accounts:

> Agencies that allow employees to send and receive official electronic mail messages using a system not operated by the agency must ensure that Federal records sent or received on such systems are preserved in the appropriate agency recordkeeping system.[36]

In the 2014 amendments to the Federal Records Act, Congress added a provision prohibiting agency employees from creating or sending a record using "a non-official electronic messaging account" unless they copy their official electronic messaging account in the original creation or transmission of the record or forward a complete copy of the record to their official electronic messaging account within 20 days.[37] Shortly before the enactment of the 2014 amendments, the Department issued an interim directive with similar requirements[38] and subsequently updated the FAM in October 2015 as follows:

> Under the Presidential and Federal Records Act Amendments of 2014, employees are prohibited from creating or sending a record using a non-official email account unless the employee (1) copies the employee's official email account in the original creation or transmission, or (2) forwards a complete copy of record (including any attachments) to the employee's official email account not later than 20 days after the original creation or transmission....The U.S. National Archives and Records Administration has advised that "personal accounts should only be used in exceptional circumstances." Therefore, Department employees are discouraged from using private email accounts (e.g., Gmail, AOL, Hotmail, etc.) for official business. However, in those very limited circumstances when it becomes necessary to do so, the email messages covering official business sent from or received in a personal account must be captured and managed in a Department email system in a manner described above in accordance with the Presidential and Federal Records Act Amendments of 2014. If an employee has any emails (regardless of age) on his or her private email account(s) that have not already been forwarded to the employee's official email account, then such emails need to be forwarded to the employee's state.gov account as soon as possible. Employees are reminded that private email accounts should not be used to transmit or receive classified information.[39]

---

[36] 36 C.F.R. § 1236.22(b).

[37] 44 U.S.C. § 2911(a).

[38] Department of State, *A Message from Under Secretary for Management Patrick F. Kennedy regarding State Department Records Responsibilities and Policy*, Announcement No. 2014_10_115, October 17, 2014.

[39] 5 FAM 443.7 (October 23, 2015). Furthermore, the Consolidated Appropriations Act of 2016, which became Public Law 114-113 on December 18, 2015, requires, at Section 7077, that the Department update policies and directives needed to comply with Federal statutes, regulations, and presidential executive orders and memoranda concerning

However, forwarding to or copying an employee's official email account alone is not sufficient to fully meet records management requirements unless an employee's email is being captured under the Capstone approach. If such an email qualifies as a record, employees are still responsible for preserving it in an appropriate agency recordkeeping system, such as through the use of SMART or printing and filing.

Safeguards for Loss or Removal of Records: Both the Federal Records Act and NARA regulations also focus on preventing the removal, loss, or alienation of Federal records. The Act requires the head of each agency to establish safeguards against the removal or loss of records, including making it known to officials and employees of the agency (1) that records in the custody of the agency are not to be alienated or destroyed and (2) the penalties provided by law for the unlawful removal or destruction of records.[40] Although the FAM itself does not contain any explicit administrative penalties for removal or destruction of records, it does advise employees that such penalties exist and cites the Federal Records Act for this assertion.[41]

NARA regulations require each agency to have procedures to ensure that departing officials and employees do not remove Federal records from agency custody.[42] The Department has implemented these requirements through various FAM and FAH provisions that prohibit employees from removing, retiring, transferring, or destroying Department records; prohibit departing employees from removing any records; require each departing employee to sign a separation statement certifying that he or she has surrendered all documentation related to the official business of the Government; and require a review of documents proposed for removal by a departing employee.[43] For example, since 1982, the Department has given the

---

the preservation of all records made or received in the conduct of official business, including record emails, instant messaging, and other online tools. The Act also required the Department to direct departing employees that their records belong to the Federal government and to report within 30 days on the steps required to implement the recommendations issued by OIG in the March 2015 Review of State Messaging and Archive Retrieval Toolset and Record Email (ISP-1-15-15) and any recommendations from the OIG review of the records management practices of the Department of State. Section 7077 also contains a prohibition from the use of certain appropriated funds to support the use or establishment of email accounts or email servers created outside the .gov domain or not fitted for automated records management as part of a Federal government records management program in contravention of the Presidential and Federal Records Act Amendments of 2014 and a provision for withholding $10,000,000 from the Capital Investment Fund until the records management reports required under Section 7077 are submitted to Congress.

[40] 44 U.S.C. § 3105.

[41] 5 FAM 413(a)(6) (September 17, 2004). NARA's regulations interpreting the Federal Records Act refer to the criminal penalties in 18 U.S.C. §§ 641, 2071, but do not cite to any administrative penalties. 36 C.F.R. § 1230.12.

[42] 36 C.F.R. § 1222.24(a)(6) (October 2, 2009).

[43] 5 FAM 431.5(d) (July 31, 2012); 5 FAM 432.4(d) (July 31, 2012); 5 FAM 414.7 (June 19, 2015); 12 FAM 564.4 (July 10, 2015); 5 FAH-4 H-217.2 (August 13, 2008). These are the most current versions of these provisions, but the requirements have existed at least since 1995. *See also* 5 FAH-4 H-218a (April 15, 1997). For related discussions of agency responsibilities concerning removal of agency documents by senior officials upon departure, see also GAO, *Federal Records: Removal of Agency Documents by Senior Officials Upon Leaving Office* (GAO/GGD-89-91, July 1989), and GAO, *Document Removal by Agency Heads Needs Independent Oversight* (GAO/GGD-91-117, August 1991).

responsibility to the management section of each bureau, office, or post to ensure that every departing employee has signed a separation statement (form DS-109) that includes the following certification: "I have surrendered to responsible officials all unclassified documents and papers relating to the official business of the Government acquired by me while in the employ of the Department."[44] Numerous Department cables and announcements have emphasized the responsibility of every employee to sign a separation statement before she or he departs.[45]

Since 2004, both the Department and NARA have issued multiple notices emphasizing the need to preserve emails that constitute Federal records and to surrender all Federal records prior to departing government employment.[46] These include an August 2004 memorandum from the Executive Secretary that reminded departing officials not to remove any documentary materials, whether personal or official and whether in written or electronic form, until such materials have been reviewed by records and security officers. The memorandum also required departing officials to ensure that all record material they possess is incorporated in the Department's official files. The Department reiterated this guidance in April, June, and October 2008.[47] S/ES conducts annual workshops with the Agency Records Officer on records management for departing senior officials and their staffs. Such workshops were held in February 2007, September 2008, June 2009, April 2010, October 2011, October 2012, October 2013, October 2014, and June 2015.

---

[44] 5 FAM 417.2 (March 16, 1982); 5 FAM 413.9 (October 30, 1995); 5 FAM 414.7 (September 17, 2004).

[45] *See, e.g., Procedures for the Removal of Personal Papers and Non-Record Material – 5 FAM 400, 5 FAH-4,* Announcement No. 2000_01_021, January 14, 2000; *Procedures for the Removal of Personal Papers and Non-Record Material,* Announcement No. 2005_02_017, February 3, 2005; 05 STATE 00018818 (February 1, 2005); 14 STATE 56010 (May 09, 2014).

[46] *See, e.g.,* NARA, *Protecting Federal records and other documentary materials from unauthorized removal,* Bulletin No. 2005-03 (December 22, 2004); NARA, *NARA Guidance for Implementing Section 207(e) of the E-Government Act of 2002,* Bulletin No. 2006-02 (December 15, 2005); Department of State, Records Management Procedures, Announcement No. 2007_02_147, February 28, 2007; Department of State, Preserving Electronic Message (E-mail) Records, Announcement No. 2009_06_090, June 17, 2009; 14 STATE 111506 (September 15, 2014); Department of State, *Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material,* Announcement No. 2008_04_089, April 17, 2008; Department of State, *Reminder – Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material,* Announcement No. 2008_06_095, June 16, 2008; Department of State, *Reminder – Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material,* Announcement No. 2008_10_087, October 16, 2008 ("The willful and unlawful removal or destruction of records is punishable by a fine or imprisonment of up to three years, or both (18 U.S.C. § 2071)."); 09 STATE 120561 (November 23, 2009); Department of State, *Records Management Responsibilities,* Announcement No. 2009_11_125, November 23, 2009; NARA, *Continuing Agency Responsibilities for Scheduling Electronic Records,* Bulletin No. 2010-02 (February 5, 2010); Department of State, *A Message from Under Secretary for Management Patrick F. Kennedy regarding State Department Records Responsibilities and Policy,* Announcement No. 2014_10_115, October 17, 2014.

[47] Memorandum from Karl Hoffman, Executive Secretary, to all Under Secretaries and Assistant Secretaries, *Refresher on Records Responsibilities and Review* (August 9, 2004).

MANAGEMENT WEAKNESSES CONTRIBUTE TO LOSS OF EMAIL RECORDS

As discussed above, the Federal Records Act and related NARA regulations impose records management responsibilities on both Federal agencies and individual employees. For agencies, these responsibilities include establishing "effective controls" to manage the creation, maintenance, use, and disposition of records in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government.[48] According to NARA, an effective records disposition program depends on scheduling[49] all records, regardless of location and regardless of physical form or characteristics (paper or electronic).[50] Therefore, agencies must implement a records maintenance program so that complete records are filed or otherwise identified and preserved, records can be readily found when needed, and permanent and temporary records are physically segregated or are segregable from each other.[51]

According to a 2010 U.S. Government Accountability Office (GAO) report, most agencies do not prioritize records management, as evidenced by lack of staff and budget resources, absence of up-to-date policies and procedures, lack of training, and lack of accountability.[52] In its most recent annual assessment of records management, NARA identified similar weaknesses across the Federal Government with regard to electronic records in particular. NARA reported that 80 percent of agencies had an elevated risk for the improper management of electronic records, reflecting serious challenges handling vast amounts of email, integrating records management functionality into electronic systems, and adapting to the changing technological and regulatory environments.[53]

In an effort to develop solutions to its own electronic records management challenges and to comply with NARA and OMB requirements, in 2013 the Department established the Electronic Records Management Working Group (ERMWG).[54] The Under Secretary for Management[55]

---

[48] 44 U.S.C. §§ 3101, 3102.

[49] A records schedule identifies records as either temporary or permanent. All records schedules must be approved by NARA. A records schedule provides mandatory instructions for the disposition of the records (including the transfer of permanent records and disposal of temporary records) when they are no longer needed by the agency. As part of the ongoing records life cycle, disposition should occur in the normal course of agency business. 44 U.S.C. §§ 3303, 3303a.

[50] *See* http://www.archives.gov/records-mgmt/publications/disposition-of-federal-records/chapter-2.html

[51] 36 C.F.R. § 1222.34.

[52] GAO, *Information Management: The Challenges of Managing Electronic Records* (GAO-10-838T, July 17, 2010).

[53] NARA, *Records Management Self-Assessment 2014* (November 6, 2015).

[54] The ERMWG is chaired by the Director of the Office of Management Policy, Rightsizing and Innovation, and its members include the Chief Information Officer (CIO) and representatives from L, IRM, and A.

[55] OMB and NARA Memorandum M-12-18, *Memorandum for The Heads of Executive Departments and Agencies and Independent Agencies: Managing Government Records Directive,* requires each agency to designate a Senior Agency Official (SAO) at the Assistant Secretary level or its equivalent with "direct responsibility for ensuring the department or agency efficiently and appropriately complies with all applicable records management statutes, regulations, and NARA policy, and the requirements of this Directive. The SAO must be located within the organization so as to make

approved recommendations submitted by the ERMWG, which included updating guidance on preserving senior officials' emails, developing a pilot program for the Capstone approach to record email, and directing IRM to perform a cost-benefit analysis of upgrading SMART as opposed to obtaining other solutions for preserving the emails of senior officials.[56]

In September 2015, Secretary Kerry named a former career Senior Foreign Service Officer as the Department's Transparency Coordinator. The Transparency Coordinator has been tasked with leading the Department's efforts in conjunction with the ERMWG to meet the President's Managing Government Records directive, responding to OIG's recommendations, and working with other agencies and the private sector to explore best practices and new technologies.

While these are positive steps, OIG identified multiple email and other electronic records management issues during the course of this evaluation. In its technical comments on this report, the Department noted that its budget has been declining over the past years and has not kept pace with inflation at a time when its national security mission is growing. According to the Department, it did request additional resources for records management for fiscal year 2017, but additional funding will still be needed to fully address its records management challenges.

Insufficient Oversight of the Recordkeeping Process: During the 20-year period covered by this evaluation, S/ES has had day-to-day responsibility for the Secretary of State's records management responsibilities, and it relies upon guidance and records schedules promulgated by the Bureau of Administration. The Bureau of Administration "plans, develops, implements, and evaluates programs, policies, rules, regulations, practices, and procedures on behalf of the Secretary to ensure compliance with the letter and spirit of relevant statutes, executive orders, and guidelines."[57] The Office of Information Programs and Services (IPS) is the component of the Bureau specifically tasked with issuing records guidance and overseeing records management efforts of the Department. Upon request, IPS reviews the records management practices of Department offices. The Acting Co-Director of IPS currently serves as the Agency Records Officer with program management responsibility for all records Department-wide throughout their life cycle (creation, acquisition, maintenance, use, and disposition). IPS has provided briefings, in conjunction with S/ES, to Office of the Secretary staff and has issued Department-wide notices and cables about records retention requirements, some of which included requirements to save email records, including records contained in personal emails. According to the FAM, the Agency Records Officer is "responsible for seeing that the Department and all of its component elements in the United States and abroad are in compliance with Federal records statutes and

---

adjustments to agency practices, personnel, and funding as may be necessary to ensure compliance and support the business needs of the department or agency." The Under Secretary for Management has served as the Department's SAO since 2012. Action Memo for the Secretary, *Designating A Senior Agency Official (SAO) for Managing Government Records* (November 27, 2012).

[56] ERMWG, *Action Memo for Under Secretary Kennedy: Preserving Electronically Senior Officials' Record Email Messages* (August 22, 2014).

[57] 5 FAM 414.3 (June 9, 2009).

regulations,"[58] yet IPS has not reviewed Office of the Secretary records retention practices during the current or past four Secretaries' terms.

Although NARA is responsible for conducting inspections or surveys of agencies' records and records management programs and practices,[59] it last reviewed the Office of the Secretary's records retention practices in 1991–a quarter century ago. Beginning in 2009, NARA has relied on annual records management self-assessments and periodic reports from the Department to gauge the need to conduct formal inspections. The Department's last two self-assessments did not highlight any deficiencies.

Print and File Requirements Not Enforced: S/ES staff have provided numerous trainings for the Office of the Secretary on records preservation responsibilities and the requirement to print and file email records. However, S/ES staff told OIG that employees in the Office of the Secretary have printed and filed such emails only sporadically. In its discussions with OIG, NARA stated that this lack of compliance exists across the government. Although the Department is aware of the failure to print and file, the FAM contains no explicit penalties for lack of compliance, and the Department has never proposed discipline against an employee for failure to comply. OIG identified one email exchange occurring shortly before Secretary Clinton joined the Department that demonstrated a reluctance to communicate the requirement to incoming staff. In the exchange, records officials within the Bureau of Administration wondered whether there was an electronic method that could be used to capture the Secretary's emails because they were "not comfortable" advising the new administration to print and file email records.

Limited Ability To Retrieve Email Records: Even when emails are printed and filed, they are generally not inventoried or indexed and are therefore difficult to retrieve. As an illustration, almost 3,000 boxes, each filled with hundreds of pages of documents, would have to be reviewed manually, on a page-by-page basis, in order to identify and review all printed and filed emails from the Office of the Secretary since 1997. To help alleviate this problem, the Office of the Secretary could have adopted an electronic email management system in 2009 with the introduction of SMART. SMART allows users to designate specific emails sent or received through the Department's email system as record emails; other SMART users can search for and access record emails, depending on the access controls set by the individual who originally saved the email. However, prior OIG reports have repeatedly found that Department employees enter relatively few of their emails into the SMART system and that compliance varies greatly across bureaus, in part because of perceptions by Department employees that SMART is not intuitive, is difficult to use, and has some technical problems.[60]

---

[58] 5 FAM 414.2 (June 9, 2009).

[59] 44 U.S.C. § 2906. For an in-depth assessment of NARA's oversight practices, see GAO, *National Archives and Records Administration: Oversight and Management Improvements Initiated, but More Action Needed* (GAO-11-15, October 2010).

[60] OIG, *Review of State Messaging and Archive Retrieval Toolset and Record Email* (ISP-I-15-15, March 2015) and OIG, *Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services*

In 2015, the Department began permanently retaining the emails of approximately 200 senior officials pursuant to the Capstone approach discussed previously. The Department also plans to purchase an off-the-shelf product to electronically manage its emails in keeping with OMB's and NARA's requirement that it do so by December 2016.[61] This product will be adapted to Department requirements to include an interface that requires users to determine the record value and sensitivity of an email with one click and an auto-tagging feature that will allow emails to be stored according to disposition schedules. The new system will also be able to process legacy email files, such as the Personal Storage Table (.pst) files of departed officials.[62] In addition, the Department expects that the product will improve the Department's ability to perform more comprehensive email searches.

No Inventory of Archived Electronic Files: The S/ES Office of Information Resources Management (S/ES-IRM), the unit that handles information technology for the Office of the Secretary, reported to OIG that it has maintained electronic copies of email records for selected senior officials dating back as far as Secretary Powell's tenure. These records consist of thousands of electronic files, principally saved as .pst files. During OIG's fieldwork, S/ES-IRM did not have an inventory of the .pst or other electronic files that consistently identified the former email account holder. However, in early 2016, S/ES-IRM began to create a comprehensive inventory of these files.[63]

Unavailable or Inaccessible Electronic Files: When OIG requested specific .pst files, it encountered difficulties in obtaining and accessing those files. S/ES-IRM was unable to produce all of the .pst files OIG requested, and some of the requested files were corrupted and their recovery required considerable resources. Some .pst files were password protected, and staff did not know the passwords needed to open those files. Other files contained no data at all. Of the .pst files OIG was able to review, many were incomplete in that they did not span the particular employee's entire term of service, were mislabeled, or were missing key files such as populated sent or inbox folders. According to S/ES-IRM, as part of the inventory process currently underway, it is moving all .pst files in its possession onto servers and clearly labeling them.

Failure To Transfer Email Records to IPS: All Department offices are required to retire, or transfer, records to IPS in accordance with the Department's records disposition schedules.[64] For records

---

(ISP-I-12-54, September 2012). As noted previously, the Office of the Secretary did not implement SMART in part because of concerns the system would allow users to access highly sensitive records.

[61] On November 30, 2015, the Department issued a Request for Information to determine the capabilities of the private sector to provide and support a system to satisfy recordkeeping requirements involving emails by December 31, 2016. Department of State Email Management, Solicitation No. SAQMMA16I0008 (November 30, 2015).

[62] The term ".pst" refers to the format used to store copies of email messages, calendar events, and other items within Microsoft software.

[63] According to NARA regulations, creating .pst files is not an approved method of preserving Federal records, because .pst files do not have the required controls of an electronic records system. 36 C.F.R. § 1236.10.

[64] 5 FAM 433 (July 31, 2012).

specific to the Office of the Secretary, the relevant schedules require transferring most records to IPS at the end of the tenure of the Secretary.[65] S/ES has regularly retired paper copies of such records throughout the Secretaries' terms. However, S/ES has not consistently retired electronic email records. In April 2015, S/ES retired nine lots of electronic records containing approximately 16 gigabytes of data, consisting of emails, memoranda, travel records, and administrative documents from the tenures of former Secretaries Powell, Rice, and Clinton. However, the only email accounts included in this material were those of six of former Secretary Powell's staff and two of former Secretary Rice's staff. No email accounts from Secretary Clinton's staff were in the retired material.

In addition to retiring records in accordance with disposition schedules, offices must comply with Department policy requiring them to electronically capture the email accounts of selected senior officials upon their departure. A January 2009 memorandum from the Under Secretary for Management required Executive Directors and Management Officers to notify their system administrators of the departure of Presidential and political appointees and directed the administrators to copy the email accounts of those officials to two sets of CDs. The memorandum instructed the office to keep one of the CDs and send the other to IPS for records preservation.[66] The memorandum included an attachment identifying all officials who were subject to these requirements, including 50 officials from the offices under the purview of S/ES.[67] In August 2014, the Under Secretary sent another memorandum reiterating the requirement to electronically capture the email accounts of senior officials and broadening the list of officials subject to the requirement.[68] The Director of S/ES-IRM told OIG that S/ES complied with this requirement by creating .pst files covering the email accounts of the specified officials upon their departure. However, S/ES has never sent any CDs to IPS. In its most recent self-assessments of its records management, the Department stated that it has "established a procedure for departing officials to have their emails sent to the Department's Records Officer for preservation," but it failed to note that it has not complied with that procedure for the most senior officials in the organization.[69]

Failure To Follow Department Separation Processes: As noted previously, NARA regulations require each agency to adopt procedures to ensure that departing officials and employees do

[65] The schedule for records specific to the Office of the Secretary is available at: https://foia.state.gov/_docs/RecordsDisposition/A-01.pdf

[66] Under Secretary Patrick F. Kennedy, *Memorandum for All Under Secretaries, Assistant Secretaries, Executive Directors and Post Management Officers: Preserving Electronically the Email of Senior Officials upon their Departure* (January 2009).

