

**This is an automatic e-mail message generated by the CM/ECF system. Please DO NOT RESPOND to this e-mail because the mail box is unattended.**

**\*\*\*NOTE TO PUBLIC ACCESS USERS\*\*\*** Judicial Conference of the United States policy permits attorneys of record and parties in a case (including pro se litigants) to receive one free electronic copy of all documents filed electronically, if receipt is required by law or directed by the filer. PACER access fees apply to all other users. To avoid later charges, download a copy of each document during this first viewing. However, if the referenced document is a transcript, the free copy and 30 page limit do not apply.

**U.S. District Court**

**District of Columbia**

### **Notice of Electronic Filing**

The following transaction was entered by Kendall, David on 7/12/2016 at 11:50 AM and filed on 7/12/2016

**Case Name:** JUDICIAL WATCH, INC. v. DEPARTMENT OF STATE

**Case Number:** [1:13-cv-01363-EGS](#)

**Filer:** HILLARY RODHAM CLINTON

**Document Number:** [102](#)

#### **Docket Text:**

**Memorandum in opposition to re [97] MOTION for Order to Depose Hillary Clinton, Clarence Finney, and John Bentel filed by HILLARY RODHAM CLINTON.**

**(Attachments: # (1) Exhibit A, # (2) Exhibit B, # (3) Exhibit C, # (4) Exhibit D, # (5) Exhibit E, # (6) Exhibit F, # (7) Exhibit G, # (8) Exhibit H, # (9) Text of Proposed Order Proposed Order)(Kendall, David)**

**1:13-cv-01363-EGS Notice has been electronically mailed to:**

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

JUDICIAL WATCH, INC.,

Plaintiff,

v.

U.S. DEPARTMENT OF STATE,

Defendant.

No. 1:13-cv-01363-EGS

**NON-PARTY HILLARY RODHAM CLINTON'S  
OPPOSITION TO PLAINTIFF'S MOTION TO DEPOSE  
HILLARY RODHAM CLINTON, CLARENCE FINNEY, AND JOHN BENTEL**

David E. Kendall (D.C. Bar No. 252890)  
Katherine M. Turner (D.C. Bar No. 495528)  
Amy Mason Saharia (D.C. Bar No. 981644)  
WILLIAMS & CONNOLLY LLP  
725 Twelfth Street, N.W.  
Washington, DC 20005  
Telephone: (202) 434-5000  
Facsimile: (202) 434-5029

*Counsel for Non-Party Hillary Rodham  
Clinton*

## TABLE OF CONTENTS

	Page
INTRODUCTION .....	1
BACKGROUND .....	2
A. Secretary Clinton’s Use of Personal E-mail .....	2
B. This Lawsuit.....	4
ARGUMENT .....	5
I. JUDICIAL WATCH HAS NOT DEMONSTRATED A NEED TO DEPOSE SECRETARY CLINTON.....	5
A. Judicial Watch Already Has an Extensive Record About the Creation, Purpose, and Use of clintonemail.com. ....	5
B. The Questions Identified by Judicial Watch Are Either Answered or Irrelevant. ....	7
1. <i>The purpose for the clintonemail.com system</i> .....	7
2. <i>Secretary Clinton’s continued use of the system</i> .....	9
3. <i>Secretary Clinton’s claim over the records on the clintonemail.com system</i> .....	10
4. <i>Secretary Clinton’s inventorying of records upon completion of her tenure as secretary</i> .....	12
5. <i>Secretary Clinton’s choice of type of e-mail system to conduct official government business</i> .....	13
6. <i>Bryan Pagliano’s role in creating and operating the clintonemail.com system</i> .....	13
C. This Court Should Not Permit a Deposition of Secretary Clinton.....	14
II. THE REQUESTED DISCOVERY IS FUTILE. ....	15
III. THIS COURT LACKS JURISDICTION TO ORDER DISCOVERY RELATED TO SECRETARY CLINTON’S USE OF PRIVATE E-MAIL IN THIS CASE.....	16
A. <i>Kissinger Controls This Case</i> .....	17

	Page
B. A General Intent To “Thwart” FOIA Does Not Render <i>Kissinger</i> Inapplicable.....	19
CONCLUSION.....	20