[67] The list of officials included the Secretary, Deputy Secretaries, Counselor, Chief of Protocol, Special Assistants to the Secretary, the Chief of Staff, and the Deputy Chief of Staff.

[68] Under Secretary Patrick F. Kennedy, *Memorandum: Senior Officials' Records Management Responsibilities* (August 28, 2014).

[69] *See, e.g.*, Department of State, *Senior Agency Official for Records Management FY 2014 Annual Report Template* (February 5, 2015).

not remove Federal records from agency custody.[70] The Department has implemented these requirements through various FAM provisions, including one that requires every departing employee to sign a separation statement (DS-109) certifying that he or she has surrendered all documentation related to the official business of the Government.[71] This function is handled for the Office of the Secretary by the Office of the S/ES Executive Director (S/ES-EX). However, S/ES-EX told OIG that, as the head of the agency, the Secretary is not asked to follow the exit process. Consequently, Secretaries Albright, Powell, Rice, and Clinton did not sign a DS-109 at the end of their tenures.

Notwithstanding the failure to adhere to separation requirements, all departing Secretaries of State from Secretary Albright on have followed the procedures governing the removal of personal papers. The FAH specifies that departing officials who wish to remove any documents must prepare an inventory of these personal papers and any non-record materials for review by Department officials.[72] Once the reviewing official is satisfied that removal of the documents would comply with Federal law and regulations, the reviewing official completes and signs Form DS-1904 (Authorization for the Removal of Personal Papers and Non-Record Materials). As the form itself notes, this process is especially important to ensure that the "the official records of the Department" are not "diminish[ed]." S/ES officials signed DS-1904 forms after the departures of Secretaries Albright, Powell, Rice, and Clinton. OIG reviewed the completed forms for these four Secretaries; none listed email as proposed for removal. However, in contrast to the Form DS-109, the DS-1904 does not impose a specific requirement to surrender documents.

Failure To Notify NARA of Loss of Records: Federal laws and regulations require an agency head to notify NARA of any actual, impending, or threatened unlawful removal or loss of agency records.[73] Although numerous senior officials emailed Secretaries Powell and Clinton on their personal email accounts to conduct official business, the Department did not make a formal request to the former Secretaries for the Federal records contained within these personal accounts until October and November 2014.[74] The Department also did not promptly notify NARA about the potential loss of records.[75] NARA officials told OIG they learned of former

[70] 36 C.F.R. § 1222.24 (2009).

[71] 12 FAM 564.4 (July 10, 2015); 5 FAM 414.7 (June 9, 2015). These are the most current versions of these provisions, but the requirements have existed since at least 1995.

[72] 5 FAH-4 H-217.2 (August 13, 2008).

[73] 44 U.S.C. § 3106; 36 C.F.R. § 1230.14.

[74] In letters to the respective representatives of Secretaries Powell and Clinton, the Department asked that, should they "be aware or become aware in the future of a federal record, such as an email sent or received on a personal email account while serving as Secretary of State, that a copy of this record be made available to the Department." In addition, the Department advised that they should "note that diverse Department records are subject to various disposition schedules, with most Secretary of State records retained permanently." Therefore, the Department asked that "a record be provided to the Department if there is reason to believe that it may not otherwise be preserved in the Department recordkeeping system."

[75] In May 2014, the Department undertook efforts to recover potential Federal records from Secretary Clinton. Thereafter, in July 2014, senior officials met with former members of Secretary Clinton's immediate staff, who were then acting as Secretary Clinton's representatives. At the meeting, her representative indicated that her practice of

Secretary Clinton's email practices through media accounts in March 2015. Immediately thereafter, NARA requested that the Department provide a report concerning "the potential alienation of Federal email records" created by former Secretary Clinton and actions taken to recover such records.[76]

In April 2015, the Department informed NARA of the information it obtained from the former Secretaries concerning their email records.[77] NARA subsequently requested additional information about how the Department implements records management requirements with regard to senior officials.[78] NARA also requested that the Department contact the Internet service providers (ISPs) associated with the personal accounts of Secretaries Powell and Clinton to inquire if "it is still possible to retrieve the email records that may still be present on their servers." The Under Secretary for Management subsequently informed NARA that the Department sent letters to the representatives of Powell and Clinton conveying this request.[79]

Well before the disclosure in April 2015, Department officials discussed in 2011 whether there was an obligation to search personal email accounts for Federal records.[80] In 2013, this issue arose again. Specifically, in early June 2013, Department staff participating in the review of potential material for production to congressional committees examining the September 2012 Benghazi attack discovered emails sent by the former Policy Planning Director via his Department email account to a personal email address associated with Secretary Clinton. In ensuing weeks, partly as a result of the staff's discovery, Department senior officials discussed

---

using a personal account was based on Secretary Powell's similar use, but Department staff instructed Clinton's representatives to provide the Department with any Federal records transmitted through her personal system. On August 22, 2014, Secretary Clinton's former Chief of Staff and then-representative advised Department leadership that hard copies of Secretary Clinton emails containing responsive information would be provided but that, given the volume of emails, it would take some time to produce. Subsequently, in October 2014, the Department began making formal, written requests to the representatives of Secretaries Albright, Powell, Rice and Clinton to produce any Federal records maintained in personal accounts. Secretary Clinton produced emails in hard copy form in December 2014. Thereafter, in March 2015, the Department made a similar request to four of Secretary Clinton's immediate staff. They produced email from their personal accounts during the summer of 2015.

[76] Letter from Paul M. Wester, Jr., Chief Records Officer for the U.S. Government, NARA, to Margaret P. Grafeld, Deputy Assistant Secretary for Global Information Systems, Bureau of Administration, U.S. Department of State (March 3, 2015).

[77] Grafeld Letter.

[78] Letter from Paul M. Wester, Jr., Chief Records Officer for the U.S. Government, NARA, to Margaret P. Grafeld, Deputy Assistant Secretary for Global Information Systems, Bureau of Administration, U.S. Department of State (July 2, 2015).

[79] Letter from Patrick F. Kennedy, Under Secretary of State for Management, to Laurence Brewer, Acting Chief Records Officer for the U.S. Government, NARA (November 6, 2015). Secretary Clinton responded to the Department that she has provided it with all official emails in her possession and pledged to provide any other record emails if they become available. As of May 2016, the Department has not received a response from Secretary Powell.

[80] This was prompted by a FOIA matter, in which a plaintiff inquired about a document it received showing that a staff assistant in the Office of the Secretary had received a work-related email on her personal account from someone who was not a Federal employee; the staff assistant had forwarded the email to her official account. This matter was ultimately resolved without further litigation.

the Department's obligations under the Federal Records Act in the context of personal email accounts. As discussed earlier in this report, laws and regulations did not prohibit employees from using their personal email accounts for the conduct of official Department business. However, email messages regarding official business sent to or from a personal email account fell within the scope of the Federal Records Act if their contents met the Act's definition of a record. OIG found that the Department took no action to notify NARA of a potential loss of records at any point in time.[81]

STAFF EMAIL USAGE AND COMPLIANCE WITH RECORDS MANAGEMENT REQUIREMENTS VARY

As part of this evaluation, OIG sought to examine whether staff in the Office of the Secretary complied with relevant email records management requirements, including those associated with the use of personal email accounts. However, OIG was unable to systematically assess the extent to which Secretaries Albright, Powell, Rice, Clinton, and Kerry and their immediate staff managed and preserved email records. In particular, OIG could not readily retrieve and analyze email records, in part because of the previously discussed weaknesses in the Department's records management processes. Although hard-copy and electronic email records dating back to Secretary Albright's tenure exist, these records have never been organized or indexed. For example, the Department could not immediately retrieve and make available for review specific email accounts identified and requested by OIG, which led to 2- to 3-month-long delays in obtaining the requested records. In addition, OIG was unable to reconstruct many events because of staff turnover and current employees' limited recollections of past events. These problems were compounded by the fact that multiple former Department employees and other individuals declined OIG requests for interviews, and OIG lacks the authority to compel anyone who is not a current Department employee to submit to interviews or to answer questions.

Moreover, OIG was unable to assess the degree to which Federal records sent though personal email accounts have been appropriately managed by Secretaries of State and their immediate staffs. Emails sent from the personal accounts of these individuals to other Department employees may or may not exist in the Department email accounts of the recipients, but OIG has limited ability to determine which accounts might contain these records unless the sender of the emails provides detailed information about the recipients. The Department currently lacks the resources and technical means to systematically review electronic files in its possession for records.

Despite these issues, OIG discovered anecdotal examples suggesting that Department staff have used personal email accounts to conduct official business, with wide variations among

[81] The current Deputy Secretary for Management and Resources, who during the summer of 2013 served as Counselor to the Department, told OIG that she recalled conversations with Secretary Kerry about email usage, but the conversations focused only on Secretary Kerry's practices. In his interview with OIG, Secretary Kerry reported that he was not involved in any of the discussions regarding Secretary Clinton's emails and that he first became aware of her exclusive use of a personal email account when an aide informed him around the time the information became public.

Secretaries and their immediate staff members. For instance, OIG reviewed the Department email accounts (.pst files) of senior Department employees who served on the immediate staffs of Secretary Powell and Secretary Rice between 2001 and 2008. Within these accounts, OIG identified more than 90 Department employees who periodically used personal email accounts to conduct official business, though OIG could not quantify the frequency of this use.

OIG also reviewed an S/ES-IRM report prepared in 2010 showing that more than 9,200 emails were sent within one week from S/ES servers to 16 web-based email domains, including gmail.com, hotmail.com, and att.net.[82] S/ES-IRM told OIG that it no longer has access to the tool used to generate this particular report. In another instance, in a June 3, 2011, email message to Secretary Clinton with the subject line "Google email hacking and woeful state of civilian technology," a former Director of Policy Planning wrote: "State's technology is so antiquated that NO ONE uses a State-issued laptop and even high officials routinely end up using their home email accounts to be able to get their work done quickly and effectively."

Notwithstanding the limitations on its ability to conduct a systematic evaluation, the information available allowed OIG to establish that email usage and compliance with statutory, regulatory, and Department requirements varied across the past five Secretaries' tenures. The practices of each Secretary and their immediate staff are discussed below.

Secretary Albright (January 23, 1997 – January 20, 2001): During Secretary Albright's tenure, desktop unclassified email and access to the Internet were not widely available to Department employees. OIG searched selected hard-copy records from her tenure and did not find any evidence to indicate that Secretary Albright used either Department or personal email accounts during that period. OIG additionally interviewed Secretary Albright and current and former Department staff, who further confirmed that she did not use email while serving as Secretary. In her interview with OIG, Secretary Albright noted that email use was still in its early stages when she became Secretary, and at the time she had no familiarity with the practice.

With regard to Secretary Albright's immediate staff, OIG did not find any emails that appeared to be to or from personal accounts and only found a few emails from staff Department accounts related to the Secretary's schedule. Staff responses on OIG questionnaires also identified minimal email usage–though two staff noted retaining emails on "Department servers."[83] These responses suggest staff may not have consistently complied with the preservation requirement to print and file emails containing Federal records.[84]

---

[82] Not all of these emails may indicate the use of personal email to conduct official business. Some of these emails could be communications with individuals outside the Department. Others could be communications by employees on personal matters, which is permissible under the Department's limited-use policy.

[83] OIG sent 13 questionnaires to former Secretary Albright's staff and received 8 responses, of which 2 were anonymous. None of the respondents reported having a personal email account while employed with the Department, and most did not acknowledge using a Department account. Two noted that they retained their emails on Department servers and one recalled receiving training on the topic of email preservation.

[84] 5 FAM 443.3 (October 30, 1995).

Secretary Powell (January 20, 2001 – January 26, 2005): During Secretary Powell's tenure, the Department introduced for the first time unclassified desktop email and access to the Internet on a system known as OpenNet, which remains in use to this day. Secretary Powell did not employ a Department email account, even after OpenNet's introduction. He has publicly written:

> To complement the official State Department computer in my office, I installed a laptop computer on a private line. My personal email account on the laptop allowed me direct access to anyone online. I started shooting emails to my principal assistants, to individual ambassadors, and increasingly to my foreign-minister colleagues ....[85]

OIG identified emails sent from and received by Secretary Powell's personal account in selected records associated with Secretary Powell. During his interview with OIG, Secretary Powell stated that he accessed the email account via his personal laptop computer in his office, while traveling, and at his residence, but not through a mobile device. His representative advised the Department that Secretary Powell "did not retain those emails or make printed copies."[86] Secretary Powell also stated that neither he nor his representatives took any specific measures to preserve Federal records in his email account. Secretary Powell's representative told OIG that she asked Department staff responsible for recordkeeping whether they needed to do anything to preserve the Secretary's emails prior to his departure, though she could not recall the names or titles of these staff. According to the representative, the Department staff responded that the Secretary's emails would be captured on Department servers because the Secretary had emailed other Department employees.

However, according to records management requirements and OIG's discussion with NARA, sending emails from a personal account to other employees at their Department accounts is not an appropriate method of preserving emails that constitute Federal records.[87] Guidance issued by both NARA and the Department emphasize that all employees have records management responsibilities and must make and preserve records that they send and receive.[88] Moreover, in keeping with NARA regulations,[89] the Department's policies specifically acknowledged that its email system at the time did not contain features necessary for long-term preservation of Federal records.[90] Therefore, Secretary Powell should have preserved any Federal records he

---

[85] Colin Powell, *It Worked for Me*, at 109 (2012).

[86] Grafeld Letter.

[87] 36 C.F.R. § 1234.24(b)(2) (August 28, 1995).

[88] 5 FAM 414.8 (September 17, 2004). The prior version was located at: 5 FAM 413.10 (October 30, 1995). *See also*, NARA, Frequently Asked Questions about Records Management in General, available at: http://www.archives.gov/records-mgmt/faqs/general.html#responsibility (January 20, 2001) (stating that "Federal employees are responsible for making and keeping records of their work.")

[89] 36 C.F.R. §1234.24(d) (August 28, 1995). In 2009, this provision was moved to 36 C.F.R. §1236.22(d) (October 2, 2009). It states, "Agencies must not use an electronic mail system to store the recordkeeping copy of electronic mail messages identified as Federal records unless that system" has certain listed attributes.

[90] As noted previously, Department guidance explained that messages must be printed and filed until "until technology allowing archival capabilities for long-term electronic storage and retrieval of E-mail records is available

created and received on his personal account by printing and filing those records with the related files in the Office of the Secretary.[91]

NARA agrees that the records should have been printed and filed but also told OIG that any effort to transfer such records to the Department would have mitigated the failure to preserve these records. At a minimum, Secretary Powell should have surrendered all emails sent from or received in his personal account that related to Department business. Because he did not do so at the time that he departed government service or at any time thereafter, Secretary Powell did not comply with Department policies that were implemented in accordance with the Federal Records Act. In an attempt to address this deficiency, NARA requested that the Department inquire with Secretary Powell's "internet service or email provider" to determine whether it is still possible to retrieve the email records that might remain on its servers.[92] The Under Secretary for Management subsequently informed NARA that the Department sent a letter to Secretary Powell's representative conveying this request.[93] As of May 2016, the Department had not received a response from Secretary Powell or his representative.

Members of Secretary Powell's immediate staff who responded to OIG questionnaires described minimal email usage overall—two staff recalled printing and filing emails in Department recordkeeping systems.[94] While the limited number of respondents also asserted they did not use personal email accounts for official business, OIG discovered some personal email usage for official business by Secretary Powell's staff through its own review of selected records.

Secretary Rice (January 26, 2005 – January 20, 2009): Secretary Rice and her representative advised the Department and OIG that the Secretary did not use either personal or Department email accounts for official business.[95] OIG searched selected records and did not find any evidence to indicate that the Secretary used such accounts during her tenure.

OIG received limited responses on questionnaires sent to former Secretary Rice's staff. Two staff recalled printing and filing emails, and only one acknowledged the use of personal email

---

and installed" that will preserve messages for "periods longer than current E-mail systems routinely maintain them." 5 FAM 443.3 (October 30, 1995).

[91] 5 FAM 443.3 (October 30, 1995).

[92] Letter from Paul M. Wester, Jr., Chief Records Officer for the U.S. Government, NARA, to Margaret P. Grafeld, Deputy Assistant Secretary for Global Information Systems, Bureau of Administration, U.S. Department of State (July 2, 2015).

[93] Letter from Patrick F. Kennedy, Under Secretary of State for Management, to Laurence Brewer, Acting Chief Records Officer for the U.S. Government, NARA (November 6, 2015).

[94] OIG sent 18 questionnaires to former Secretary Powell's staff and received 6 responses, of which one was anonymous. Two respondents stated they created records by printing copies of emails from their Department accounts and filing them into the Department's records system. One respondent recalled receiving records retention training.

[95] Grafeld Letter.

accounts for official business.[96] OIG reviewed hard-copy and electronic records of Secretary Rice's immediate staff and discovered that other staff who did not reply to the questionnaire did use personal email accounts to conduct official business.

Secretary Clinton (January 21, 2009 – February 1, 2013): Former Secretary Clinton did not use a Department email account and has acknowledged using an email account maintained on a private server for official business. As discussed above, in December 2014, her representative produced to the Department 55,000 hard-copy pages of documents, representing approximately 30,000 emails that could potentially constitute Federal records that she sent or received from April 2009 through early 2013. Secretary Clinton's representative asserted that, because the Secretary emailed Department officials at their government email accounts, the Department already had records of the Secretary's email preserved within its recordkeeping systems.[97]

As previously discussed, however, sending emails from a personal account to other employees at their Department accounts is not an appropriate method of preserving any such emails that would constitute a Federal record. Therefore, Secretary Clinton should have preserved any Federal records she created and received on her personal account by printing and filing those records with the related files in the Office of the Secretary.[98] At a minimum, Secretary Clinton should have surrendered all emails dealing with Department business before leaving government service and, because she did not do so, she did not comply with the Department's policies that were implemented in accordance with the Federal Records Act.

NARA agrees with the foregoing assessment but told OIG that Secretary Clinton's production of 55,000 pages of emails mitigated her failure to properly preserve emails that qualified as Federal records during her tenure and to surrender such records upon her departure. OIG concurs with NARA but also notes that Secretary Clinton's production was incomplete. For example, the Department and OIG both determined that the production included no email covering the first few months of Secretary Clinton's tenure—from January 21, 2009, to March 17, 2009, for received messages; and from January 21, 2009, to April 12, 2009, for sent messages. OIG discovered multiple instances in which Secretary Clinton's personal email account sent and received official business email during this period. For instance, the Department of Defense provided to OIG in September 2015 copies of 19 emails between Secretary Clinton and General David Petraeus on his official Department of Defense email account; these 19 emails were not in the Secretary's 55,000-page production. OIG also learned that the 55,000-page production did

[96] OIG sent 23 questionnaires to Secretary Rice's former staff and received 9 responses. Only one respondent reported using personal email accounts to conduct official business when "Department accounts were down or inaccessible." Two respondents said they printed emails and filed them into the Department's records systems; another said he believed IRM "backed up" all emails. One respondent stated she did not recall any specific instructions about retaining emails but assumed all emails were captured electronically.

[97] Letter from Cheryl Mills, cdmills Group, to Patrick F. Kennedy, Under Secretary of State for Management (December 5, 2014).

[98] 5 FAM 443.3 (October 30, 1995).

not contain some emails that an external contact not employed by the Department sent to Secretary Clinton regarding Department business. In an attempt to address these deficiencies, NARA requested that the Department inquire with Secretary Clinton's "internet service or email provider" to determine whether it is still possible to retrieve the email records that might remain on its servers.[99] The Department conveyed this request to Secretary Clinton's representative and on November 6, 2015, the Under Secretary for Management reported to NARA that the representative responded as follows:

> With regard to her tenure as Secretary of State, former Secretary Clinton has provided the Department on December 5, 2014, with all federal e-mail records in her custody, regardless of their format or the domain on which they were stored or created, that may not otherwise be preserved, to our knowledge, in the Department's recordkeeping system. She does not have custody of e-mails sent or received during the first few weeks of her tenure as she was transitioning to a new address, and we have been unable to obtain these. In the event we do, we will immediately provide the Department with federal record e-mails in this collection. [100]

With regard to Secretary Clinton's immediate staff, OIG received limited responses to its questionnaires, though two of Secretary Clinton's staff acknowledged occasional use of personal email accounts for official business.[101] However, OIG learned of extensive use of personal email accounts by four immediate staff members (none of whom responded to the questionnaire). During the summer of 2015, their representatives produced Federal records in response to a request from the Department, portions of which included material sent and received via their personal email accounts.[102] The material consists of nearly 72,000 pages in hard copy and more than 7.5 gigabytes of electronic data. One of the staff submitted 9,585 emails spanning January 22, 2009, to February 24, 2013, averaging 9 emails per workday sent on a personal email account. In this material, there are instances where the four individuals sent or received emails

[99] Letter from Paul M. Wester, Jr., Chief Records Officer for the U.S. Government, NARA, to Margaret P. Grafeld, Deputy Assistant Secretary for Global Information Systems, Bureau of Administration, U.S. Department of State (July 2, 2015).

[100] Letter from Patrick F. Kennedy, Under Secretary of State for Management, to Laurence Brewer, Acting Chief Records Officer for the U.S. Government, NARA (November 6, 2015).