## INTRODUCTION

This case arises from a FOIA request submitted by Plaintiff Judicial Watch, Inc. seeking records related to Ms. Huma Abedin's status as a special government employee. On May 4, 2016, this Court permitted Judicial Watch to take "limited" discovery deemed relevant to the "narrow legal question" of whether the State Department, "in good faith, conduct[ed] a search reasonably calculated to uncover all relevant documents." Docket Entry ("Dkt.") 73 at 1. In particular, the Court authorized discovery related to "the creation, purpose and use of the clintonemail.com server" to determine whether there is evidence substantiating Judicial Watch's allegation that the State Department sought to "thwart" FOIA. *Id.* at 1, 11. As a result of this Court's order, Judicial Watch deposed seven current and former State Department employees.

In addition, Judicial Watch now has available to it a vast public record on this subject. Secretary Clinton testified publicly about her e-mail before the Benghazi Select Committee on October 22, 2015. The testimony on this topic by Secretary Clinton's aides as well as other State Department employees to the Select Committee also has been publicly released. In May 2016, the State Department Inspector General issued a report on e-mail records management in the Office of the Secretary, which included an assessment of practices during Secretary Clinton's tenure. On July 5, 2016, FBI Director James Comey publicly announced the findings of the FBI's year-long investigation of a security referral from the Intelligence Community Inspector General related to Secretary Clinton's e-mail. Director Comey later testified for more than four hours on this subject before the House Oversight and Government Reform Committee on July 7, 2016.

Despite this public testimony and the various investigative reports, Judicial Watch claims that it needs to depose Secretary Clinton, a former Cabinet Secretary, about six purportedly unanswered questions. The record, however, already answers those questions or makes clear that Secretary Clinton has no personal knowledge to provide. And many of Judicial Watch's proposed

topics are irrelevant to the issue for which it sought discovery: “whether the State Department and Mrs. Clinton deliberately thwarted FOIA.” Dkt. 48 at 3; Dkt. 51 at 1. Indeed, Judicial Watch ignores that issue altogether in its Motion. That failure is unsurprising, as the FBI concluded after its year-long investigation that Secretary Clinton did not intend to conceal records from the public.

In any event, the discovery requested by Judicial Watch is futile. The ostensible purpose of the requested discovery is to determine whether this Court should compel Secretary Clinton to produce her @clintonemail.com account (including any personal e-mail) from her private e-mail server equipment to the State Department for further searching in response to Judicial Watch’s FOIA request. Even if this Court had authority to issue such unprecedented relief, Secretary Clinton has nothing to produce, as the server equipment used to host her @clintonemail.com account is in the possession of the FBI.

Finally, for the sake of preserving any and all rights, counsel to Secretary Clinton respectfully submit that discovery is unwarranted in this case as a general matter. Under *Kissinger v. Reporters Committee for Freedom of the Press*, 445 U.S. 136 (1980), this Court lacks jurisdiction to compel disclosure of documents on Secretary Clinton’s private server equipment—irrespective of any alleged intent to “thwart” FOIA—because those documents were outside the State Department’s possession or control when Judicial Watch submitted its FOIA request.

## **BACKGROUND**

### **A. Secretary Clinton’s Use of Personal E-mail**

Secretary Clinton was Secretary of State from January 21, 2009 to February 1, 2013. Before becoming Secretary of State, she served in the Senate. When she arrived at the State Department, she already had been using a personal e-mail account for both Senate-related and personal e-mail. Mills Deposition (“Dep.”) at 45:7–48:5; Abedin Dep. at 38:11–39:8. She continued that practice upon becoming Secretary of State. Mills Dep. at 45:7–48:5; Abedin Dep. at 38:11–39:8.

Secretary Clinton has stated that the reason she used a private e-mail address for work was the convenience of doing so. Mills Dep. at 172:20–173:4; Ex. B at 188 (Testimony of Huma Abedin to the Benghazi Select Committee); *see also* Ex. D at 1. The FBI confirmed as a result of its investigation that Secretary Clinton used private e-mail for the sake of convenience. *See* Ex. C at 20, 74 (Testimony of James Comey to the House Oversight and Government Reform Committee).