[101] OIG sent 26 questionnaires to Secretary Clinton's staff and received 5 responses. Three respondents reported that they did not use personal email accounts to conduct official business. Another reported occasionally using personal email accounts while traveling with the Secretary and when Department accounts were not working. Another said he occasionally used his personal laptop or desktop at home to access the Department's OpenNet and that he assumed all data processed on OpenNet would be available to the Department.

[102] The material was produced to the Department for the following individuals:

Title	Production Dates
Counselor and Chief of Staff	6/25/2015; 8/10/2015; 8/12/2015
Deputy Chief of Staff for Operations	7/9/2015; 8/7/2015
Deputy Chief of Staff/Director of Policy Planning	7/30/2015
Deputy Assistant Secretary, Strategic Communications	7/28/2015; 8/6/15

regarding Department business using only their personal web-based email accounts. Accordingly, these staff failed to comply with Department policies intended to implement NARA regulations, because none of these emails were preserved in Department recordkeeping systems prior to their production in 2015.[103] As noted above, NARA has concluded that these subsequent productions mitigated their failure to properly preserve emails that qualified as Federal records during their service as Department employees. However, OIG did not attempt to determine whether these productions were complete. None of these individuals are currently employed by the Department.

Secretary Kerry (February 1, 2013 – Present): Secretary Kerry uses a Department email account on OpenNet and stated that, while he has used a personal email account to conduct official business, he has done so infrequently. In his interview with OIG, Secretary Kerry stated that he used his personal email more frequently when he was transitioning from the U.S. Senate to the Office of the Secretary. However, after discussions with his aides and other Department staff, he began primarily using his Department email account to conduct official business. The Secretary stated he may occasionally use personal email for official business when responding to a sender who emailed him on his personal account. The Secretary also stated that he either copies or forwards such emails to his Department account and copies his assistant. OIG's limited review of electronic records shows some personal email account usage by Secretary Kerry. Secretary Kerry's emails are now being retained using the Capstone approach discussed previously, which complies with the Federal Records Act and email records management requirements.[104]

OIG received responses to questionnaires from most of Secretary Kerry's immediate staff, who reported occasional use of personal email accounts for official business. [105] A number of staff also reported that they follow current policy on forwarding emails containing Federal records from personal accounts to Department accounts.[106] OIG's limited review of electronic records shows some personal email account usage by these staff.

Other staff reported that their emails are being retained using the Capstone approach, and some mentioned preserving emails through printing and filing. Several staff mentioned preserving emails by saving them in their Department email accounts. However, as previously

[103] 36 C.F.R. §1236.22(d) (October 2, 2009); 5 FAM 443.3 (October 30, 1995).

[104] NARA, *Guidance on a New Approach to Managing Email Records*, Bulletin No. 2013-02 (August 29, 2013), available at https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html.

[105] OIG sent 36 questionnaires to Secretary Kerry's staff and received 30 responses (several of the non-respondents had departed or were departing the Office of the Secretary), as well as a completed questionnaire from Secretary Kerry. With regard to preservation of Department emails, many reported retaining files in Microsoft Outlook and others reported that the Department was permanently retaining their email as part of the new Capstone program for senior officials. Most staff reported receiving training or other guidance on records preservation requirements through a variety of means, including formal training sessions, briefings, memos, and Department notices. Eleven staff reported using personal email accounts or other devices for official business, usually because of Internet connectivity interruptions while traveling.

[106] Eight stated that they forwarded or copied these emails to their Department accounts for records preservation purposes.

noted, NARA regulations state that agencies may only use an electronic mail system to store the recordkeeping copy of electronic mail messages identified as Federal records if that system contains specific features;[107] the current Department email system does not contain these features. Given that the Office of the Secretary does not use the SMART system, staff whose emails are not being retained under the Capstone approach should still be preserving emails through printing and filing. However, as previously noted, the Department is in the process of adopting a new email records management system that will cover the Office of the Secretary with the goal of meeting the requirement to manage all email records in an electronic format by December 31, 2016.[108] The Department plans that this system will eventually capture some of the email currently saved in Department email accounts and all of the email of senior officials currently being preserved.

CYBERSECURITY RISKS RESULT FROM THE USE OF NON-DEPARTMENTAL SYSTEMS AND EMAIL ACCOUNTS

In addition to complying with records management and preservation requirements, Department employees, including those in the Office of the Secretary, must comply with cybersecurity policies. Department information must be secure and protected from threats.

DS and IRM are the two bureaus within the Department with primary responsibility for ensuring the security of Department electronic information.[109] IRM is responsible for establishing effective information resource management planning and policies; ensuring the availability of information technology systems and operations; and approving development and administration of the Department's computer and information security programs and policies. DS is responsible for providing a safe and secure environment for the conduct of U.S. foreign policy, including personal, physical, and information security.[110]

According to DS and IRM officials, Department employees must use agency-authorized information systems to conduct normal day-to-day operations because the use of non-Departmental systems creates significant security risks. Department policies have evolved considerably over the past two decades; but since 1996, the FAM and FAH have contained numerous provisions regulating the use of such outside systems, including computers, personal devices, Internet connections, and email. (See Appendix A for a compilation of related cybersecurity laws and policies that were in effect during the tenures of each Secretary, from Secretary Albright through Secretary Kerry.) These provisions do contemplate limited use of non-Departmental systems, but the exceptions are quite narrow. Among the risks is the

[107] 36 C.F.R. § 1236.22 (October 2, 2009).

[108] OMB and NARA, *Memorandum for The Heads of Executive Departments and Agencies and Independent Agencies: Managing Government Records Directive* (OMB Memorandum M-12-18) (August 24, 2012).

[109] 1 FAM 271.1(4) (March 5, 2010).

[110] 12 FAM 010 (December 21, 2004).

targeting and penetration of the personal email accounts of Department employees, which was brought to the attention of the most senior officials of the Department as early as 2011.[111] Another significant risk is the introduction of viruses and malware onto Department systems, which increases their vulnerability to intrusion.

Based on this evaluation and a previous OIG inspection, OIG identified three Department officials—Secretary Powell, Secretary Clinton, and a former U.S. Ambassador to Kenya—who exclusively used non-Departmental systems to conduct official business. As will be discussed in greater detail below, OIG acknowledges significant differences in the facts and circumstances surrounding each of these cases.

Employees Generally Must Use Department Information Systems To Conduct Official Business

The Department's current policy, implemented in 2005, is that normal day-to-day operations should be conducted on an authorized Automated Information System (AIS), which "has the proper level of security control to ... ensure confidentiality, integrity, and availability of the resident information."[112] The FAM defines an AIS as an assembly of hardware, software, and firmware used to electronically input, process, store, and/or output data.[113] Examples include: mainframes, servers, desktop workstations, and mobile devices (such as laptops, e-readers, smartphones, and tablets).

This policy comports with FISMA, which was enacted in December 2002 and requires Federal agencies to ensure information security for the systems that support the agency's operations and assets, including information security protections for information systems used by a contractor of an agency or other organization on behalf of an agency.[114] FISMA defines information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide for the integrity, confidentiality, and availability of the information and systems.[115] In 2006, as required by FISMA, NIST promulgated minimum security requirements that apply to all information within the Federal Government and to Federal information systems.[116] Among these are requirements for certifying and accrediting information systems, retaining system audit records for monitoring purposes, conducting risk assessments, and ensuring the protection of communications.

---

[111] *See, e.g.,* 11 STATE 65111 (June 28, 2011).

[112] 12 FAM 544.3 (November 4, 2005). This provision also states that "The Department's authorized telework solution(s) are designed in a manner that meet these requirements and are not considered end points outside of the Department's management control."

[113] 12 FAM 091 (January 11, 2016).

[114] 44 U.S.C. § 3554.

[115] 44 U.S.C. § 3552(b)(3).

[116] NIST, FIPS PUB 200: *Minimum Security Requirements for Federal Information and Information Systems* (March 2006).

In 2007, the Department adopted additional policies to implement these requirements, including numerous provisions intended to ensure that non-Departmental information systems that process or store Department information maintain the same minimum security controls. Further, non-Departmental systems that are sponsored by the Department to process information on its behalf must be registered with the Department.[117]

Restrictions Apply to the Use of Non-Departmental Systems

The FAM and FAH contain a number of restrictions regarding the use of non-Departmental computers, mobile devices, Internet connections, and personal email to transmit Department information. These provisions have evolved since 1996, but employees must implement safeguards or request approval before using such equipment. Figure 2 shows the evolution of these provisions and related statutes and regulations.

[117] 5 FAH-11 H-412.4(c)(4) (June 25, 2007).

Figure 2: Timeline of Selected Security Requirements and Policies

1987

Computer Security Act requires agencies to develop computer security plans and conduct security training.

1996

FAM prohibits installation or use of privately owned computers in Department facilities.

1997–2001 Madeleine Albright

2000

OMB Circular A-130 required Federal agencies to establish information security programs containing specified elements, including development of a security plan and security controls.

2001–2005 Colin Powell

2002

FISMA requires that all information systems that process or store agency information be certified and accredited according to NIST standards.

FAM requires all Department facilities to use OpenNet to access the Internet or request a waiver.

2004

FAM requires permission for Department offices to use commercial Internet service providers.

2005–2009 Condoleezza Rice

2005

FAM states: "It is the Department's general policy that normal day-to-day operations be conducted on an authorized AIS, which has the proper level of security control to provide nonrepudiation, authentication and encryption, to ensure confidentiality, integrity, and availability of the resident information."

FAM allows SBU information to be sent over the Internet with caution.

Department begins Cyber Security Incident Program.

2008

FAM requires administrative, technical, and physical safeguards for the remote processing of SBU information.

FAM amended to allow use or installation of privately owned computers only with DS and IRM approval.

2009–2013 Hillary Clinton

2009

FAM prohibits use of personal digital assistants (PDAs) in Department facilities except for strictly unclassified areas.

2013–Present John Kerry

2015

PDA restrictions moved to FAH and somewhat eased; requirement to use authorized AIS for day-to-day operations added to FAH.

Source: OIG analysis of laws and policies.

Privately Owned Computers and Mobile Devices: In 1996, the FAM directed Department systems managers to ensure that privately owned computers were not installed or used in any Department office building.[118] In 2008, the Department amended this provision to prohibit the use or installation of non-U.S. Government-owned computers in any Department facility without the written approval of DS and IRM, with certain exceptions.[119]

In 2009, the Department adopted polices addressing the specific requirements for use of non-Department-owned personal digital assistants (PDAs).[120] Under this policy, PDAs could only be turned on and used within Department areas that are strictly unclassified (such as the cafeteria) and could not connect with a Department network except via a Department-approved remote-access program, such as Global OpenNet.[121] In 2014, the Department amended this provision to authorize Department managers in domestic locations to allow non-Department-owned PDAs within their specific work areas, provided users maintain a minimum 10-foot separation between the PDA and classified processing equipment. In 2015, the Department replaced these provisions with a new FAH provision that included the domestic 10-foot-separation rule and the ban on connecting to a Department network except via a Department-approved remote-access program.[122]

Related to these provisions is the Department policy on "remote processing"—the processing of Department unclassified or sensitive but unclassified (SBU) information on non-Department-owned systems (such as a home computer or a tablet) or on Department-owned systems (such as a Department-issued laptop) at non-Departmental facilities (such as at an employee's home or a hotel)—which has been in place since 2008.[123] Under this policy, management and employees must exercise "particular care and judgment" when remotely processing SBU information.[124] Offices that allow employees to remotely process SBU information must ensure that appropriate administrative, technical, and physical safeguards are maintained to protect the

[118] 12 FAM 625.2-1 (April 12, 1996).

[119] 12 FAM 625.2-1 (July 28, 2008). This provision was removed from the FAM in 2015, but a FAH provision prohibits the installation of non-Department owned information systems within Department facilities without the written authorization of DS and IRM. 12 FAH-10 H-112.14-2 (September 19, 2014). Both the FAM and FAH provisions include an exception for a non-Department entity that has an approved dedicated space within a Department facility.

[120] The FAM defined PDAs as "hand-held computers" including "standard personal digital assistants; e.g., Palm devices, Win CE devices, etc., and multi-function automated information system (AIS) devices; e.g., BlackBerry devices, PDA/cell phones, etc." 12 FAM 683.1 (December 2, 2009).

[121] 12 FAM 683.2-3 (December 2, 2009).

[122] 12 FAH-10 H-165.4 (May 20, 2015). These devices are referred to as Non-Department Owned Mobile Devices (NDOMDs).

[123] 12 FAM 682 (August 4, 2008). This subchapter was later removed from the FAM and moved to the FAH at 12 FAH-10 H-170 (as amended January 11, 2016).

[124] 12 FAM 682.2-4 (August 4, 2008). This requirement is currently located at 12 FAH-10 H-173.4 (January 11, 2016). SBU information is defined in the FAM as information that is not classified for national security reasons but that warrants or requires administrative control and protection from public or other unauthorized disclosure for other reasons. Examples include personnel data, visa and asylum records, law enforcement information, privileged communications, and deliberative inter- or intra-agency communications. 12 FAM 541 (March 5, 2013).

confidentiality and integrity of records and to ensure encryption of SBU information with products certified by NIST. Employees must implement and regularly update basic home security controls, including a firewall, anti-spyware, antivirus, and file-destruction applications for all computers on the network.[125] In 2014, the Department added a provision to the FAH to require users who process SBU information on non-Department-owned storage media to encrypt it with products certified by NIST. [126]

Internet Connections: Since the end of 2002, the FAM has required all Department facilities to use the Department's primary Internet connection, OpenNet, to establish Internet connectivity.[127] The Department further regulated access to the Internet by establishing rules in 2004 addressing the use of non-Departmental Internet connections in Department facilities.[128]

Personal Email: Since 2002, Department employees have been prohibited from auto-forwarding their email to a personal email address "to preclude inadvertent transmission of SBU email on the Internet."[129]

The FAM also reminds employees that "transmissions from the Department's OpenNet to and from non-U.S. Government Internet addresses, and other .gov or .mil addresses, unless specifically directed through an approved secure means, traverse the Internet unencrypted."[130] The FAM further states that, with regard to SBU information, the Department is expected to provide, and employees are expected to use, approved secure methods to transmit such information when available and practical. However, if such secure methods are not available, employees with a valid business need may transmit SBU information over the Internet unencrypted so long as they carefully consider that unencrypted emails can pass through foreign and domestic controlled ISPs, placing the confidentiality and integrity of the information at risk. In addition, the FAM instructs employees transmitting SBU information outside the

[125] 12 FAM 682.2-5 (August 4, 2008). Currently, these requirements, as amended, are located at 12 FAH-10 H-173.4 (January 11, 2016). The amended provision requires NIST FIPS 140-2 encryption for SBU information in addition to the use of a firewall anti-spyware, anti-virus, and file destruction applications.

[126] 12 FAH-10 H-172.1 (September 25, 2014). Currently, this requirement is located at 12 FAH-10 H-173.4 (January 11, 2016). If the employee has a wireless home network, the FAH requires use of a NIST-validated product to secure the wireless connection. 12 FAH-10 H-173.4(9) (September 25, 2014).

[127] 5 FAM 871 (December 30, 2002). The language of this provision was amended in 2004, 2009, and 2013, but the basic requirement to use OpenNet has remained consistent.

[128] 5 FAM 874.2 (May 4, 2004). Currently, these rules are at 5 FAM 872 (May 1, 2014). Department facilities must seek authorization from the bureau Executive Director or post Management Officer to use such a connection. 5 FAM 872.1 (May 1, 2014). Such systems may not be used to process SBU information, except in limited amounts under exigent circumstances. 5 FAM 872.2 (May 1, 2014).

[129] 5 FAM 751.2 (February 27, 2002). This rule was amended in 2011 to incorporate a prohibition on including a personal email address in an auto-reply message. 5 FAM 752.1(e) (November 14, 2011).

[130] 12 FAM 544.3 (November 4, 2005). From 2002 to 2005, transmission of SBU information over the Internet was completely prohibited. 5 FAM 751.2 (February 27, 2002).

Department's OpenNet network on a regular basis to the same official or personal email address to request a solution from IRM.[131]

In 2015, the Department amended the FAM to incorporate NARA's guidance, which advises employees that "personal accounts should only be used in exceptional circumstances."[132] This provision also states that "Department employees are discouraged from using private email accounts (e.g., Gmail, AOL, Hotmail, etc.) for official business [except] in those very limited circumstances when it becomes necessary to do so." However, the FAM gives no further guidance about what type of circumstances would permit use of personal email.

The Department Has Issued Numerous Warnings About Cybersecurity Risks

One of the primary reasons that Department policy requires the use of Department systems is to guard against cybersecurity incidents. Threats and actual attacks against the Department have been on the rise for nearly a decade. For example, in May 2006, the Department experienced large-scale computer intrusions that targeted its headquarters and its East Asian posts.[133] Consequently, the Department has issued numerous announcements, cables, training requirements, and memos to highlight the various restrictions and risks associated with the use of non-Departmental systems, especially the use of personal email accounts.

As early as 2004, Department cables reminded staff that only Department-approved software should be installed on the Department's information systems because outside software may bypass firewall and anti-virus checks, creating an open channel for hackers and malicious code, thus placing Department networks at serious risk.[134] Since then, the Department has published prohibitions or warnings related to the use of instant messaging, PDAs and smartphones, thumb drives, CDs and DVDs, Internet browsers, and personally owned devices.[135] Employees are also reminded of these issues through the Department's required annual Cybersecurity Awareness course.[136] Further, in 2005 DS's Cyber Threat Analysis Division (CTAD) began issuing notices to Department computer users specifically highlighting cybersecurity threats. For example, CTAD's

[131] 12 FAM 544.2 (November 4, 2005).

[132] 5 FAM 443.7 (October 23, 2015).

[133] *See Cyber Insecurity: Hackers Are Penetrating Federal Systems And Critical Infrastructure: Hearing Before the House Committee on Homeland Security, Subcommittee On Emerging Threats, Cybersecurity And Science And Technology*, 110th Congress (2007) (statement of Donald Reid, Senior Coordinator for Security Infrastructure, Bureau of Diplomatic Security, U.S. Department of State), at 13-15.

[134] 04 STATE 204864 (September 22, 2004).

[135] *See e.g.*, 05 STATE 096534 (May 2005); *Prohibition Against Use of Privately Owned Software/Hardware on Department Automated Information Systems*, Announcement No. 2006_01_074 (January 24, 2006); *Use Of Unclassified/SBU Thumb Drives*, Announcement No. 2008_09_046 (September 9, 2008); *Using PEDs Abroad*, Announcement No. 2008_09_068 (September 12, 2008); *Remote Accessing and Processing*, Announcement No. 2008_11_061 (November 14, 2008); 09 STATE 130999 (December 24, 2009); *Use of Non-Department Owned Personal Digital Assistants (PDAs) and Smartphones in Department Facilities*, Announcement No. 2010_10_150 (October 26, 2010).

[136] 5 FAM 845 (July 12, 2013).

notices from 2005 to 2011 addressed BlackBerry security vulnerabilities, generally citing mobile devices as a weak link in computer networks.[137] CTAD warned that BlackBerry devices must be configured in accordance with the Department's security guidelines.

In July 2005, IRM introduced its BlackBerry service that provided domestic users access to their OpenNet email, calendar, and contacts.[138] From the beginning, the BlackBerry servers were required to be configured in accordance with the current DS Information Technology Security Guide, which contains an extensive list of security settings that lock down the devices. These security standards continue to apply to current Department BlackBerry devices.

In March 2009, after unsuccessful efforts to supply Secretary Clinton with a secure government smartphone, DS was informed that Secretary Clinton's staff had been asking to use BlackBerry devices inside classified areas. The Assistant Secretary of DS then sent a classified memorandum to Secretary Clinton's Chief of Staff that described the vulnerabilities associated with the use of BlackBerry devices and also noted the prohibition on the use of Blackberry devices in sensitive areas. According to a DS official, shortly after the memorandum was delivered, Secretary Clinton approached the Assistant Secretary and told him she "gets it."

The use of personal email accounts to conduct official business has been a particular concern over the past several years. For example, on March 11, 2011, the Assistant Secretary for Diplomatic Security sent a memorandum on cybersecurity threats directly to Secretary Clinton.[139] A portion of the unclassified version of this memorandum states:

> Threat analysis by the DS cyber security team and related incident reports indicate a dramatic increase since January 2011 in attempts by [redacted] cyber actors to compromise the private home e-mail accounts of senior Department officials. ... Although the targets are unclassified, personal e-mail accounts, the likely objective is to compromise user accounts and thereby gain access to policy documents and personal information that could enable technical surveillance and possible blackmail. The personal e-mail of family members also is at risk.

The memorandum included as an attachment "a snapshot of affected Department personnel," noting that many of the email account owners play major roles in forming diplomatic and economic policy.[140] It concluded by noting, "We also urge Department users to minimize the use

---

[137] *See, e.g.,* CTAD, *Cyber Security Awareness* (March 3, 2011).

[138] Department of State, *Blackberry Wireless PDA Use in the Department of State*, Announcement No. 2005_07_018, July 7, 2005. This announcement also notes: "Personal Blackberry devices are not allowed." In September 2005, overseas posts were also authorized to procure, install, and operate their own BlackBerry Enterprise Server (BES) and BlackBerry devices. 05 STATE 172062 (September 2005).

[139] OIG asked DS if it had sent memoranda warning of similar risks to other Secretaries, but it could not find any similar examples.

[140] Spear phishing was one of the several types of threats included in the Memorandum. It is an attack on a single user or department within an organization, such as asking employees to update their username and passwords. Once

of personal web email for business, as some compromised home systems have been reconfigured by these actors to automatically forward copies of all composed emails to an undisclosed recipient."

Following the March 2011 memorandum, DS cybersecurity staff conducted two cybersecurity briefings of S/ES staff, the Secretary's immediate staff, and Bureau of Public Affairs staff in April and May 2011. OIG discovered in Secretary Clinton's retired paper files a copy of the classified presentation used during the briefing. It contains material similar to the type provided in the March 11, 2011, memorandum.

On June 28, 2011, the Department, in a cable entitled "Securing Personal E-mail Accounts" that was approved by the Assistant Secretary for Diplomatic Security and sent over Secretary Clinton's name to all diplomatic and consular posts, encouraged Department users "to check the security settings and change passwords of their home e-mail accounts because of recent targeting of personal email accounts by online adversaries."[141] The cable further elaborated that "recently, Google asserted that online adversaries are targeting the personal Gmail accounts of U.S. government employees. Although the company believes it has taken appropriate steps to remediate identified activity, users should exercise caution and follow best practices in order to protect personal e-mail and prevent the compromise of government and personal information." It then recommended best practices for Department users and their family members to follow, including "avoid conducting official Department business from your personal e-mail accounts."[142]

Three Officials Exclusively Used Non-Departmental Systems for Day-to-Day Operations

Cybersecurity risks demonstrate the need both for restrictions on the use of non-Departmental systems and for requirements to seek approval before using such systems. A senior IRM official

---

hackers obtain this information, they can easily access entry into secured networks. Another example of spear phishing is asking users to click on a link, which deploys spyware.

[141] 11 STATE 65111 (June 28, 2011).

[142] That portion of the cable reads in full as follows:

> 3. What can you and your family members do?
>
> (a) Follow the personal e-mail guides posted on the Awareness site to change your password, to ensure that messages are not auto-forwarding to an unintended address, and to verify that other security settings are properly configured.
>
> (b) Beware of e-mail messages that include links to password reset web pages. These can be easily faked.
>
> (c) Create strong passwords for all of your online accounts, change them often, and never use the same password for more than one account.
>
> (d) Avoid conducting official Department business from your personal e-mail accounts.
>
> (e) Do not reveal your personal e-mail address in your work "Out of Office" message.
>
> (f) Do not auto-forward Department e-mail to personal e-mail accounts, which is prohibited by Department policy (12 FAM 544.3).

reported to OIG that many Department employees have requested to use non-Departmental systems to conduct business; examples include requests to use outside video conferencing systems and file sharing software. According to this official, the Department typically refuses such requests. For instance, in 2012, Department staff submitted a request to IRM to use an Internet-based teleconference service. In response, IRM cited the 2005 FAM provision (12 FAM 544.3) requiring that normal day-to-day operations be conducted on an authorized AIS and further noted that the Department "expect[s] employees to use the tools provided by the Department to protect sensitive information from unauthorized access or disclosure" and only permits the use of non-Departmental systems "when absolutely necessary." Other employees have sought to use Dropbox, a cloud-based file hosting service, but IRM has blocked access to the site on OpenNet since 2011 because of the risk of unauthorized access to Department data. The senior IRM official told OIG that the Department seldom encounters "an 'absolutely necessary' condition that would lead to approval for non-emergency processing/transmission of Department work outside [the Department's] network."

OIG identified many examples of staff using personal email accounts to conduct official business; however, OIG could only identify three cases where officials used non-Departmental systems on an exclusive basis for day-to-day operations. These include former Secretaries Powell and Clinton, as well as Jonathan Scott Gration, a former Ambassador to Kenya. Although the former Ambassador was not a member of the Office of the Secretary, the Department's response to his actions demonstrates how such usage is normally handled when Department cybersecurity officials become aware of it. The facts and circumstances surrounding each of these cases are discussed below:

Secretary Powell: Secretary Powell has acknowledged using a personal email account from a commercial Internet provider, which he accessed on a "private line" in his Department office. He further stated that he had two computers at his desk: "a secure State Department machine ... used for secure material, and...a laptop [used] for email."[143] Neither the Secretary nor his representative could recall whether Secretary Powell owned the laptop or whether the Department provided it to him. However, the Secretary characterized the use of the laptop as his "unclassified system," which was not connected to OpenNet. In his interview with OIG, Secretary Powell explained that, when he arrived at the Department, the email system in place only permitted communication among Department staff. He therefore requested that information technology staff install the private line so that he could use his personal account to communicate with people outside the Department.[144] He described his email usage as "daily," though OIG was unable to determine how many emails he actually sent and received during his tenure.

[143] *Meet the Press* (NBC television broadcast September 6, 2015) (interview with Colin Powell), available at http://www.nbcnews.com/meet-the-press/meet-press-transcript-september-6-2015-n422606.

[144] Secretary Powell also acknowledged using his personal account to communicate with Department employees. *Meet the Press* (NBC television broadcast September 6, 2015) (interview with Colin Powell).

Various DS and IRM staff told OIG that, before Secretary Powell arrived at the Department, employees did not have Internet connectivity on their desktop computers. The Department's Chief Information Officer (CIO) and Under Secretary for Management during Secretary Powell's tenure reported to OIG that they were aware of Secretary Powell's use of a personal email account and also noted the Secretary's goal was to provide every Department employee with similar Internet and email capabilities at their desktops. The current CIO and Assistant Secretary for Diplomatic Security, who were Department employees during Secretary Powell's tenure, also were both aware of the Secretary's use of a personal email account and recall numerous discussions with senior staff throughout the Department about how to implement the Secretary's intent to provide all employees with Internet connectivity.

However, it is not clear whether staff explicitly addressed restrictions on the use of non-Departmental systems with Secretary Powell. For example, at the beginning of Secretary Powell's tenure, the Department had an outright prohibition on both the installation of privately owned computers in Department facilities and the transmission of SBU information on the Internet.[145] By 2002, the Department had established the requirement to connect to the Internet only on OpenNet.[146] The CIO and Under Secretary for Management during Secretary's Powell's tenure reported to OIG that they believe that these issues were addressed, either by installing a firewall to protect the Secretary's Internet connection or providing the Secretary with a Department laptop. They also reported having multiple discussions with Secretary Powell about the Department's implementation of FISMA requirements. In contrast, current DS and IRM officials who worked at the Department during Secretary Powell's tenure are unsure about the exact configuration of Secretary Powell's systems and whether staff addressed applicable restrictions with the Secretary. However, they reported to OIG that the Department's technology and information security policies were very fluid during Secretary Powell's tenure and that the Department was not aware at the time of the magnitude of the security risks associated with information technology.

Secretary Clinton: By Secretary Clinton's tenure, the Department's guidance was considerably more detailed and more sophisticated. Beginning in late 2005 and continuing through 2011, the Department revised the FAM and issued various memoranda specifically discussing the obligation to use Department systems in most circumstances and identifying the risks of not doing so. Secretary Clinton's cybersecurity practices accordingly must be evaluated in light of these more comprehensive directives.

Secretary Clinton used mobile devices to conduct official business using the personal email account on her private server extensively, as illustrated by the 55,000 pages of material making up the approximately 30,000 emails she provided to the Department in December 2014. Throughout Secretary Clinton's tenure, the FAM stated that normal day-to-day operations

[145] 12 FAM 625.2-1 (April 12, 1996); 5 FAM 751.2 (February 27, 2002).

[146] 5 FAM 871 (December 30, 2002).

should be conducted on an authorized AIS,[147] yet OIG found no evidence that the Secretary requested or obtained guidance or approval to conduct official business via a personal email account on her private server. According to the current CIO and Assistant Secretary for Diplomatic Security, Secretary Clinton had an obligation to discuss using her personal email account to conduct official business with their offices, who in turn would have attempted to provide her with approved and secured means that met her business needs. However, according to these officials, DS and IRM did not—and would not—approve her exclusive reliance on a personal email account to conduct Department business, because of the restrictions in the FAM and the security risks in doing so.

During Secretary Clinton's tenure, the FAM also instructed employees that they were expected to use approved, secure methods to transmit SBU information and that, if they needed to transmit SBU information outside the Department's OpenNet network on a regular basis to non-Departmental addresses, they should request a solution from IRM.[148] However, OIG found no evidence that Secretary Clinton ever contacted IRM to request such a solution, despite the fact that emails exchanged on her personal account regularly contained information marked as SBU.

Similarly, the FAM contained provisions requiring employees who process SBU information on their own devices to ensure that appropriate administrative, technical, and physical safeguards are maintained to protect the confidentiality and integrity of records and to ensure encryption of SBU information with products certified by NIST.[149] With regard to encryption, Secretary Clinton's website states that "robust protections were put in place and additional upgrades and techniques employed over time as they became available, including consulting and employing third party experts."[150] Although this report does not address the safety or security of her system, DS and IRM reported to OIG that Secretary Clinton never demonstrated to them that her private server or mobile device met minimum information security requirements specified by FISMA and the FAM.

In addition to interviewing current and former officials in DS and IRM, OIG interviewed other senior Department officials with relevant knowledge who served under Secretary Clinton, including the Under Secretary for Management, who supervises both DS and IRM; current and former Executive Secretaries; and attorneys within the Office of the Legal Adviser. These officials all stated that they were not asked to approve or otherwise review the use of Secretary Clinton's server and that they had no knowledge of approval or review by other Department staff. These officials also stated that they were unaware of the scope or extent of Secretary Clinton's use of a personal email account, though many of them sent emails to the Secretary on this account. Secretary Clinton's Chief of Staff also testified before the House Select Committee on Benghazi that she was unaware of anyone being consulted about the Secretary's exclusive use of a

[147] 12 FAM 544.3 (November 4, 2005).

[148] 12 FAM 544.2 (November 4, 2005).

[149] 12 FAM 682 (August 4, 2008).

[150] https://www.hillaryclinton.com/briefing/factsheets/2015/07/13/email-facts/ (date last downloaded April 20, 2016).

personal email address.[151] OIG did find evidence that various staff and senior officials throughout the Department had discussions related to the Secretary's use of non-Departmental systems, suggesting there was some awareness of Secretary Clinton's practices. For example:

- In late-January 2009, in response to Secretary Clinton's desire to take her BlackBerry device into secure areas, her Chief of Staff discussed with senior officials in S/ES and with the Under Secretary for Management alternative solutions, such as setting up a separate stand-alone computer connected to the Internet for Secretary Clinton "to enable her to check her emails from her desk." The Under Secretary's response was "the stand-alone separate network PC is [a] great idea" and that it is "the best solution." According to the Department, no such computer was ever set up.

- In November 2010, Secretary Clinton and her Deputy Chief of Staff for Operations discussed the fact that Secretary Clinton's emails to Department employees were not being received. The Deputy Chief of Staff emailed the Secretary that "we should talk about putting you on state email or releasing your email address to the department so you are not going to spam." In response, the Secretary wrote, "Let's get separate address or device but I don't want any risk of the personal being accessible."[152]

- In August 2011, the Executive Secretary, the Under Secretary for Management, and Secretary Clinton's Chief of Staff and Deputy Chief of Staff, in response to the Secretary's request, discussed via email providing her with a Department BlackBerry to replace her personal BlackBerry, which was malfunctioning, possibly because "her personal email server is down." The then-Executive Secretary informed staff of his intent to provide two devices for the Secretary to use: "one with an operating State Department email account (which would mask her identity, but which would also be subject to FOIA requests), and another which would just have phone and internet capability." In another email exchange, the Director of S/ES-IRM noted that an email account and address had already

[151] The pertinent testimony from the former Chief of Staff, who declined OIG's request for an interview, reads as follows:

Q Was anyone consulted about Secretary Clinton exclusively using a personal email address for her work?
A I don't recall that. If it did happen, I wasn't part of that process. But I don't believe there was a consultation around it, or at least there's not one that I'm aware of, maybe I should better answer that way based on my knowledge.
Q So no private counsel?
A Not that I'm aware of.
Q Okay. The general counsel for the State Department?
A Not that I'm aware of.
Q Okay. Anybody from the National Archives?
A Not that I'm aware of. But I can only speak to my knowledge, obviously.
Q Sure. And anyone from the White House?
A Not that I'm aware of.

[152] Secretary Clinton declined OIG's request for an interview. The former Deputy Chief of Staff for Operations has not responded to OIG's request for an interview.

been set up for the Secretary[153] and also stated that "you should be aware that any email would go through the Department's infrastructure and subject to FOIA searches."[154] However, the Secretary's Deputy Chief of Staff rejected the proposal to use two devices, stating that it "doesn't make a whole lot of sense." OIG found no evidence that the Secretary obtained a Department address or device after this discussion.

- OIG identified two individuals who provided technical support to Secretary Clinton. The first, who was at one time an advisor to former President Clinton but was never a Department employee, registered the clintonemail.com domain name on January 13, 2009.[155] The second, a Schedule C political appointee who worked in IRM as a Senior Advisor from May 2009 through February 2013,[156] provided technical support for BlackBerry communications during the Secretary's 2008 campaign for President.[157] OIG reviewed emails showing communications between Department staff and both individuals concerning operational issues affecting the Secretary's email and server from 2010 through at least October 2012. For example, in December 2010, the Senior Advisor worked with S/ES-IRM and IRM staff to resolve issues affecting the ability of emails transmitted through the clintonemail.com domain used by Secretary Clinton to reach Department email addresses using the state.gov domain.[158]

---

[153] According to the Department, this account was only used by Secretary Clinton's staff to maintain an Outlook calendar.

[154] The former Director of S/ES-IRM declined OIG's request for an interview.

[155] The clintonemail.com domain name was registered with Network Solutions Certificate Authority on January 13, 2009 and identifies the advisor to former President Clinton as the registrant.

[156] Schedule C appointments are those of a "confidential or policy-determining character" 5 C.F.R. § 6.2.

[157] Secretary Clinton's counsel advised OIG that the Senior Advisor "performed technology services for the Clinton family for which he was compensated" by check or wire transfer in varying amounts and various times between 2009 and 2013. In addition, the Senior Advisor's direct supervisors in IRM from 2009 to 2013 told OIG they were unaware of his technical support of the Secretary's email system. While working at the Department, the Senior Advisor reported directly to the Deputy Chief Information Officer (DCIO) for Operations, who in turn reported to the Chief Information Officer (CIO). The DCIO and CIO, who prepared and approved the Senior Advisor's annual evaluations, believed that the Senior Advisor's job functions were limited to supporting mobile computing issues across the entire Department. They told OIG that while they were aware that the Senior Advisor had provided IT support to the Clinton Presidential campaign, they did not know he was providing ongoing support to the Secretary's email system during working hours. They also told OIG that they questioned whether he could support a private client during work hours, given his capacity as a full-time government employee.

[158] At that time, S/ES IRM staff met with the Senior Advisor, who accessed the Secretary's email system and looked at its logs. The issue was ultimately resolved and, on December 21, 2010, S/ES-IRM staff sent senior S/ES staffers an email describing the issue and summarizing the activities undertaken to resolve it. On another occasion, the Senior Advisor met with staff within CTAD and received a briefing on cyber security risks facing the Department. A third interaction took place on October 30, 2012, during the period when Hurricane Sandy disrupted power in the New York City area. An email exchange between Deputy Chief of Staff for Operations and another member of the Secretary's staff revealed that the server located in Secretary Clinton's New York residence was down. Thereafter, the Senior Advisor met with S/ES-IRM staff to ascertain whether the Department could provide support for the server. S/ES-IRM staff reported to OIG that they told the Senior Advisor they could not provide support because it was a private server.

- Two staff in S/ES-IRM reported to OIG that, in late 2010, they each discussed their concerns about Secretary Clinton's use of a personal email account in separate meetings with the then-Director of S/ES-IRM. In one meeting, one staff member raised concerns that information sent and received on Secretary Clinton's account could contain Federal records that needed to be preserved in order to satisfy Federal recordkeeping requirements. According to the staff member, the Director stated that the Secretary's personal system had been reviewed and approved by Department legal staff and that the matter was not to be discussed any further. As previously noted, OIG found no evidence that staff in the Office of the Legal Adviser reviewed or approved Secretary Clinton's personal system. According to the other S/ES-IRM staff member who raised concerns about the server, the Director stated that the mission of S/ES-IRM is to support the Secretary and instructed the staff never to speak of the Secretary's personal email system again.

- On January 9, 2011, the non-Departmental advisor to President Clinton who provided technical support to the Clinton email system notified the Secretary's Deputy Chief of Staff for Operations that he had to shut down the server because he believed "someone was trying to hack us and while they did not get in i didnt [sic] want to let them have the chance to." Later that day, the advisor again wrote to the Deputy Chief of Staff for Operations, "We were attacked again so I shut [the server] down for a few min." On January 10, the Deputy Chief of Staff for Operations emailed the Chief of Staff and the Deputy Chief of Staff for Planning and instructed them not to email the Secretary "anything sensitive" and stated that she could "explain more in person."[159]

Ambassador Gration: Ambassador Gration served as the U.S. Ambassador to Kenya from mid-2011 through mid-2012. OIG first publicly reported on the activities of Ambassador Gration as part of its 2012 inspection of Embassy Nairobi.[160] Prior to the inspection, in June 2011, DS learned that the newly posted Ambassador had drafted and distributed a revised mission policy concerning communications security that authorized him and other mission personnel to use commercial email for daily communication of official government business. That prompted senior DS management and cybersecurity staff to email the Ambassador to advise him that DS was dispatching an experienced Regional Computer Security Officer to provide expertise and

[159] In another incident occurring on May 13, 2011, two of Secretary Clinton's immediate staff discussed via email the Secretary's concern that someone was "hacking into her email" after she received an email with a suspicious link. Several hours later, Secretary Clinton received an email from the personal account of then-Under Secretary of State for Political Affairs that also had a link to a suspect website. The next morning, Secretary Clinton replied to the email with the following message to the Under Secretary: "Is this really from you? I was worried about opening it!" Department policy requires employees to report cybersecurity incidents to IRM security officials when any improper cyber-security practice comes to their attention. 12 FAM 592.4 (January 10, 2007). Notification is required when a user suspects compromise of, among other things, a personally owned device containing personally identifiable information. 12 FAM 682.2-6 (August 4, 2008). However, OIG found no evidence that the Secretary or her staff reported these incidents to computer security personnel or anyone else within the Department.

[160] ISP-I-12-38A (August 2012).

advice in establishing procedures for handling SBU information that adhered to Department standards for the processing of sensitive material. DS further noted that this visit would be "especially timely in the wake of recent headlines concerning a significant hacking effort directed against the private, web-based email accounts of dozens of senior USG officials, which has generated substantial concern from the Secretary, Deputy Secretary Steinberg, and other Department principals." Notwithstanding the Department's concerns, the Ambassador continued to use commercial email for official business.

DS then notified the Ambassador via cable on July 20, 2011, that the FAM did not permit him to use non-government email for day-to-day operations.[161] The cable stated in relevant part:

> The language in 12 FAM 544.3, which states that "it is the Department's general policy that normal day-to-day operations be conducted on an authorized [automated information system]" is purposely included to place employees on notice that if they are given a tool that provides an adequate level of security encryption, such as an OpenNet terminal ... or any other Department-supplied security mechanism that works in the given circumstance, they must use it. 12 FAM 544.3 goes on to say that in the absence of a Department-supplied security solution employees can send most SBU information unencrypted via the internet only when necessary, with the knowledge that the nature of the transmission lends itself to unauthorized access, however remote that chance might be. ... Given the threats that have emerged since 2005, especially in regard to phishing and spoofing of certain web-based email accounts, we cannot allow the proliferation of this practice beyond maintaining contact during emergencies. We are all working toward the same end—to protect the availability, integrity and confidentiality of Department information and systems, while recognizing that emergency situations may arise, particularly for our employees serving overseas. ... The Department is not aware of any exigent circumstances in Nairobi that would authorize a deviation from the requirement to use Department systems for official business.

However, the Ambassador continued to use unauthorized systems to conduct official business. The Department subsequently initiated disciplinary proceedings against him for his failure to follow these directions and for several other infractions, but he resigned before any disciplinary measures were imposed.

OIG could find no other instances where the Department initiated disciplinary procedures against a senior official for using non-Departmental systems for day-to-day operations.

[161] 11 STATE 73417 (July 20, 2011).

CONCLUSION

Longstanding, systemic weaknesses related to electronic records and communications have existed within the Office of the Secretary that go well beyond the tenure of any one Secretary of State. OIG recognizes that technology and Department policy have evolved considerably since Secretary Albright's tenure began in 1997. Nevertheless, the Department generally and the Office of the Secretary in particular have been slow to recognize and to manage effectively the legal requirements and cybersecurity risks associated with electronic data communications, particularly as those risks pertain to its most senior leadership. OIG expects that its recommendations will move the Department steps closer to meaningfully addressing these risks.

RECOMMENDATIONS

To ensure compliance with Federal and Department requirements regarding records preservation and use of non-Departmental systems, OIG has issued the following recommendations to the Bureau of Administration, the Office of the Secretary, the Bureau of Information Resources Management, the Bureau of Human Resources, and the Department's Transparency Coordinator. Their complete responses can be found in Appendix B. The Department also provided technical comments that OIG incorporated as appropriate into this report.