Although e-mail was not her primary means of communication, *see* Ex. A at 285, 401 (Testimony of Hillary Rodham Clinton to the Benghazi Select Committee); Mills Dep. at 257:8–258:19; Abedin Dep. at 157:2–158:6, Secretary Clinton did use e-mail for State Department business. During virtually all of her tenure as Secretary of State, Secretary Clinton used a personal e-mail account, `hdr22@clintonemail.com`, for work-related and personal e-mail.<sup>1</sup> Ex. A at 335. During her tenure, that account was hosted on server equipment in the Clinton home in Chappaqua, New York. Mills Dep. at 264:21–265:12; Dkt. 48-6, at 237. The server equipment was set up for the use of former President Clinton’s staff, and Secretary Clinton’s e-mail account was added to it. Ex. A at 403; Mills Dep. at 259:2–13. In 2013, after Secretary Clinton left the State Department, the account was transitioned to equipment managed by Platte River Networks, a private company. Ex. A at 403; Mills Dep. at 103:8–104:2; Dkt. 48-6, at 237.

Secretary Clinton’s practice was to e-mail State Department officials on their `state.gov` e-mail accounts. Ex. A at 408; *see also* Abedin Dep. at 120:19–121:3. She corresponded with numerous State Department officials—including Legal Adviser Harold Koh, Under Secretary for Management Patrick Kennedy (the Department’s senior agency official for records management), and other senior Department officials. *See, e.g.*, Ex. E; Kennedy Dep. at 10:7–12, 61:11–14. In

---

<sup>1</sup> Secretary Clinton briefly used an AT&T account after initially arriving at the State Department. Mills Dep. at 47:17–49:12.

other words, “it wasn’t a secret that she was using this e-mail account to be communicating with U.S. government officials, because they were receiving e-mails from her.” Abedin Dep. at 52:9–12. Secretary Clinton has testified that her understanding was that “all of [her] work-related emails to [government e-mail] accounts were being captured and preserved.” Ex. A at 425.

In the fall of 2014, the State Department requested that Secretary Clinton and other former Secretaries of State provide copies of federal records that may not otherwise have been preserved in the Department’s record-keeping system. Dkt. 18-1. Secretary Clinton’s attorneys oversaw the process of responding to the Department’s request. Ex. A at 401. Secretary Clinton sought to produce all e-mails that “could be possibly construed as work-related.” Ex. A at 402; Dkt. 22-1. As a result of her attorneys’ review, in December 2014 counsel to Secretary Clinton provided the State Department with approximately 55,000 pages of e-mails. *See* Dkt. 22-1; Dkt. 26-1, ¶ 13.

## **B. This Lawsuit**

Judicial Watch submitted the FOIA request at issue in this case on May 21, 2013, nearly four months after Secretary Clinton’s tenure as Secretary of State ended. *See* Dkt. 1. After State produced responsive documents, Judicial Watch dismissed the case with prejudice in March 2014. Dkt. 12. In March 2015, the parties agreed to reopen the case. Dkt. 14. The State Department then searched the e-mails that Secretary Clinton had provided to the Department in December 2014 using agreed-upon search terms. Dkt. 47-2, ¶ 43. No responsive e-mails were located. *Id.* ¶ 45.

After the Department moved for summary judgment, Judicial Watch moved for discovery under Rule 56(d). This Court granted that motion, concluding that “questions surrounding the creation, purpose and use of the clintonemail.com server must be explored before this Court can decide, as a matter of law, whether the Government has conducted an adequate search in response to Judicial Watch’s FOIA request.” Dkt. 73 at 1. Judicial Watch does not appear to contest the



adequacy of the Department's search of the 55,000 pages of e-mails that Secretary Clinton provided to it. Instead, Judicial Watch contends that FOIA requires the Department to attempt to acquire and search Secretary Clinton's @clintonemail.com account, including any personal e-mail, that once resided on her private e-mail server equipment. *See* Feb. 23, 2016 Hr'g Tr. at 45:6–22, 47:1–6.