Recommendation 1: The Bureau of Administration should

- continue to issue guidance, including periodic, regular notices, to Department employees to remind them that the use of personal email accounts to conduct official business is discouraged in most circumstances,
- clarify and give specific examples of the types of limited circumstances in which such use would be permissible, and
- instruct employees how to preserve Federal records when using personal email accounts.

Management Response: In its May 23, 2016, response, the Bureau of Administration concurred with this recommendation. It will continue to issue guidance on records management practices and policies, and will ensure that this guidance explicitly reminds employees that the use of personal emails accounts to conduct official business is discouraged.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation of this additional guidance.

Recommendation 2: The Bureau of Administration should amend the *Foreign Affairs Manual* to reflect the updates to Department recordkeeping systems that provide alternatives to print and file emails that constitute Federal records.

Management Response: In its May 23, 2016, response, the Bureau of Administration concurred with this recommendation. It noted that it is currently working with the Transparency Coordinator to update sections of the FAM related to the Department's recordkeeping/retention schedules, with a goal to eliminate the practice of print and file as the Department's policy for the retention of emails by December 31, 2016.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation of the amendment.

Recommendation 3: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to conduct an inventory of all electronic and hard-copy files in its custody and evaluate them to determine which files should be transferred to the Office of Information Programs and Services in accordance with records disposition schedules or Department email preservation requirements.

Management Response: In its May 16, 2016, response, the Executive Secretariat concurred with this recommendation. It noted that the inventory of electronic and hard copy files has been ongoing since January 2016 and that once it is complete, the Executive Secretariat will retire all such records according to applicable records schedules.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that this effort has been completed.

Recommendation 4: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to improve policies and procedures to promote compliance by all employees within its purview, including the Secretary, with records management requirements. These policies should cover the retirement of records in accordance with records disposition schedules, preservation of email and other electronic records of departing officials, and training of employees on their records preservation responsibilities.

Management Response: In its May 16, 2016, response, the Executive Secretariat concurred with this recommendation. It noted that it is committed to coordinating closely with the Office of Information Programs and Services to provide updated guidance and training to all staff.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts a copy of the policies and procedures.

Recommendation 5: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to ensure that all departing officials within its purview, including the Secretary of State, sign a separation form (DS-109) certifying that they have surrendered all Federal records and classified or administratively controlled documents. In addition, staff should ensure that all incoming officials within its purview, including the Secretary, are thoroughly briefed on their records preservation and retention responsibilities, including records contained on personal email accounts.

Management Response: In its May 16, 2016, response, the Executive Secretariat concurred with this recommendation. It noted that it is instituting a process whereby completed DS-109 forms are placed in the employee's permanent electronic performance files to ensure they are easily accessible.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation of this process.

Recommendation 6: The Department's Transparency Coordinator should work with the Office of Information Programs and Services to develop a quality assurance plan to promptly identify and address Department-wide vulnerabilities in the records preservation process, including lack of oversight and the broad inaccessibility of electronic records.

Management Response: In her May 16, 2016, response, the Transparency Coordinator concurred with this recommendation. She noted that this plan will be part of her continuing efforts, in coordination with the Office of Information Programs and Services and the Executive Secretariat, to improve overall governance of the Department's information, including how it is captured, stored, shared, disposed of, and archived.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts a copy of the quality assurance plan.

Recommendation 7: The Bureau of Information Resource Management should

- issue regular notices to remind Department employees of the risks associated with the use of non-Departmental systems;
- provide periodic briefings on such risks to staff at all levels; and
- evaluate the cost and feasibility of conducting regular audits of computer system usage to ascertain the degree to which Department employees are following the laws and policies concerning the use of personal email accounts.

Management Response: In its May 23, 2016, response, the Bureau of Information Resource Management concurred with this recommendation. It noted that it will continue to issue regular notices regarding the risks associated with the use of non-Departmental systems. With regard to the evaluation of the cost and feasibility of regular computer system audits, the Bureau has considered such an effort but has concluded that audits conducted on such a wide scale would not be beneficial or feasible, especially because the Department already conducts continuous monitoring to ensure the integrity of the Department's networks and systems.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation of additional educational efforts.

Recommendation 8: The Director General of the Foreign Service and Director of Human Resources should amend the *Foreign Affairs Manual* to provide for administrative penalties for Department employees who (1) fail to comply with recordkeeping laws and regulations or (2) fail to comply with Department policy that only authorized information systems are to be used to conduct day-to-day operations. The amendment should include explicit steps employees should take if a reasonable suspicion exists that documents are not being preserved appropriately, including a reminder that the Office of Inspector General has jurisdiction to investigate and refer to appropriate authorities suspected violations of records preservation requirements.

Management Response: In its May 23, 2016, response, the Department concurred with this recommendation. It will revise the FAM accordingly. The Department also noted that under 3 FAM 4370, it currently has authority to discipline violations of any administrative regulations that do not provide a penalty.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation of the revision.

APPENDIX A: RELEVANT LAWS AND POLICIES DURING THE TENURES OF THE FIVE MOST RECENT SECRETARIES OF STATE

Madeleine Albright (January 23, 1997 – January 20, 2001)

***Foreign Affairs Manual* (FAM) and *Foreign Affairs Handbook* (FAH) Requirements for Use of Non-Departmental Systems:** Since 1996, the FAM directed Department of State (Department) systems managers to ensure that privately owned computers were not installed or used in any Department office building.[1]

Applicable Cybersecurity Provisions and Related Guidance: In 1988, Congress enacted the Computer Security Act to require all Federal agencies to identify computer systems containing sensitive information, conduct computer security training, and develop computer security plans.[2] Office of Management and Budget (OMB) Circular A-130 (Appendix III) required Federal agencies to establish security programs containing specified elements, including development of a System Security Plan, assignment of responsibility for security to individuals knowledgeable in information security technology, and regular review of information system security controls. The FAM did not contain specific computer or cybersecurity provisions.

Statutory and Regulatory Requirements for Email Records Preservation: The Federal Records Act of 1950 requires the head of every Federal agency to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency."[3] The agency head is also required to establish and maintain an active, continuing program for the economical and efficient management of agency records that provides for:

- Effective controls over the creation and the maintenance and use of records in the conduct of current business;
- Cooperation with the Archivist in applying standards, procedures, and techniques designed to improve the management of records, promote the maintenance and security of records deemed appropriate for preservation, and facilitate the segregation and disposal of records of temporary value; and
- Compliance with Federal law and regulations.[4]

As part of this program, the agency head must establish safeguards against the removal or loss of records, including making it known to agency employees that agency records may not be

[1] 12 FAM 625.2-1 (April 12, 1996).

[2] Pub. L. No. 100-235 (January 8, 1988).

[3] 44 U.S.C. § 3101.

[4] 44 U.S.C. § 3102. 44 U.S.C. § 3102(3) specifically references "compliance with sections 2101-2117, 2501-2507, 2901-2909, and 3101-3107, of this title and the regulations issued under them."

unlawfully alienated or destroyed and that penalties exist for the unlawful removal or destruction of records.[5] The agency head must notify the Archivist of any actual, impending, or threatened unlawful removal, defacing, alteration, corruption, deletion, erasure, or other destruction of records in the agency's custody.[6] The Federal Records Act define records broadly as

> all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government ... or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.[7]

The regulations issued by the National Archives and Records Administration (NARA) in title 36 of the Code of Federal Regulations (C.F.R.) that were in effect during Secretary Albright's tenure specified actions that must be taken by an agency in establishing a records program. These included:

- Assigning an office the responsibility for the development and implementation of agency-wide programs to identify, develop, issue, and periodically review recordkeeping requirements for records for all agency activities at all levels and locations in all media including paper, microform, audiovisual, cartographic, and electronic (including those created or received using electronic mail);
- Integrating programs for the identification, development, issuance, and periodic review of recordkeeping requirements with other records and information resources management programs of the agency;
- Issuing a directive establishing program objectives, responsibilities, and authorities for agency recordkeeping requirements;
- Establishing procedures for the participation of records management officials in developing new or revised agency programs, processes, systems, and procedures in order to ensure that adequate recordkeeping requirements are established and implemented;
- Ensuring that adequate training is provided to all agency personnel on policies, responsibilities, and techniques for the implementation of recordkeeping requirements and the distinction between records and non-record materials, regardless of media, including those materials created by individuals using computers to send or receive electronic mail;

[5] 44 U.S.C. § 3105.

[6] 44 U.S.C. § 3106.

[7] 44 U.S.C. § 3301 (amended 2014). The regulations stated that the medium may be "paper, film, disk, or other physical type or form" and that the method of recording may be "manual, mechanical, photographic, electronic, or any other combination of these or other technologies." 36 C.F.R. § 1222.12(b)(2) (1990).

- Developing and implementing records schedules for all records created and received by the agency;
- Reviewing recordkeeping requirements, as part of the periodic information resources management reviews; and
- Reminding all employees annually of the agency's recordkeeping policies and of the sanctions provided for the unlawful removal or destruction of Federal records.[8]

The regulations explicitly noted that "messages created or received on electronic mail systems may meet the definition of record."[9] Furthermore, the regulations required agencies to develop procedures to ensure that departing officials do not remove Federal records from agency custody.[10] The regulations gave further guidance as to what constitutes a Federal record, specifying that records are those documents that:

- Document the persons, places, things, or matters dealt with by the agency;
- Facilitate action by agency officials and their successors in office;
- Make possible a proper scrutiny by the Congress or other duly authorized agencies of the Government;
- Protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions;
- Document the formulation and execution of basic policies and decisions and the taking of necessary actions, including all significant decisions and commitments reached orally; or
- Document important board, committee, or staff meetings.[11]

The regulations issued by NARA included separate provisions on electronic records management, including email.[12] The requirements for electronic records management largely matched those for general records management, but they did require integrating electronic records management with other records and information resources management and ensuring that adequate training is provided for users of electronic mail systems on recordkeeping requirements.[13] The management of email records had to include instructions on preservation of data regarding transmission, calendar and task lists, and acknowledgements.[14] Agencies were restricted from storing the recordkeeping copy of email messages solely on the electronic mail

[8] 36 C.F.R. § 1222.20 (1995).

[9] 36 C.F.R. § 1222.34(e) (1995). Even prior to the issuance of this provision, emails would have been considered a Federal record based on the broad definition of "record" in the Federal Records Act. 44 U.S.C. § 3301.

[10] 36 C.F.R. § 1222.40 (1990). Even for non-records, the regulations permit removal only with the approval of the head of the agency or the individual authorized to act for the agency on matters pertaining to agency records. 36 C.F.R. § 1222.42.

[11] 36 C.F.R. § 1222.38 (1990).

[12] 36 C.F.R. part 1234 (1995).

[13] 36 C.F.R. § 1234.10 (1995).

[14] 36 C.F.R. § 1234.24(a) (1995).

system, unless the system was able to meet regulatory requirements.[15] If an agency used paper files as its recordkeeping system, it was required to print email records and the related transmission and receipt data.[16]

The regulations also noted that the use of external communications systems to which an agency has access, but which are neither owned nor controlled by the agency, does not alter in any way the agency's obligation under the Federal Records Act. Specifically, the regulations provided that

> agencies with access to external electronic mail systems shall ensure that Federal records sent or received on these systems are preserved in the appropriate recordkeeping system and that reasonable steps are taken to capture available transmission and receipt data needed by the agency for recordkeeping purposes.[17]

The regulations also focused on the security of electronic records, requiring an effective records security program that ensures that only authorized personnel have access to electronic records; provides for backup and recovery of records; ensures that appropriate agency personnel are trained to safeguard sensitive or classified electronic records; minimizes the risk of unauthorized alteration or erasure of electronic records; and ensures that electronic records security is included in computer systems security plans.[18]

FAM and FAH Requirements for Email Records Preservation: The FAM largely mirrored the statutory requirements. It created a Records Management Program headed by the Chief of the Records Management Branch within the Bureau of Administration (A).[19] The FAM required that all official files must remain in the custody of the Department and must be maintained in accordance with the *Records Management Handbook*, and it prohibited Department employees from improperly removing, retiring, transferring, or destroying Department records.[20] The FAM noted that it is the responsibility of all Department employees and contractors to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the Department."[21]

The FAM emphasized that "all employees must be aware that some of the variety of the messages being exchanged on E-mail are important to the Department and must be preserved; such messages are considered Federal records under the law."[22] It gave examples of emails that could constitute agency records, such as email providing key substantive comments on a draft

[15] 36 C.F.R. § 1234.24(b)(2) (1995).

[16] 36 C.F.R. § 1234.24(d) (1995).

[17] 36 C.F.R. § 1234.24(a)(4) (1995).

[18] 36 C.F.R. § 1234.28 (1995).

[19] 5 FAM 413.1 (October 30, 1995).

[20] 5 FAM 422.1 (October 30, 1995); 5 FAM 423.1 (October 30, 1995).

[21] 5 FAM 413.10 (October 30, 1995).

[22] 5 FAM 443.1(c) (October 30, 1995).

action memorandum; email providing documentation of significant Department decisions and commitments reached orally; and email conveying information of value on important Department activities, such as data on significant programs specially compiled by posts in response to a Department solicitation.[23] The FAM gave instructions on how to preserve email records, noting that

> until technology allowing archival capabilities for long-term electronic storage and retrieval of E-mail messages is available and installed, those messages warranting preservation as records (for periods longer than current E-mail systems routinely maintain them) must be printed out and filed with related records.[24]

For departing employees, the FAM gave the administrative section of each office, bureau, or post the responsibility for reminding all employees who are about to leave the Department or the Foreign Service of the laws and regulations pertaining to the disposition of personal papers and official records; seeing that form OF-109, Separation Statement, is executed for each departing employee and is forwarded to the Office of Personnel for filing in the employee's Official Personnel Folder; and advising departing officials ranked Assistant Secretary and above, or Ambassador, to consult with the Department's Records Officer about depositing in the National Archives or a Presidential archival depository papers that they may have accumulated during their tenure and that may have historical interest.[25] Form OF-109 required the employee to certify that "I have surrendered to responsible officials all unclassified documents and papers relating to the official business of the Government acquired by me while in the employ of the Department."

Other Preservation Guidance: On February 3, 1997, at the beginning of Secretary Albright's tenure, the Office of the Secretary's Executive Secretary sent a memorandum to all Assistant Secretaries on "Records Responsibilities and Reviews." The memorandum referred to a Department Notice on the subject, as well as the Federal Records Act and 5 FAM 443, which covered email records. The memorandum stated that information maintained in email may constitute a record if it meets the statutory definition of a record and stated, "You need not preserve every e-mail message. If a record in electronic media or electronic mail must be preserved, print the files or messages and place the paper record in the appropriate official file; or continue to maintain electronically if feasible."

On July 28, 2000, a notice reminded all Department employees to preserve emails that qualify as records, stating that "those messages containing information that documents Departmental

[23] 5 FAM 443.2(d) (October 30, 1995).

[24] 5 FAM 443.3 (October 30, 1995). For emails considered records, the FAM required preserving the email message, any attachments, and transmission data such as sender, addressee, cc's, and the date and time sent. If the email system did not print this necessary data, employees were instructed to annotate the printed copies with that data.

[25] 5 FAM 413.9 (October 30, 1995).

policies, programs, and activities must be preserved in paper form." It instructed employees to print out such emails and file them with related paper records.

In August 2000, the Bureau of Administration published a Briefing Booklet for Departing Officials on "Senior Officials and Government Records" that included a signed letter from the Secretary stating that records "must be preserved to enhance our national archives and to provide accurate and complete records." The Secretary also noted that "we [senior officials] have a special obligation as the officials who welcomed in a new century and technological era to preserve e-mail messages as federal records, as appropriate."

A December 2000 cable to all ambassadors and administrative officers reminded departing officials to not remove any papers, whether personal or official, from the Department until such materials have been reviewed to ensure compliance with records laws and regulations.[26] It noted that electronic records must be preserved by printing the files or messages and placing the paper record in the appropriate official file.

Colin Powell (January 20, 2001 – January 26, 2005)

FAM and FAH Requirements for Use of Non-Departmental Systems: Beginning in December 2002, the FAM required all Department facilities to use the Department's primary Internet connection, OpenNet, to establish Internet connectivity.[27] OpenNet provided improved information management and heightened information security throughout the Department. If a bureau or post wanted an exception to this policy, it was required to request a waiver.[28]

The Department established rules in May 2004 regulating the use of non-government information systems, called Dedicated Internet Networks (DINs), to access the Internet.[29] A DIN is a stand-alone information network, such as a local network or server, with dedicated Internet access provided by a commercial Internet service provider (ISP). DINs were not to be used to carry out Department business or to transmit sensitive but unclassified (SBU) information. All bureaus and posts were required to submit a waiver to request an exception in order to use a commercial Internet connection for a stand-alone local network or server. The request for a waiver needed to contain detailed information about the network or server, including an explanation of compliance with Department's standards and specific reasons why OpenNet did not meet the requester's official business requirements. The FAM required all waivers to be approved by the Department's Information Technology Change Control Board (IT CCB).[30] According to the IT CCB, it approved approximately 180 such waivers during the first year this provision was in effect.

[26] 00 STATE 228951.

[27] 5 FAM 871 (December 30, 2002). At the time, OpenNet was referred to as "OpenNet Plus."

[28] 5 FAM 872 (December 30, 2002).

[29] 5 FAM 874.2 (May 4, 2004).

[30] 5 FAM 874.2 (May 4, 2004).

Applicable Cybersecurity Provisions and Related Guidance: The E-Government Act, signed into law in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the Act, the Federal Information Security Management Act (FISMA), gave the National Institute of Standards and Technology (NIST) responsibility to develop Federal Government information security standards and guidelines.[31]

Statutory and Regulatory Requirements for Email Records Preservation: The requirements in the Federal Records Act of 1950 and related regulations in title 36 of the C.F.R. did not change.

FAM and FAH Requirements for Email Records Preservation: The requirements in the FAM generally had not changed from Secretary Albright's tenure. However, in 2002, the Department added a section to the FAM on email usage that included a requirement that email users "determine the significance and value of information created on e-mail systems [and] determine the need to preserve those messages that qualify as records."[32] In 2004, the FAM was amended to designate the Director of the Office of Information Programs and Services (IPS) as the Department's Records Officer.[33] This amendment also noted that "email sent or received as a Department official is not personal."[34] Finally, the amendment assigned the responsibilities related to departing officials, including ensuring the OF-109 was signed, to Management Officers, but eliminated the requirement that the OF-109 be filed in the employee's personnel folder.[35]

Other Preservation Guidance: On August 9, 2004, the Executive Secretary sent a memorandum to all Under Secretaries and Assistant Secretaries entitled "Refresher on Records Responsibilities and Review." The memorandum stated that:

> Departing officials may not remove any documentary materials, whether personal or official and whether in written or electronic form, from the Department until they have been reviewed by records and security officers to ensure compliance with records laws and regulations. ... In addition, departing officials must ensure that all record material they possess is incorporated in the Department's official files. ... Finally, the administrative section of each office and bureau in the Department will ensure that departing officials receive a mandatory briefing and that all departing officials will execute a Separation Statement (OF-109) certifying that they have not retained in their possession classified or administratively controlled documents.

---

[31] E-Government Act of 2002 (Pub. L. No. 107-347), Title III, Information Security, titled Federal Information Security Management Act of 2002, 116 STAT. 2946 (December 17, 2002). NIST did not promulgate guidance on minimum security requirements until March 2006.

[32] 5 FAM 751.4 (February 27, 2002).

[33] 5 FAM 414.2 (September 17, 2004).

[34] 5 FAM 415.1 (September 17, 2004).

[35] 5 FAM 414.7 (September 17, 2004).

In December 2004, NARA issued a bulletin to remind heads of Federal agencies that official records must remain in the custody of the agency and that they must notify officials and employees that there are criminal penalties for the unlawful removal or destruction of Federal records.[36] Employees may remove extra copies of records or other work-related non-record materials when they leave the agency with the approval of a designated agency official such as the Records Officer or legal counsel. It also noted that "officials and employees must know how to ensure that records are incorporated into files or electronic recordkeeping systems, especially records that were generated electronically on personal computers." Further, the bulletin stated that, "in many cases, officials and employees intermingle their personal and official files. In those cases, the agency may need to review and approve the removal of personal material to ensure that all agency policies are properly followed."

A January 2005 cable to all embassies, posts, and offices reminded them of their responsibilities to preserve records under the Federal Records Act and noted that responsibility for implementing and administering records policies and procedures is given to the Management Section of each Department office.[37]

Condoleezza Rice (January 26, 2005 – January 20, 2009)

FAM and FAH Requirements for Use of Non-Departmental Systems: In November 2005, the FAM listed the connection of prohibited hardware or electronic devices to a Department Automated Information System (AIS) as a cybersecurity violation.[38] In 2007, the Department restated this provision to prohibit the connection of "unauthorized hardware/electronic devices to Department networks," which included non-Department-owned hardware/electronic devices.[39]

Also in November 2005, the Department adopted the policy that normal day-to-day Internet operations are to be conducted on an authorized AIS designed with the proper level of security control to provide authentication and encryption to ensure confidentiality and integrity for transmitting Departmental SBU data and information.[40] Employees with a valid business need may transmit SBU information over the Internet unencrypted so long as they carefully consider that unencrypted emails can pass through foreign and domestic controlled ISPs, putting the confidentiality and integrity of the information at risk. The FAM further specified that employees transmitting SBU information outside the Department's OpenNet network on a regular basis to the same non-Departmental email address should obtain a secure technical solution for those Internet transmissions from the Bureau of Information Resource Management (IRM).[41] The FAM

[36] NARA, *Protecting Federal records and other documentary materials from unauthorized removal*, Bulletin No. 2005-03 (December 22, 2004).

[37] 05 STATE 013345 (January 24, 2005).

[38] 12 FAM 592.2 (November 1, 2005).

[39] 12 FAM 592.2 (January 10, 2007).

[40] 12 FAM 544.3 (November 4, 2005).

[41] 12 FAM 544.2 (November 4, 2005).

noted that SBU information resident on personally owned computers is generally more susceptible to cyber-attacks and/or compromise than information on government-owned computers connected to the Internet.[42] All employees who possessed SBU information on personally owned computers must ensure adequate and appropriate security for the SBU information.[43]

In 2008, the Department amended the FAM to define "remote processing" as the processing of Department information on non-Department-owned systems at non-Departmental facilities.[44] Offices that allow employees to remotely process SBU information must ensure that appropriate administrative, technical, and physical safeguards are maintained to protect the confidentiality and integrity of records.[45] Employees are prohibited from storing or processing SBU information on non-Department-owned computers unless it is necessary in the performance of their duties.[46] Employees must (1) ensure that SBU information is encrypted; (2) destroy SBU information on their personally owned and managed computers and removable media when the files are no longer required; and (3) when using personally owned computers, implement and regularly update basic home security controls, including a firewall, anti-spyware, antivirus, and file-destruction applications, and if those computers are networked, also ensure the same basic controls, plus NIST-certified encryption, for all computers on the network.[47]

Also in 2008, the Department eased the FAM restriction regarding the use or installation of non-Federal-Government-owned computers in any Department facility; such use was now allowed with the written approval of the Bureau of Diplomatic Security (DS) and IRM with certain exceptions.[48]

Applicable Cybersecurity Provisions and Related Guidance: The Department implemented the Cyber Security Incident Program (CSIP) in November 2005 to improve protection of the Department's unclassified/SBU cyber infrastructure by identifying, evaluating, and assigning responsibility for breaches of cybersecurity.[49] CSIP focused on accountability of personnel for actions leading to damage or risk to Department information systems and infrastructure, even when only unclassified material or information is involved.[50] Cybersecurity incidents are defined as acts against, or failure to protect, the Department's unclassified cyber infrastructure.[51]

---

[42] 12 FAM 544.3 (November 4, 2005).

[43] 12 FAM 544.3 (November 4, 2005).

[44] 12 FAM 682.1 (August 4, 2008).

[45] 12 FAM 682.2-4 (August 4, 2008).

[46] 12 FAM 682.2-4 (August 4, 2008).

[47] 12 FAM 682.2-5 (August 4, 2008). Although the FAM chapter relating to remote access and processing was amended in 2009, 2011, 2014, and 2015, these basic requirements did not change.

[48] 12 FAM 625.2-1 (July 28, 2008).

[49] 12 FAM 591.1(a) (November 1, 2005).

[50] 12 FAM 591.1 (November 1, 2005).

[51] 12 FAM 592 (January 10, 2007).

Reporting cybersecurity incidents is every employee's responsibility, and each employee must be familiar with the list of cybersecurity infractions and violations.[52] Employees must inform their Information Systems Security Office and their Regional or Bureau Security Officer when any improper cybersecurity practice comes to their attention.[53] Improper security practices include personnel compromising the confidentiality of sensitive information, deliberate introduction of a malicious program code, and use of encryption to conceal an unauthorized act, such as the transfer of SBU information to an unauthorized individual.[54]

NIST was tasked with responsibility to develop Federal standards and guidelines to implement FISMA. NIST responded in February 2004 with Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, which established security categories for both information and information systems that are used in conjunction with vulnerability and threat information for assessing the risk to an organization.[55] This was followed in March 2006 by FIPS Publication 200, which specified minimum security requirements for information and information systems supporting Federal agencies. NIST's announcement of the publication of FIPS Publication 200 noted

> this standard is applicable to: (i) all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and (ii) all federal information systems other than those information systems designated as national security systems as defined in [44 U.S.C. § 3552(b)(6)].

Section 3 of FIPS 200 sets forth 17 specifications for minimum security requirements, including the following:

- The Audit and Accountability specification states: "Organizations must (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions."
- The Risk Assessment specification states: "Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational

[52] 12 FAM 592.4 (January 10, 2007).

[53] 12 FAM 592.4 (January 10, 2007).

[54] 12 FAM 592.1 and 592.2 (January 10, 2007).

[55] NIST, FIPS PUB 199: *Standards for Security Categorization of Federal Information and Information Systems* (February 2004).

information systems and the associated processing, storage, or transmission of organizational information."

- The System and Communications Protection specification states: "Organizations must (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

Federal agencies were required to comply with these standards by March 2007.[56]

In 2007, the Department adopted rules implementing these FISMA requirements, including the requirement that non-Departmental information systems that process or store bureau-sponsored Department information on behalf of the Department maintain a baseline of minimum security controls to protect Department information and information systems.[57] Key personnel identified to perform certification and accreditation of non-Departmental systems must not be involved with its development, implementation, or operation, or be under the sponsoring bureau's direct management authority.[58]

DS reported to the Office of Inspector General that, in 2005, the Bureau of Intelligence and Research (INR) issued guidance permitting BlackBerry devices to be used inside secure areas. However, in January 2006, the Office of the Director of National Intelligence issued a clear prohibition on such use, and the INR guidance was immediately rescinded.

Statutory and Regulatory Requirements for Email Records Preservation: The requirements in the Federal Records Act of 1950 had not changed. The records requirements in title 36 of the C.F.R. were also largely the same, except that, in 2006, NARA amended the regulations to allow agencies to store transitory email records (which have minimal or no documentary or evidential value) on an email system rather than requiring employees to print and file them or store them in a recordkeeping system, as long as the transitory records are maintained through the applicable NARA-approved retention period.[59]

FAM and FAH Requirements for Email Records Preservation: The requirements in the FAM generally had not changed. In 2005, the FAM was amended to include a reminder that "every Department of State employee must create and preserve records that properly and adequately

[56] NIST, FIPS PUB 200: *Minimum Security Requirements for Federal Information and Information Systems* (March 2006).

[57] 5 FAM 1065.1-6 (February 22, 2007); 5 FAH-11 H-411.4 (June 25, 2007).

[58] 5 FAH-11 H-411.5 (June 25, 2007).

[59] 71 Fed. Reg. 8807 (February 21, 2006) (amending 36 C.F.R. § 1234.24). NARA also amended 36 C.F.R. § 1234.32 to provide a NARA-approved disposition authority for transitory emails.

document the organization, functions, policies, decisions, procedures, and essential transactions of the Department."[60]

Other Preservation Guidance: A February 2005 cable drafted by the Bureau of Administration and sent over the Secretary's name to all embassies and posts and an announcement to all employees reminded departing officials not to remove any papers until they have been reviewed to ensure compliance with records laws and regulations.[61]

In December 2005, NARA issued a bulletin that reminded agencies that all electronic records created and received by agencies are subject to the same existing statutory and regulatory records management requirements as records in other formats and on other media.[62]

A February 2007 cable drafted by the Bureau of Administration and sent over the Secretary's name to all embassies and posts and an announcement to all employees were distributed to remind employees that, until the new State Messaging and Archive Retrieval Toolset (SMART) is implemented, email, Short Message Service messages, or instant messages that qualify as records must be printed and filed with related paper records, including any attachments and transmission data.[63]

In April, June, and October 2008, announcements to all employees again reminded departing employees not to remove any papers until they had been reviewed. They also stated that "e-mail messages must generally be printed out and filed with related paper records."[64]

On January 15, 2009, the Under Secretary for Management issued a memorandum to all Under Secretaries, Assistant Secretaries, Executive Directors, and Post Management Officers on "Preserving Electronically the Email of Senior Officials upon their Departure." The memorandum required bureaus to copy the email accounts of senior departing officials onto CDs and deliver those CDs to IPS. The requirement was applicable to political appointees, not career staff, and was put in place to supplement the traditional print and file policy for record email.

Hillary Clinton (January 21, 2009 – February 1, 2013)

---

[60] 5 FAM 422.3 (October 11, 2005).

[61] 05 STATE 018818; Department of State, *Procedures for the Removal of Personal Papers and Non-Record Material*, Announcement No. 2005_02_017, February 3, 2005.

[62] NARA, *NARA Guidance for Implementing Section 207(e) of the E-Government Act of 2002*, Bulletin No. 2006-02 (December 15, 2005).

[63] 07 STATE 024044; Department of State, *Records Management Procedures*, Announcement No. 2007_02_147, February 28, 2007.

[64] Department of State, *Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material*, Announcement No. 2008_04_089, April 17, 2008; Department of State, *Reminder – Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material*, Announcement No. 2008_06_095, June 16, 2008; Department of State, *Reminder – Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material*, Announcement No. 2008_10_087, October, 16, 2008.

FAM and FAH Requirements for Use of Non-Departmental Systems: A December 2009 FAM provision states that non-Department-owned personal digital assistants (PDAs) may only be turned on and used within Department areas that are strictly unclassified (such as the cafeteria) and may not connect with a Department network except via a Department-approved remote-access program.[65]

Applicable Cybersecurity Provisions and Related Guidance: To meet the requirements of FISMA, the Department implemented a mandatory annual requirement for all Department computer users to take Cybersecurity Awareness training.[66]

Beginning in 2009, the Cyber Threat Analysis Division (CTAD) in DS issued regular notices to Department computer users highlighting cybersecurity threats. CTAD notices addressed BlackBerry security vulnerabilities, citing this device as a weak link in a computer network.[67] CTAD warned that BlackBerry devices must be configured in accordance with Department security guidelines.

CTAD's concerns also included cybersecurity risks faced during international travel. According to an article posted by CTAD, digital threats begin immediately after landing in a foreign country. A primary threat is traced to the traveler's mobile device (BlackBerry or other smart device) which is necessarily connected to the local cellular tower. This connection gives foreign entities the opportunity to intercept voice and email transmissions immediately after the traveler arrives overseas.[68]

The E-Government Act and NIST FIPS PUB 200 were unchanged.

Statutory and Regulatory Requirements for Email Records Preservation: The requirements in the Federal Records Act of 1950 had not changed. In October 2009, NARA published a final rule that revised and reorganized its records management regulations.[69] The existing requirements were largely retained, but renumbered.[70] New responsibilities were added to agencies' records program duties, including assigning records management responsibilities in each program/mission to ensure incorporation of recordkeeping requirements into agency

---

[65] 12 FAM 683.2-3 (December 2, 2009).

[66] 13 FAM 331 (December 22, 2010).

[67] CTAD, *Security Checklist* (December 15, 2009); CTAD, *Cyber Security Awareness* (March 3, 2011).

[68] *How to manage cybersecurity risks of international travel* (September 15, 2010) by (ISC)2 Government Advisory Board Executive Writers Bureau (posted by CTAD on January 26, 2011).

[69] 74 Fed. Reg. 51004 (Oct 2, 2009).

[70] For example, the requirements of an agency records program were moved from 36 C.F.R. § 1222.20 to 36 C.F.R. §§ 1220.30, 1220.32, and 1220.34. Requirements regarding departing officials were moved from 36 C.F.R. §§ 1222.40, 1222.42 to 36 C.F.R. §§ 1222.18, 1222.24(a)(6).

programs.[71] The new section on managing email records required preservation of email attachments that are an integral part of the record.[72] It also stated:

> Agencies that allow employees to send and receive official electronic mail messages using a system not operated by the agency must ensure that Federal records sent or received on such systems are preserved in the appropriate agency recordkeeping system.[73]

FAM and FAH Requirements for Email Records Preservation: The requirements in the FAM and FAH generally had not changed.

Other Preservation Guidance: In June 2009, the Department sent an announcement regarding preservation of email messages.[74] It reminded employees of the requirement to preserve email records, citing the FAM and C.F.R. provisions, and noted that, until SMART becomes available, employees must print and file emails that are Federal records.

In November 2009, the Department sent a cable to all embassies and posts and an announcement to all employees reminding them that all Department employees have records management responsibilities.[75] It noted that Federal records can be found "in any media including e-mail, instant messages, social media, etc."

On November 28, 2011, President Obama issued a memorandum to the heads of executive departments and agencies requiring them to submit a report to the Archivist and the Director of OMB that

> (i) describes the agency's current plans for improving or maintaining its records management program, particularly with respect to managing electronic records, including email and social media, deploying cloud based services or storage solutions, and meeting other records challenges; (ii) identifies any provisions, or omissions, in relevant statutes, regulations, or official NARA guidance that currently pose an obstacle to the agency's adoption of sound, cost effective records management policies and practices; and (iii) identifies policies or programs that, if included in the Records Management Directive required by section 3 of this memorandum or adopted or implemented by NARA, would assist the agency's efforts to improve records management.[76]

---

[71] 36 C.F.R. § 1220.34 (2010).

[72] 36 C.F.R. § 1236.22(a)(2) (2010).

[73] 36 C.F.R. § 1236.22(b) (2010).

[74] Department of State, *Preserving Electronic Message (E-mail) Records*, Announcement No. 2009_06_090, June 17, 2009.

[75] 09 STATE 120561; Department of State, *Records Management Responsibilities*, Announcement No. 2009_11_125, November 23, 2009.

[76] *Presidential Memorandum – Managing Government Records* (November 28, 2011).

In August 2012, OMB and NARA issued a memorandum to the heads of executive departments, agencies, and independent agencies in part directing agencies to eliminate paper and use electronic recordkeeping. Per this memorandum, agencies will be required to manage all email records in an electronic format by December 31, 2016. [77]

John Kerry (February 1, 2013 – Present)

FAM and FAH Requirements for Use of Non-Departmental Systems: On May 1, 2014, the Department amended the definition of a DIN to require the DIN to be on a Department-owned and operated discrete non-sensitive unclassified local area network that is not connected to any other Department system.[78] In addition, the domestic approving authority for a DIN changed from the Department's IT CCB to the relevant bureau's Executive Director or equivalent.[79]

A September 2014 FAH provision stated that supervisors must exercise "particular care and judgment" in allowing users to remotely process SBU information and must advise users that all non-Department-owned storage media containing Department SBU information must be encrypted with products certified by NIST.[80] Employees were prohibited from remotely processing classified or SBU/NOFORN (not releasable to foreign nationals) information.[81] Employees were also required to (1) exercise "particular care and judgment" in remotely processing SBU information; (2) destroy SBU files saved on personally owned and managed information systems and removable media when the files are no longer required; and (3) implement and regularly update basic home security controls, including a firewall, anti-spyware, antivirus, and file-destruction applications. If an employee used a networked personally owned information system, he or she had to ensure that all information systems on the network implemented these security requirements.

The FAH further prohibits the installation of non-Departmental information systems within Department facilities without the written authorization of DS and IRM.[82] This provision replaced an identical FAM provision issued in 2008.

In 2015, a new FAH provision was added regarding non-Department-owned mobile devices. The FAH provision included a rule requiring a 10-foot separation between a PDA and classified processing equipment, a ban on connecting to a Department network except via a Department-

[77] *Memorandum for the Heads of Executive Departments and Agencies and Independent Agencies: Managing Government Records Directive*, M-12-18 (August 24, 2012).

[78] 5 FAM 872 (May 1, 2014).

[79] 5 FAM 872.1 (May 1, 2014).

[80] 12 FAH-10 H-172.1 (September 25, 2014). These provisions are currently located at 12 FAH-10 H-173.1 (January 11, 2016).

[81] 12 FAH-10 H-172.4 (September 25, 2014). These provisions are currently located at 12 FAH-10 H-173.4 (January 11, 2016).

[82] 12 FAH-10 H-112.14-2 (September 19, 2014).

approved remote-access program, and a requirement to conduct normal day-to-day Department operations on a Department information system because it has the proper security controls to protect Department information.[83]

Applicable Cybersecurity Provisions and Related Guidance: The Federal Information Security Modernization Act of 2014, enacted in December 2014, updated FISMA by clarifying the roles of OMB and the Department of Homeland Security, improving security by moving away from paperwork requirements, and making improvements in the way that Federal data breaches are managed and reported.[84] Rules and guidance governing cybersecurity threats have not changed.

Statutory and Regulatory Requirements for Email Records Preservation: In 2014, Congress enacted the Presidential and Federal Records Act Amendments of 2014, which amended several sections of the Federal Records Act.[85] It simplified the definition of record to:

> all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them...[86]

The Act noted that the definition of "recorded information" includes "information created, manipulated, communicated, or stored in digital or electronic form." The Act also added a provision that prohibited agency employees from creating or sending a record from a non-official electronic messaging account unless they copy their official electronic messaging account in the original creation or transmission of the record or forward a complete copy of the record to their official electronic messaging account within 20 days.[87]

The requirements in title 36 of the C.F.R. had not changed.

FAM and FAH Requirements for Email Records Preservation: The requirements in the FAM generally had not changed. However, in October 2014, the Department issued an interim directive superseding some of the FAM requirements.[88] The directive noted that employees may delete personal emails, but that "the only e-mails that are personal or non-record are those that

[83] 12 FAH-10 H-165.4 (May 20, 2015).

[84] Pub. L. No. 113-283 (December 18, 2014).

[85] Pub. L. No. 113-187 (November 26, 2014).

[86] 44 U.S.C. § 3301(a).

[87] 44 U.S.C. § 2911(a).

[88] Department of State, *A Message from Under Secretary for Management Patrick F. Kennedy regarding State Department Records Responsibilities and Policy*, Announcement No. 2014_10_115, October 17, 2014.

do not relate to or affect the transaction of Government business." The directive also noted that departing employees may only take personal papers and non-record materials, subject to review by records officials. It reminded employees that "all federal records generated by employees, including senior officials, belong to the Department of State." Finally, the directive stated that:

> employees generally should not use private e-mail accounts (e.g., Gmail, AOL, Yahoo, etc.) for official business. However, in those very limited circumstances when it becomes necessary to do so, the email messages covering official business sent from or received in a personal account must be captured and preserved in one of the Department's official electronic records systems. The best way for employees to ensure this is to forward e-mail messages from a private account to their respective State account. Private email accounts should not be used for classified information.

In October 2015, the Department updated the FAM to incorporate these requirements.[89]

The responsibilities of Management Officers related to departing employees have not changed since Secretary Powell's tenure; however, in 2015, the Department changed the name of the separation form from OF-109 to DS-109. The pertinent language in the form did not change.[90]

Other Preservation Guidance: In February 2013, the Department sent an announcement to all employees reminding senior officials that they may only take personal papers and non-record materials following a review by a records official to ensure compliance with Federal records laws and regulations.[91]

In August 2013, NARA published a bulletin authorizing agencies to use a "Capstone" approach to managing email records, in lieu of print and file.[92] The Capstone approach allows for the automatic capture of records that should be preserved as permanent from the accounts of officials at or near the top of an agency or an organizational subcomponent. In September 2013, NARA published a bulletin that stated that, "while agency employees should not generally use personal email accounts to conduct official agency business, there may be times when agencies authorize the use of personal email accounts." In these cases, "agency employees must ensure that all Federal records sent or received on personal email systems are captured and managed in

[89] 5 FAM 443.7 (October 23, 2015).

[90] 5 FAM 414.7 (June 19, 2015).

[91] Department of State, *Departing Senior Officials: Government Records and Personal Papers*, Announcement No. 2013_02_122, February 26, 2013.

[92] NARA, *Guidance on a New Approach to Managing Email Records*, Bulletin No. 2013-02 (August 29, 2013). In 2014, NARA and OMB issued guidance on managing emails to be used in conjunction with NARA's Capstone guidance. *Memorandum for the Heads of Executive Departments and Agencies and Independent Agencies: Guidance on Managing Email*, M-14-16 (September 15, 2014).

accordance with agency recordkeeping practices."[93] In 2015, NARA issued guidance on managing other forms of electronic messaging, including social media and texts.[94]

On August 28, 2014, the Under Secretary for Management sent a memorandum to the Office of the Secretary, all Under Secretaries and Assistant Secretaries, and a number of other offices to remind them of their responsibility for creating, managing, and preserving records "regardless of physical format or media." It noted that "records may exist in many formats, including Instant Messages (IM) and records on mobile devices like BlackBerrys, mobile phones, and iPads." It also included specific requirements relating to emails, including:

- At no time during designated senior officials' tenure will their e-mail accounts be cleared, deleted, or wiped for any reason.
- While senior officials may delete personal e-mails, they should be aware that the definition of a personal e-mail is very narrow. The only e-mails that are personal are those that do not relate to or affect the transaction of Government business.
- As a general matter, to ensure a complete record of their activities, senior officials should not use their private e-mail accounts (e.g., Gmail) for official business. If a senior official uses his or her private email account for the conduct of official business, she or he must ensure that records pertaining to official business that are sent from or received on such e-mail account are captured and maintained. The best way to ensure this is to forward incoming emails received on a private account to the senior official's State account and copy outgoing messages to their State account.[95]

[93] NARA, *Guidance for agency employees on the management of Federal records, including email accounts, and the protection of Federal records from unauthorized removal*, Bulletin No. 2013-03 (September 9, 2013).