## **ARGUMENT**

Judicial Watch has not demonstrated a need to depose Secretary Clinton, a former Cabinet Secretary. Although Judicial Watch identifies six questions it would like to ask Secretary Clinton, the voluminous record available to Judicial Watch—which includes Secretary Clinton's sworn testimony—answers many of those questions. The remainder are irrelevant to the narrow issue on which limited discovery was permitted. The requested deposition, moreover, would be an exercise in futility. No matter how much discovery Judicial Watch takes, the ultimate relief it seeks—production and search of Secretary Clinton's clintonemail.com account by either the State Department or Secretary Clinton—is impossible to obtain in this case, as Secretary Clinton does not have possession or control of the equipment that housed that account. Finally, this Court lacks jurisdiction to order the requested discovery. Because the State Department did not possess or control the e-mail account when Judicial Watch submitted the at-issue request (or at any time subsequent to the request), it could not withhold e-mails from that account even if, as Judicial Watch incorrectly claims, there was an intent to “thwart” FOIA generally.

### **I. JUDICIAL WATCH HAS NOT DEMONSTRATED A NEED TO DEPOSE SECRETARY CLINTON.**

#### **A. Judicial Watch Already Has an Extensive Record About the Creation, Purpose, and Use of clintonemail.com.**

Discovery in FOIA cases is “rare.” *Schrecker v. U.S. DOJ*, 217 F. Supp. 2d 29, 36–37 (D.D.C. 2002), *aff'd*, 349 F.3d 657 (D.C. Cir. 2003); *see Thomas v. Dep't of Health & Human*

*Servs.*, 587 F. Supp. 2d 114, 115 n.2 (D.D.C. 2008); *Judicial Watch, Inc. v. Exp.-Imp. Bank*, 108 F. Supp. 2d 19, 25 (D.D.C. 2000). This Court already has taken the unusual step of permitting Judicial Watch to take limited discovery related to the creation, purpose, and use of clintonemail.com. The Benghazi Select Committee, the State Department Inspector General, and the FBI also have conducted inquiries and made findings on this subject. The findings of those inquiries have been made public, which had not occurred when this Court first permitted discovery. *See* Feb. 23, 2016 Hr'g Tr. at 57:5–17. Judicial Watch now has a voluminous record related to Secretary Clinton's use of private e-mail. That record includes:

- Secretary Clinton's public testimony during an eleven-hour hearing before the Benghazi Select Committee on October 22, 2015, *see* Ex. A;
- The testimony of current and former State Department witnesses before the Benghazi Select Committee, including Under Secretary for Management Patrick Kennedy, the former director of Information Resource Management for the Executive Secretariat, and Secretary Clinton's senior aides Cheryl Mills, Huma Abedin, and Jacob Sullivan<sup>2</sup>;
- Depositions of six fact witnesses in this case, including Ms. Mills and Ms. Abedin;
- A deposition of the State Department's Rule 30(b)(6) witness in this case;
- Verified interrogatory responses from the State Department in this case, *see* Dkt. 97-1;
- A January 2016 report by the State Department Inspector General regarding FOIA processes for requests involving the Office of the Secretary, *see* Ex. F;
- A May 2016 report by the State Department Inspector General regarding e-mail records management in the Office of the Secretary, which covers the period of Secretary Clinton's tenure, *see* Ex. G;
- The State Department's production to Judicial Watch of documents cited in the May 2016 State Department Inspector General report, *see* Dkt. 97-2;
- The June 28, 2016 Report of the Select Committee on the Events Surrounding the 2012 Terrorist Attack in Benghazi;

---

<sup>2</sup> [Http://democrats-benghazi.house.gov/work/interview-transcripts](http://democrats-benghazi.house.gov/work/interview-transcripts).

- FBI Director Comey’s July 5, 2016 public remarks regarding the findings of the FBI investigation, which included a voluntary interview of Secretary Clinton<sup>3</sup>;
- FBI Director Comey’s testimony to the House Oversight and Government Reform Committee on July 7, 2016, *see* Ex. C; and
- 30,322 e-mails and corresponding e-mail attachments provided by counsel to Secretary Clinton to the State Department available to the public on the Department’s website.