[94] NARA, *Guidance on Managing Electronic Messages*, Bulletin No. 2015-02 (July 29, 2015).

[95] The Under Secretary sent this same message to all Chiefs of Mission in September 2014. 14 STATE 111506 (September 15, 2014).

APPENDIX B: MANAGEMENT RESPONSES

UNCLASSIFIED

TO: Inspector General – Steve Linick

FROM: Transparency Coordinator - Janice L. Jacobs

SUBJECT: OIG Draft Report – "Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements (ESP-16-03): Responses to Recommendations

In March 2015, Secretary Kerry asked the Office of the Inspector General to review the Department's efforts to preserve a full and complete record of American foreign policy, and our procedures for making that record available to the American public. We welcome the opportunity to respond to your report, *Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements*, the fourth installment of your review. As your reports recognize, through our work with your office, as well as the Department's efforts to meet Presidential and Department directives, we have made great progress towards a better preserved and more accessible public record. As demonstrated in the enclosed responses and comments to your specific recommendations, the Department is committed to continuing to improve. However, I also want to acknowledge and highlight how far we have already come.

For decades, the government has been working to adapt longstanding recordkeeping principles and rules to the email-dominated modern era. The Federal Records Act and the Freedom of Information Act are established pillars of transparent government, but email and other communications technologies create difficult challenges for implementation. As your report describes, over the years the Department has been good at drafting principles on the importance of preserving email; however, only recently have we begun to match results with our aspirations. The National Archives and Records Administration (NARA) has acknowledged that the entire federal government—not just the State Department—continues to grapple with these challenges. In fact, NARA has issued some of its most relevant guidance regarding these matters in the last three years.

Today, I can attest to the Department's goal of leading on these issues in the future. Earlier this year, Secretary Kerry issued a Department-wide notice on the critical importance of the Freedom of Information Act, demonstrating a

commitment to transparency at the most senior level. In September 2015, Secretary Kerry announced my appointment as the Department's Transparency Coordinator to oversee the Department's efforts on these matters. At the time, the Department was already engaged in a process to meet the President's *Managing Government Records* directive, including through the robust work of our Electronic Records Management Working Group. We are on track to meet the benchmarks of the President's directive for 2016; for example, your report notes that the Department is in the process of procuring new technology to manage emails electronically.

In addition, in 2014 the Department issued guidance on the use of personal emails—in effect anticipating later changes to the Federal Records Act—and initiated the Department's implementation of the Capstone program in February 2015 to archive automatically senior officials' emails. Over 200 officials are already covered by Capstone, with more on the way. We also have already closed a number of the recommendations in your first three reports.

Finally, the Executive Secretariat, Bureau of Administration, and other relevant bureaus have established a strong working relationship to improve records management. We are already cataloguing our current holdings of electronic archives, improving the way we search email records, and establishing procedures for archiving records going forward.

As a result of these and other efforts, today the Department is much differently situated than during historical periods described in your report. It is clear that the Department could have done better at preserving emails of Secretaries of State and their senior staff going back several administrations. However, by early 2015, the Department had already taken important steps to address these issues. As noted above, our Electronic Records Management Working Group was already established. In addition, the Department had already received Secretary Clinton's emails and undertook to release over 30,000 of them to the public. The National Archives and Records Administration concluded that our efforts with respect to Secretary Clinton and her senior staff mitigated past problems, as has a federal district court in a suit brought under the Federal Records Act. As you note in the report, you concur with this conclusion.

The way we conduct diplomacy has evolved significantly in recent years from a time when official cables were one of the primary ways we communicated. Modern technology has unquestionably enhanced our mission; however, there is still work to do to ensure that we preserve a record of our work. We look forward

to working with your office in the future on these issues, and remain committed to building on what we have already accomplished.

May 23, 2016

UNCLASSIFIED

TO: Inspector General – Steve Linick

FROM: M – Patrick Kennedy

SUBJECT: Draft report – "Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements" (ESP-16-03 dated May 2016)

Thank you for the opportunity to comment on subject draft report. Over the past year, the Department has taken steps to improve its records management practices and we believe we have made progress. However, more progress can be made, and we are committed to reaching the December 2016 goal set by NARA for email retention and continue advancing sound records management.

Responses to recommendations from bureaus within the M family follow below.

Recommendation 1: The Bureau of Administration should

- issue guidance, including periodic, regular notices, to Department employees to remind them that the use of personal email accounts to conduct official business is discouraged in most circumstances,
- clarify and give specific examples of the types of limited circumstances in which such use would be permissible, and
- instruct employees how to preserve Federal records when using personal email accounts.

Department Response: The Bureau of Administration concurs with this recommendation and will continue to issue guidance on records management practices and policies, and will ensure that this guidance explicitly reminds employees that the use of personal emails accounts to conduct official business is discouraged. Similar to previous records management guidance, such guidance will be provided to employees in writing (via Department Notices and ALDACs) and in appropriate briefings (i.e. training courses, meetings, etc.) to remind employees of their responsibility for preserving documentation of official activities, including emails. The Department will consider additional means by which to inform employees of records management requirements and best practices.

Recommendation 2: The Bureau of Administration should amend the *Foreign Affairs Manual* to reflect the updates to Department recordkeeping systems that provide alternatives to print and file.

Department Response: We concur with this recommendation, but please edit to read "alternatives to print and file emails that are records."

The Bureau of Administration is currently working with the Office of the Transparency Coordinator to update 5 FAM and chapter subparts related to Department's recordkeeping/retention schedules. The goal to eliminate the practice of print and file as the Department's policy and practice for the retention of emails by December 31, 2016, which is also the deadline by which the Department is supposed to implement a solution to manage all emails. All other electronic documents should follow this electronic retention practice by the end of 2019.

Recommendation 7: The Bureau of Information Resource Management (IRM) should

- issue regular notices to remind Department employees of the risks associated with the use of non-Departmental systems;
- provide periodic briefings on such risks to staff at all levels; and
- evaluate the cost and feasibility of conducting regular audits of computer system usage to ascertain the degree to which Department employees are following the laws and policies concerning the use of personal email accounts.

Department Response: The Department concurs with the first two bullet points of this recommendation. IRM will continue to issue regular notices regarding the risks associated with the use of non-Departmental systems.

Regarding the third bullet, audits conducted on such a wide scale would not be beneficial or feasible. Limited use of personal email is acceptable under current policy and allowable under law. The Department already conducts continuous monitoring to ensure the integrity of the Department networks and systems and in fact was a government leader in this regard. State's Continuous Diagnostics and Monitoring which is also known as iPost has been adopted and modified by DHS into the new government-wide Continuous Diagnostics and Mitigation program (CDM). Under 5 FAM 724, the Department can audit an employee's network activity or workstation

use, which includes but is not limited to electronic communication, Internet access, local disk files, and server files when there is suspicion that improper use of government equipment has occurred. In addition, Information Systems Security Officers (ISSOs) worldwide are required to review systems and security logs on a regular basis.

Regarding the first bullet point, the Bureau of Information Resource Management continues to issue notices and provide briefings on risks associated with the use of non-Departmental systems. For example:

- Mandatory PS 800 Cyber Security Awareness Training course
- Informational links
  - https://intranet.ds.state.sbu/DS/SI/CS/Awareness1/Content/Email.aspx for email, or
  - one level higher for other types of awareness information
- Department Notices (recent)
  - 2016_03_128 Global Cyber Foreign Policy Training Workshop on April 25-29, 2016
  - 2016_02_035 Revised 12 FAM 620 and New 12 FAH-10 (Unclassified Cyber Security Policies) are published
  - 2015_11_063 October was National Cyber Security Awareness Month
- IT Customer Service Bulletins (e.g., 7/30/15) and also Information Announcements on http://irm.m.state.sbu/sites/ops/CSO/ITSC/default.aspx
- DS Cybersecurity Awareness In Case You Missed It
- Cyber Security Awareness month – October
- Tips of the Day
  - Tips of the Day and StateNet advertisement on *Protecting SBU Outside the Department* and *Protecting Personal Email Accounts*
- Fact Sheet on *Protecting Personal Email Accounts*
- Fact Sheet on *How to Handle Suspicious Email* (including personal email)
- Fact Sheet on *Email Safety*
- Personal Email Security Best Practices guide
- How to Report Suspicious Messages/Activity on Webmail Accounts guide
- *Notes* blast emails on Personal Email Addresses, Personal Email Reminder, How to Handle Suspicious Email, Sending SBU Over the

Internet, Cloud Computing, Cloud Security, Protecting OpenNet When Accessing Personal Email Accounts
- *Awareness Bulletin* on Personal Email Accounts and Out of Office Messages
- Personal Email Guides (Gmail, Hotmail, Yahoo, Outlook)
- Information Systems Security Officer (ISSO) Role-Based Training – mandatory for ISSOs
- A-100 Foreign Service Generalist class – general overview
- IRM Tradecraft
  - YW319 - IRM Tradecraft for the Information Technology Manager
  - YW387 - Information Resources Management Tradecraft
- Diplomatic Security Training Center (DSTC) summary:
  - For FY 2015 DSTC conducted 80 course sessions in different cybersecurity areas (including those for ISSOs)
  - For FY-2016, DSTC has scheduled 81 different cybersecurity courses
- Ambassador/PO and DCM seminars – overview

We will review whether the material in these notices and courses needs to be updated or expanded.

Recommendation 8: The Director General of the Foreign Service and Director of Human Resources should amend the *Foreign Affairs Manual* to provide for administrative penalties for Department employees who (1) fail to comply with recordkeeping laws and regulations or (2) fail to comply with the requirement that only authorized information systems are to be used to conduct day-to-day operations. The amendment should include explicit steps employees should take if a reasonable suspicion exists that documents are not being preserved appropriately, including a reminder that the Office of Inspector General has jurisdiction to investigate and refer to appropriate authorities suspected violations of records preservation requirements.

> **Department Response:** The Department concurs with this recommendation and will implement it by revising, following any appropriate consultation with the unions, the lists of disciplinary offenses contained at 3 FAM 4377 and 4542 to include explicitly violations of laws, regulations and directives regarding records management, including preservation. (At present, such offenses would fall into general catch-all provisions contained in each list.)

With respect to the second sentence of Recommendation 8, as part of its continuing issuance of records guidance, the Bureau of Administration, in coordination with the Bureau of Human Resources, will include guidance on how and where to raise records management concerns. Such guidance will remind employees of the jurisdiction of the Office of Inspector General.

United States Department of State

Washington, D.C. 20520

May 16, 2016

UNCLASSIFIED

TO: Steve Linick, Inspector General

FROM: Joseph E. Macmanus, Executive Secretary

SUBJECT: Response to Draft OIG Review of Email Records Management and Cybersecurity Requirements Involving the Office of the Secretary

The Executive Secretariat thanks the OIG for the opportunity to respond to this review. The Secretariat values the OIG's study of electronic records management – a Department-wide challenge that we will continue to address. The Secretariat has the following specific responses to the recommendations contained in the report.

Recommendation 3: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to conduct an inventory of all electronic and hard-copy files in its custody and evaluate them to determine which files should be transferred to the Office of Information Programs and Services in accordance with records disposition schedules or Department email preservation requirements.

> **Department Response**: The Executive Secretariat agrees with this recommendation and notes that the inventory of electronic and hard copy files has been ongoing since January 2016. The Executive Secretariat agrees this is an important and necessary project.

Recommendation 4: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to adopt policies and procedures to ensure compliance by all employees within its purview, including the Secretary, with records management requirements. These policies should cover the retirement of records in accordance with records disposition schedules, preservation of email and other electronic records of departing officials, and training of employees in their records preservation responsibilities.

UNCLASSIFIED

Department Response: The Executive Secretariat strongly agrees with the OIG recommendation that it should work closely with the Office of Information Programs and Services to fully implement policies and procedures to improve compliance with records management responsibilities, including the retirement of records in accordance with records disposition schedules, preservation of email and other electronic records of departing officials, and training of employees on their records preservation responsibilities. The Executive Secretariat staff is committed to coordinating closely with the Office of Information Programs and Services to provide updated guidance and training to all staff.

Recommendation 5: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to ensure that all departing officials within its purview, including the Secretary of State, sign a separation form (DS-109) certifying that they have surrendered all Federal records and classified or administratively controlled documents. In addition, staff should ensure that all incoming officials within its purview, including the Secretary, clearly understand their records preservation and retention responsibilities, including records contained on personal email accounts.

Department Response: The Executive Secretariat agrees with the OIG recommendation that it should ensure all departing officials within its purview, including the Secretary of State, sign a separation agreement form (DS-109), and that all incoming staff clearly understand their records preservation and retention responsibilities. The Executive Secretariat is instituting a process whereby employees' completed DS-109 forms are placed in their permanent electronic performance files (eOPF) to ensure they easily accessible.

UNCLASSIFIED

TO: Inspector General – Steve Linick

FROM: Transparency Coordinator – Janice L. Jacobs

SUBJECT: Draft report – "Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements" (ESP-16-03 dated May 2016)

Thank you for the opportunity to comment on subject draft report, which includes the following recommendation:

"The Department's Transparency Coordinator should work with the Office of Information Programs and Services to develop a quality assurance plan to promptly identify and address Department-wide vulnerabilities in the records preservation process, including lack of oversight and the broad inaccessibility of electronic records."

I concur and am happy to comply with your recommendation as part of my continuing efforts, in coordination with the Office of Information Programs and Services (A/GIS/IPS) and the Executive Secretariat (S/ES), to improve overall governance of the Department's information – how it is captured, stored, shared, disposed of, and archived as appropriate. Your findings will help inform these efforts. The report's focus on email records is particularly relevant given that all federal agencies have been directed by the White House and the National Archives and Records Administration (NARA) to manage all email records in an electronic format by December 31 of this year. Department progress towards this goal is well underway with measures either already in place or on the horizon. The Capstone program mentioned in your report, whereby the emails of designated senior officials are all captured and retained permanently, is one such step already taken by the Department.

By December 2019, all permanent electronic records in federal agencies must be managed electronically to the fullest extent possible. This will be a huge undertaking requiring a governance structure for all forms of information created or received by the Department. The Department is committed to getting this right to help assure a 21st century enterprise-wide information management system that advances the Department's goals of increased efficiency, transparency and accountability. We will not succeed without sufficient metrics, quality controls, and general oversight of the system we create. This is why the quality assurance plan you've recommended is so important.

As I move forward, I remain mindful of Secretary Kerry's strong commitment to improving the Department's records management and transparency systems in order to preserve the record of U.S. foreign policy and to share that story with the wider public.

ABBREVIATIONS

A	Bureau of Administration
AIS	Automated Information System
C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
CSIP	Cyber Security Incident Program
CTAD	Cyber Threat Analysis Division
D-MR	Deputy Secretary for Management and Resources
DCIO	Deputy Chief Information Officer
Department	Department of State
DIN	Dedicated Internet Network
DS	Bureau of Diplomatic Security
ERMWG	Electronic Records Management Working Group
FAH	*Foreign Affairs Handbook*
FAM	*Foreign Affairs Manual*
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GAO	Government Accountability Office
INR	Bureau of Intelligence and Research
IPS	Office of Information Programs and Services
IRM	Bureau of Information Resource Management
ISP	Internet service provider

IT CCB	Information Technology Change Control Board
L	Office of the Legal Adviser
M	Under Secretary for Management
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NOFORN	not releasable to foreign nationals
OIG	Office of Inspector General
OMB	Office of Management and Budget
PDA	personal digital assistant
.pst	Personal Storage Table (Microsoft Outlook file format)
S	Office of the Secretary
S/ES	Office of the Secretary, Executive Secretariat
S/ES-EX	Office of the Executive Director, S/ES
S/ES-IRM	Office of Information Resources Management, S/ES
SAO	Senior Agency Official
SBU	sensitive but unclassified
SMART	State Messaging and Archive Retrieval Toolset

OIG TEAM MEMBERS

Jennifer L. Costello, Team Leader, Office of Evaluations and Special Projects
David Z. Seide, Team Leader, Office of Evaluations and Special Projects
Jeffrey McDermott, Office of Evaluations and Special Projects
Robert Lovely, Office of Evaluations and Special Projects
Michael Bosserdet, Office of Inspections
Brett Fegley, Office of Inspections
Kristene McMinn, Office of Inspections
Timothy Williams, Office of Inspections
Aaron Leonard, Office of Audits
Phillip Ropella, Office of Audits
Kelly Minghella, Office of Investigations
Eric Myers, Office of Investigations

HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926
OIG.state.gov/HOTLINE
If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:
OIGWPEAOmbuds@state.gov

UNCLASSIFIED

July 17, 2015

MEMORANDUM

TO: Patrick F. Kennedy, Under Secretary for Management, Department of State

FROM: Steve A. Linick, Inspector General, Department of State
I. Charles McCullough, III, Inspector General, Intelligence Community

SUBJECT: Potential Issues Identified by the Office of the Inspector General of the Intelligence Community Concerning the Department of State's Process for the Review of Former Secretary Clinton's Emails under the Freedom of Information Act (ESP-15-04)

The Office of Evaluations and Special Projects within the Office of Inspector General (OIG) is reviewing the use of personal communications hardware and software by five Secretaries of State and their immediate staffs. This work includes an evaluation of the Department of State's ongoing efforts to publish the emails of former Secretary of State Clinton, which were provided to the Department in December 2014. To assist in the review, OIG consulted with the Office of the Inspector General of the Intelligence Community (ICIG).

ICIG staff conducted a preliminary assessment of the Department's ongoing Freedom of Information Act (FOIA) process for the Clinton emails, including 296 emails publicly released by the Department on May 22, 2015. This preliminary assessment identified four areas that require immediate attention by Department leadership. Attachment A contains OIG's and ICIG's Memorandum, dated June 19, 2015, which makes four recommendations related to these areas. Attachment B contains your June 25, 2015, and July 14, 2015, responses. Based on these responses, OIG and ICIG consider two of these recommendations to be closed, whereas the other two remain unresolved. Attachment C contains more detailed information about the status of each recommendation.

On June 29, 2015, OIG and ICIG sent you a follow-up memorandum providing additional information supporting our concerns about the FOIA process used for the Clinton emails (see Attachment D). Since then, ICIG has received confirmation from IC FOIA officials that several of these emails contained classified IC information, though they were not marked as classified. In addition, at least one of these emails has been released to the public and can be accessed on the Department's FOIA website. OIG and ICIG will continue to assess whether further actions need to be taken to ensure that no additional classified information is publicly released.

Attachments: As stated.

cc: D(MR) - Heather A. Higginbottom

ATTACHMENT A

OIG and ICIG Memorandum to the Department, Dated June 19, 2015

UNCLASSIFIED

June 19, 2015

MEMORANDUM FOR UNDER SECRETARY KENNEDY

FROM: Steve A. Linick, Inspector General, Office of Inspector General, Department of State
I. Charles McCullough, III, Inspector General, Intelligence Community

SUBJECT: Potential Issues Identified by the Office of the Inspector General of the Intelligence Community Concerning the Department of State's Process for the Review of Former Secretary Clinton's Emails under the Freedom of Information Act (ESP-15-04)

Pursuant to a notification letter dated April 16, 2015, the Office of Evaluations & Special Projects within the Office of the Inspector General (OIG) is reviewing the use of personal communications hardware and software by five Secretaries of State and their immediate staffs. On June 4, 2015, OIG notified the Department of State (Department) that this review would include an evaluation of the Department's ongoing efforts to review, categorize, and publish the e-mails of former Secretary of State Clinton, which were provided to the Department in December 2014. To assist in the review, OIG consulted with the Office of the Inspector General of the Intelligence Community (ICIG). As part of the ongoing review, ICIG staff conducted a preliminary assessment of the Department's Freedom of Information Act (FOIA) review process as well as 296 emails released by State FOIA officials on May 22, 2015. This preliminary assessment identified four areas that may require immediate attention by Department leadership. The ICIG Memorandum for the Record containing recommendations and an accompanying cover letter from the Inspector General of the Intelligence Community are attached.

Please provide comments to the ICIG Memorandum and information on actions taken or planned on each of the recommendations, no later than close of business, Friday, June 26, 2015, to Inspector General Steve A. Linick at [redacted] and to Inspector General I. Charles McCullough at [redacted]. If you have any questions about this request, please contact I. Charles McCullough, III at [redacted]. Thank you for your attention to this matter.

Attachments: As stated.

cc: D-MR - Heather A. Higginbottom

INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY
WASHINGTON, DC 20511

15 June 2015

The Honorable Steve Linick
Inspector General
Department of State
2201 C Street, NW (SA-3, Suite 8100)
Washington, DC 20520

Dear Mr. Linick:

(U//~~FOUO~~) Thank you for reaching out to my office to assist you in your current review entitled "Use of Personal Communications Hardware and Software by Five Secretaries of State and Their Immediate Staffs." Thus far, our assistance has been tailored to reviewing State Department's Freedom of Information Act (FOIA) process and how classified information is safeguarded in that process.

(U//~~FOUO~~) Our preliminary review identified four areas that may require immediate attention by State FOIA officials, in coordination with Intelligence Community FOIA officials. Those areas are detailed in the attached memorandum. My team has briefed your team members on these developments and will continue to refine findings and recommendations as the review progresses.

Sincerely,

I. Charles McCullough, III

cc: David Seide, Counselor,
State Department Office of Inspector General

[redacted] General Counsel
Office of the Inspector General of the Intelligence Community

Attachment:
(U) MFR, [redacted] (dtd 15 June, 2015) (U//~~FOUO~~)

OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY
INSPECTIONS AND EVALUATIONS DIVISION
WASHINGTON, DC 20511

MEMORANDUM FOR THE RECORD

15 June 2015

PROJECT:	(U) Special Inquiry 2015-001: Assistance to State Department Inspector General Review of Use of Personal Communications Hardware and Software by Five Secretaries of State and Their Immediate Staffs
INSPECTOR:	(U) [redacted]
PURPOSE:	(U//~~FOUO~~) Document Potential Issues Identified in Preliminary Review of the State Department FOIA Process.

(U//~~FOUO~~) The Office of the Inspector General of the Intelligence Community (IC IG) is assisting the State Department IG's office in the above referenced review; focused on the handling of potentially classified material during the State Department Freedom of Information Act (FOIA) review process. I am conducting a preliminary review of the handling of potentially classified material during the State FOIA review process being used to review the 33,000 emails provided by former Secretary Clinton from her personal email server. Thus far, I have identified four areas that may require expedited attention by State FOIA officials, in coordination with IC FOIA officials. Those areas are:

1. (U//~~FOUO~~) **Evaluation of other agencies' equities is not optimal.** State Department is currently relying on retired senior Foreign Service Officers to review for other agencies' equities in FOIA cases. For example, a review of the first set of 296 emails received from former-Secretary Clinton and released on the State Department FOIA website identified material that should have been referred to IC FOIA officials for review prior to release. **Recommend State Department FOIA Office request staff support from IC FOIA offices to assist in the identification of intelligence community equities.**

THIS IS A DELIBERATIVE PROCESS DOCUMENT AND INTENDED SOLELY FOR OFFICIAL USE BY THE IC IG. RECIPIENTS MAY NOT FURTHER DISSEMINATE WITHOUT THE EXPRESS PERMISSION OF IC IG PERSONNEL.

(U//~~FOUO~~) Document Potential Issues Identified in Preliminary Review of the State Department FOIA Process.

2. (U//~~FOUO~~) **Storage and distribution of FOIA material is occurring on a SECRET level network.** State Department is using a SECRET level network (ClassNet) to store the 33,000 emails acquired from former-Secretary Clinton. State is also using ClassNet to distribute the FOIA material for review by both the intra-and-inter-agency. Material at the SECRET//NOFORN level was identified in the first set of 296 emails prior to their release. **Recommend IC FOIA officers review the emails to ensure ClassNet use is appropriate before transmitting to the State Bureaus for review.**

3. (U//~~FOUO~~) **Applying appropriate FOIA exemptions to protect classified information.** State Department FOIA personnel recommended five "B1" (Classified National Security Information) FOIA exemptions for proposed redactions in the first set of 296 emails to protect classified information. According to State FOIA personnel, during the State Department Legal Office's review, four of the B1 exemptions were removed and changed to "B5" FOIA exemptions (Privileged Communications). **Recommend State Department FOIA Office seek classification expertise from the interagency to act as a final arbiter if there is a question regarding potentially classified materials.**

4. (U//~~FOUO~~) **It is unclear if the Department of Justice is reviewing the emails before FOIA release.** Former-Secretary Clinton's emails are the subject of numerous FOIA requests and multiple FOIA lawsuits. It may be prudent to integrate the Department of Justice into the FOIA process review to ensure the redactions can withstand potential legal challenges. **If not already being done, recommend the State Department FOIA Office incorporate the Department of Justice into the FOIA process to ensure the legal sufficiency review of the FOIA exemptions and redactions.**

THIS IS A DELIBERATIVE PROCESS DOCUMENT AND INTENDED SOLELY FOR OFFICIAL USE BY THE IC IG. RECIPIENTS MAY NOT FURTHER DISSEMINATE WITHOUT THE EXPRESS PERMISSION OF IC IG PERSONNEL.

UNDER SECRETARY OF STATE

FOR MANAGEMENT

WASHINGTON

UNCLASSIFIED

JUN 25 2015

MEMORANDUM FOR THE INSPECTOR GENERAL

FROM: M – Patrick F. Kennedy PFK

SUBJECT: Potential Issues Identified by the Office of the Inspector General of the Intelligence Community Concerning the Department of State's Process for the Review of Former Secretary Clinton's Emails under the Freedom of Information Act (ESP-15-04)

I am in receipt of the subject Memorandum (dated June 19, 2015) and its accompanying Memorandum and Attachment from the Inspector General of the Intelligence Community (ICIG). Responses to the four recommendations are contained in the attached.

The Department of State's FOIA processes are consistent with of those of other agencies. State's FOIA personnel analyze responsive records for disclosure pursuant to the provisions of the FOIA and apply exemptions to the documents as appropriate. Department FOIA reviewers are trained in applying the exemptions, using guidance made available by the Department of Justice's Office of Information Policy. The reviewers consult with subject matter experts in Department components and with FOIA attorneys in the Department's Office of the Legal Adviser, as appropriate. In turn, the Department's attorneys consult regularly with attorneys at DOJ's Federal Programs Branch and attorneys at U.S. Attorney's Offices on legal issues that arise in the context of the FOIA and FOIA litigation. Consistent with the long-standing practice of third-agency review within the Executive branch and DOJ Policy on Referrals, Consultations, and Coordination, the Department consults with other agencies with respect to the review and disclosure of records that contain information that is of interest to another agency.

Taking the above in account, the Department finds the issues raised by the ICIG are either already addressed in current processes or are inconsistent with interagency practices. Further, the recommendations provided by the ICIG would add to the FOIA review process schedule and make it more difficult to meet the U.S. District Court order for rolling productions without meaningfully enhancing the review process.

Attachment:

As stated.

Recommendation #1

The process utilized by the State Department to identify other agency equities is one with parallels throughout the United States Government.

Prior to undertaking the current effort, a senior level meeting was held with representatives of a number of agencies (including the CIA and ODNI); the process to be utilized was outlined; and no objection was entered.

The retired senior Foreign Service Officers are utilized because of their years of both FOIA experience and substantive expertise in the various regional and functional issues that are reviewed.

If there are specific examples from the "Benghazi" 296 set that are of concern, the Department would welcome further information.

Recommendation #2

The State Department Classified network is authorized to handle up to SECRET material, including NOFORN, and thus ClassNet is the appropriate system for the storage and distribution of these FOIA materials.

Should the Department identify an e-mail that potentially contains material that could be classified at a higher level, that material would be pulled from the database and transmitted for review via an appropriate channel.

Recommendation #3

Final determinations of classification decisions are made by senior personnel within the Department's FOIA office, assisted by subject matter experts in relevant bureaus and in the Office of the Legal Adviser, after referral of other agency equities have been made to the appropriate agencies and their comments received. These individuals have the experience and expertise necessary to carry out this responsibility correctly.

Recommendation #4

Emails with Department of Justice equities (including those of its component entities) are forwarded to the relevant DOJ entities for review. Legal sufficiency review of the FOIA exemptions and redactions are conducted by attorneys from the Office of the Legal Adviser; they consult regularly with the Department of Justice's Federal Programs Branch regarding FOIA issues and litigation, including litigation involving the former Secretary's emails. This type of process is common throughout the interagency.

United States Department of State
Under Secretary of State
for Management
Washington, D.C. 20520

UNCLASSIFIED

July 14, 2015

MEMORANDUM FOR THE INSPECTOR GENERAL

FROM: Patrick F. Kennedy PFK

SUBJECT: Potential Issues Identified by the Office of the Inspector General of the Intelligence Community Concerning the Department of State's Process for the Review of Former Secretary Clinton's Emails under the Freedom of Information Act (ESP-15-04)

The following information is provided in response to your request for supplemental information. First, the Bureau of Administration's Global Information Services (A/GIS) has been in contact with the Director of ODNI's Information Management Division and is making arrangements for the Intelligence Community (IC) to provide reviewers to assist the Department of State in identifying potential IC equities in its review of former Secretary Clinton's emails. A/GIS is expecting to host more than 10 IC reviewers and will be holding an orientation for the reviewers on July 15.

Second, as we explained, CLASSNET is a secure, classified intranet system. It may be used to process information up to and including SECRET. Should any of the documents in the FOIA review be upgraded to a higher classification than SECRET, they would be moved off CLASSNET. Resource constraints preclude conducting the entire FOIA review on a TOP SECRET system.

Regarding the third recommendation, four of the documents were identified for review by the Bureau of Near Eastern Affairs (NEA), which is the bureau with relevant subject matter expertise; two of the documents were substantively duplicates of each other. NEA consulted with the Office of the Legal Adviser regarding FOIA exemptions that were potentially available, including exemptions 1 (§ 1.4(d) of E.O. 13526) & 5. NEA decided, consistent with the Attorney General's 2009 FOIA guidance, to redact certain limited information under exemption 5 which reflected deliberations among policy officials. Two other documents were proposed for possible upgrade which involved equities of other agencies. In one document, the Department of Defense decided not to seek a

classification upgrade. The other document, which contained an FBI equity, could have been redacted under either exemption 1, pursuant to § 1.4 (d) of E.O. 13526, or exemption 7, as law enforcement information.

Fourth, as noted previously, Department attorneys consult regularly with the Department of Justice's Federal Programs Branch on legal issues that arise in the context of the FOIA and FOIA litigation. This practice is longstanding and continues with respect to this review; L attorneys met with attorneys from Federal Programs on Monday of this week.

ATTACHMENT C

OIG and ICIG Response to the Department

Recommendation 1: The State Department FOIA Office should request staff support from IC FOIA offices to assist in the identification of intelligence community equities.

Management Response: The Department's July 14, 2015, response (July 14 response) states that the Bureau of Administration's Global Information Services (A/GIS) has been in contact with the Director of ODNI's Information Management Division and is making arrangements for the Intelligence Community (IC) to provide reviewers to assist the Department of State in identifying potential IC equities in its review of former Secretary Clinton's emails. A/GIS is expecting to host more than 10 IC reviewers and will be holding an orientation for the reviewers on July 15.

OIG and ICIG Reply: OIG and ICIG consider this recommendation to be closed. A/GIS has made arrangements for the IC reviewers and these additional reviewers will assist the Department of State in identifying potential IC equities in its review of former Secretary Clinton's emails. The additional IC reviewers will assist in identifying and safeguarding IC information. OIG and ICIG will continue to assess the State FOIA review process and the implementation of this recommendation.

Recommendation 2: IC FOIA officers should review the emails to ensure ClassNet use is appropriate before transmitting to the State Bureaus for review.

Management Response: The Department's June 25, 2015, response (June 25 response) states that the State Department Classified network is authorized to handle up to SECRET material, including NOFORN, and thus ClassNet is the appropriate system for the storage and distribution of these FOIA materials. The July 14 response further states that resource constraints preclude conducting the entire review on a TOP SECRET system.

OIG and ICIG Reply: OIG and ICIG consider this recommendation to be unresolved. The ICIG understands the resource constraints presented by conducting the entire FOIA review on a TOP SECRET system. However, given that it is more likely than not that information classified higher than SECRET is present in this collection, it is prudent to seek an alternative to the ClassNet system.

Recommendation 3: The State Department FOIA Office should seek classification expertise from the interagency to act as a final arbiter if there is a question regarding potentially classified materials.

Management Response: The June 25 response states that final determinations of classification decisions are made by senior personnel within the Department's FOIA office, assisted by subject matter experts in relevant bureaus and in the Office of the Legal Adviser, after referral of other agency equities have been made to the appropriate agencies and their comments received.

The July 14 response refers specifically to four emails that were identified for additional consultations regarding a proposed "B1" (Classified Information) FOIA exemption being changed to a "B5" (Privileged Communications) FOIA exemption during the State Department Legal Office's review. The July 14 response states the following:

> Four of the emails were identified for review by the Bureau of Near Eastern Affairs (NEA), which is the Bureau with relevant subject matter expertise; two of the documents were substantively duplicates of each other. NEA consulted with the Office of the Legal Adviser regarding FOIA exemptions that were potentially available, including B1 (§ 1.4 (d) of E.O. 13526) and B5. NEA decided, consistent with the Attorney General's 2009 FOIA guidance, to redact certain limited information under exemption B5 which reflected deliberations among policy officials. Two other documents were proposed for possible upgrade which involved equites of other agencies. In one document, the Department of Defense decided not to seek a classification upgrade. The other document, which contained an FBI equity, could have been redacted under exemption 1, pursuant to § 1.4 (d) of E.O. 13526, or exemption 7, as law enforcement information.

OIG and ICIG Reply: OIG and ICIG consider this recommendation to be unresolved. OIG and ICIG are assessing the information provided in the July 14 response and will further advise the Department after the assessment is completed. Consulting with State Department experts may be sufficient to protect classified State Department equities. However, the information may also be classified due to intelligence equities. OIG and ICIG reiterate the need to seek classification expertise from the interagency to act as a final arbiter if there is a question regarding potentially classified materials.

Recommendation 4: If not already being done, the State Department FOIA Office should incorporate the Department of Justice into the FOIA process to ensure the legal sufficiency review of the FOIA exemptions and redactions.

Management Response: The June 25 response stated that emails with the Department of Justice (DOJ) equities (including those of its component equities) are forwarded to the relevant DOJ entities for review. Legal sufficiency review of the FOIA exemptions and redactions are conducted by attorneys from the Office of the Legal Adviser; they consult regularly with the DOJ's Federal Programs Branch regarding FOIA issues and litigation, including litigation following the former Secretary's emails. This type of process is common throughout the interagency.

OIG and ICIG Reply: OIG and ICIG consider this recommendation to be closed.

UNCLASSIFIED

ATTACHMENT D
OIG and ICIG Memorandum to the Department, Dated June 29, 2015

UNCLASSIFIED

June 29, 2015

MEMORANDUM FOR UNDER SECRETARY KENNEDY

FROM: Steve A. Linick, Inspector General, Department of State
I. Charles McCullough, III, Inspector General, Intelligence Community

SUBJECT: Potential Issues Identified by the Office of the Inspector General of the Intelligence Community Concerning the Department of State's Process for the Review of Former Secretary Clinton's Emails under the Freedom of Information Act (ESP-15-05)

We understand that, in compliance with a federal court order connected to pending Freedom of Information Act (FOIA) litigation, the Department plans to publish tomorrow a portion of the 55,000 pages of emails produced by former Secretary Clinton. We are therefore providing this Memorandum as follow up to our June 19, 2015, Memorandum to you, to provide additional information supporting our concerns about the current process underway to review the 55,000 pages of emails prior to publication.

On June 26 and June 27, 2015, Department staff responsible for FOIA issues further reviewed a portion of the 55,000 pages that have been or are to be reviewed. They report discovering hundreds of potentially classified emails within the collection. In addition, there is concern that possible classified material will be posted in tomorrow's release. Staff members from the Office of Inspector General for the Intelligence Community (IC IG) are now taking steps to verify the classification of some of these emails.

Under the circumstances, we continue to urge the Department to adopt the recommendations made by the IC IG in our June 19 Memorandum in order to enhance the current review system and to further minimize risk. The Department should ensure that no classified documents are publically released.

cc: D-MR - Heather A. Higginbottom

UNCLASSIFIED

INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY
WASHINGTON, DC 20511

14 January 2016

The Honorable Richard Burr
Chairman
Select Committee on Intelligence
U.S. Senate
Washington D.C. 20510

The Honorable Bob Corker
Chairman
Foreign Relations Committee
U.S. Senate
Washington D.C. 20510

SUBJECT: IC IG Response to Congressional Inquiry

Dear Chairman Burr and Chairman Corker:

Thank you for your recent inquiry regarding the classification determination processes used within the Intelligence Community (IC) for reviewing former Secretary of State Clinton's emails. In response to your inquiry, I requested sworn declarations from two IC elements involved in the Freedom of Information Act (FOIA) review process for these emails.

To date, I have received two sworn declarations from one IC element. These declarations cover several dozen emails containing classified information determined by the IC element to be at the CONFIDENTIAL, SECRET, and TOP SECRET/SAP levels. According to the declarant, these documents contain information derived from classified IC element sources. Due to the presence of TOP SECRET/SAP information, I provided these declarations under separate cover to the Intelligence oversight committees and Senate and House Leadership. The IC element is coordinating with State to determine how these documents should be properly treated in the FOIA litigation.

The Honorable Richard Burr
The Honorable Bob Corker

I have yet to receive a declaration from the second classifying IC element, and have referred the matter to the IG of that IC element for follow-up.

You also requested that my office update you on the status of the two open recommendations made in our 15 June 2015 memorandum to State. There is no change since our last reporting. Recommendation 2 that State review the use of a SECRET-level IT system for the FOIA review remains unresolved. The State OIG is still assessing issues related to Recommendation 3 that the State FOIA office seek interagency classification expertise in applying appropriate FOIA exemptions.

If you have any questions or concerns, please contact me or my Legislative Counsel, Melissa H. Wright, at 571-204-8149.

Sincerely,

I. Charles McCullough, III

cc: The Honorable Dianne Feinstein
The Honorable Ben Cardin
The Honorable Devin Nunes
The Honorable Adam Schiff
The Honorable James Clapper, Director of National Intelligence
The Honorable Steve Linick, Inspector General, Department of State

JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5074
MINORITY (202) 225–5051
http://oversight.house.gov

Opening Statement
Ranking Member Elijah E. Cummings

Emergency Hearing with FBI Director James Comey
July 7, 2016

Director Comey, thank you for being here today. I want to begin by commending you and the public servants at the FBI for the independent investigation you conducted.

You had a thankless task. No matter what recommendation you made, you were sure to be criticized. There is no question that you were extremely thorough. In fact, some may even say you went too far in your investigation. But of course, that was your job.

Secretary Clinton has acknowledged that she made a mistake in using a personal email account. And you explained on Tuesday that she and her colleagues at the State Department were extremely careless with their emails.

But after conducting this exhaustive review, you determined that no reasonable prosecutor would bring a case based on this evidence, and you and the career staff recommended against prosecution.

Based on the previous cases you examined, if prosecutors had gone forward, they would have been holding the Secretary to a different standard than everyone else.

Amazingly, some Republicans who were praising you just days ago for your independence and integrity and honesty instantly turned against you because your recommendation conflicted with the predetermined outcome they wanted.

In their eyes, you had one job—and one job only—to prosecute Hillary Clinton. But you refused, so now you are being summoned here to answer for your alleged transgressions.

Contrary to the claims of your critics, there is absolutely no evidence that you made your recommendation for political reasons, no evidence that you were bribed or coerced or influenced, and no evidence that you came to your conclusion based on anything but the facts and the law.

Today, House Republicans are doing what they always do—using taxpayer funds to continue investigating claims that have already been debunked just to keep them in the headlines one more day.

When they hear a political siren, they rush towards it over and over again—even if the evidence is not there.

Exhibit A is Majority Leader Kevin McCarthy, who admitted on national television that Republicans established the Benghazi Select Committee to bring down Secretary Clinton's poll numbers. This fact was confirmed by a Republican staffer on that Committee who reported that he was fired in part for not going along with the "hyper focus" on Secretary Clinton.

I give House Republicans credit—they certainly are not shy about what they are doing. They have turned political investigations into an art form.

If our concerns here today are with the proper treatment of classified information, then we should start with a review of our previous hearing on General David Petraeus, who pled guilty last year to intentionally and knowingly compromising highly classified information.

The problem is, we never had that hearing. This Committee ignored that breach of national security because it did not match the political goals of House Republicans.

If our concerns today were with finally addressing a broken classification system in which security levels are arbitrarily changed up and down, that would have been a legitimate goal. That would have been a valuable addition to reforming and improving our government.

We could have held today's hearing on the Zika virus, preventing gun massacres like the one in Orlando, or a host of other topics that could actually save people's lives.

But that is not why we are here. That is not why our Chairman called this emergency hearing 48 hours after Director Comey made his recommendation. Everyone knows what this Committee is doing, and it's an abuse of taxpayer dollars for political purposes.

Honestly, I would not be surprised—and I say this with all seriousness—I would not be surprised if tomorrow House Republicans set up a new committee to spend another $7 million on why the FBI failed to prosecute Hillary Clinton.

Director Comey, let me conclude with this request. Even with all I have said, I believe there is a critical role for you here today. I have listened carefully to the coverage on this issue, and I have heard people say, as recently as this morning, that they are mystified by your decision. There is a perceived gap between the things you said on Tuesday and your recommendation.

So this is your moment. Fill in that gap. Share with us and the American people your process and your thinking. Explain how you examined the evidence, the law, and the precedent. Describe in clear terms how you and your team of career professionals arrived at this decision. If you can do that today, that could go a long way towards helping people understand your decision.

Finally, I want to make clear that I condemn these completely unwarranted political attacks against you. They have attacked you personally, they have attacked your integrity, they

have impugned your professionalism, and they have even suggested that you were somehow bought and paid for because you made your recommendation based on the facts.

I know you are used to working in the world of politics, but these attacks are beyond the pale. You do not deserve this. Your family does not deserve this. And the highly skilled and dedicated agents at the FBI do not deserve this.

I honor your professionalism and your service to our country, and I thank you for being willing to testify here today on such incredibly short notice.

Contact: Jennifer Werner, Communications Director, (202) 226-5181.

○