**B. The Questions Identified by Judicial Watch Are Either Answered or Irrelevant.**

“Discovery in a FOIA case . . . is not a punishment for a deficient agency performance.” *Asarco, Inc. v. U.S. EPA*, No. 08-1332 (EGS/JMF), 2009 WL 1138830, at \*2 (D.D.C. Apr. 28, 2009). A FOIA requester is entitled to discovery only “when there has emerged a genuine issue of material fact which can only be resolved by an evidentiary hearing.” *Id.* at \*1. The ostensible reason for requesting discovery here is to resolve a dispute of fact regarding whether the State Department deliberately “thwarted” FOIA through Secretary Clinton’s use of clintonemail.com. *See* Dkt. 48 at 3; *see also infra* Part III. Judicial Watch ignores this fundamental question in its motion. Instead, it simply lists a series of topics related to Secretary Clinton’s e-mail—completely divorced from the ultimate question of fact—for which it claims to want testimony from Secretary Clinton. This Court granted discovery, however, to resolve “a narrow legal question.” Dkt. 73 at 1. Many of Judicial Watch’s topics bear no rational connection to that narrow question. And the voluminous record available to Judicial Watch already provides answers to those that do.

***1. The purpose for the clintonemail.com system***

Secretary Clinton has repeatedly stated that the purpose of using the clintonemail.com system was convenience, as a continuation of her Senate practice. *See* Mills Dep. at 172:20–173:4;

---

<sup>3</sup> <https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b.-comey-on-the-investigation-of-secretary-hillary-clintons-use-of-a-personal-e-mail-system>.

Ex. B at 188; *see also* Ex. D at 1. FBI Director Comey testified before Congress that Secretary Clinton told the FBI in her interview that she used the clintonemail.com system for the sake of convenience. *See* Ex. C at 74. According to Director Comey, “Our best information is that she set it up as a matter of convenience. It was an existing system her husband had and she decided to have a domain on that system.” Ex. C at 20.

Moreover, there is no evidence that the purpose of the clintonemail.com system was to thwart FOIA, as Judicial Watch claims. Secretary Clinton herself has testified that her practice was to e-mail State officials on their government accounts, and she thought that those e-mails were being captured and preserved in the Department’s record-keeping systems.<sup>4</sup> *See* Ex. A at 408, 425. Ms. Mills shared that belief. *See* Mills Dep. at 183:9–184:4, 218:3–7, 238:16–239:21, 261:4–10. Even if that understanding was mistaken, it does not amount to an intent to evade FOIA. Notably, Secretary Clinton’s use of a private e-mail account was transparent to State Department officials, including those responsible for records management. *See supra* pp.3–4. The fact that she corresponded with the Department’s Legal Adviser and Under Secretary for Management belies any notion that the e-mail system was intended to thwart FOIA.

Although Secretary Clinton corresponded widely with senior officials at the Department, there is no evidence that anyone expressed concern to Secretary Clinton or her aides about the record-keeping implications of her use of personal e-mail. Neither Ms. Abedin nor Ms. Mills recalled anyone raising such concerns with them or the Secretary, or participating in conversations on that topic. Mills Dep. at 183:9–16, 190:15–21; Abedin Dep. at 114:4–9, 117:18–118:3, 135:18–

---

<sup>4</sup> That belief, even if mistaken, was not unreasonable. As the State Department Inspector General reported, when Secretary Colin Powell’s representative asked Department staff “whether they needed to do anything to preserve the Secretary’s emails [on a private e-mail address] prior to his departure,” the staff “responded that the Secretary’s emails would be captured on Department servers because the Secretary had emailed other Department employees.” Ex. G at 21.

138:22; Ex. B at 123, 161. Ambassador Stephen Mull, who was ultimately responsible for FOIA activities in the Executive Secretariat during much of Secretary Clinton’s tenure, testified that he did not hear of any concerns about Secretary Clinton’s e-mail not being subject to FOIA. Mull Dep. at 28:6–15, 80:1–11; *see also* Mull Dep. at 86:7–16; Kennedy Dep. at 58:1–4.

Given these facts, it is not surprising that Secretary Clinton’s closest aides, Ms. Mills and Ms. Abedin, testified that they have “[a]bsolutely” no “reason to believe that Secretary Clinton used Clintonemail.com to conduct government business because she or anyone else at the State Department was seeking to avoid FOIA.” Mills Dep. at 263:7–11; Abedin Dep. at 164:22–165:6, 195:15–19, 220:22–221:3. And, after a year-long investigation, the FBI did *not* find that Secretary Clinton used a private server “because she wanted to shield communications from Congress and the public.” Ex. C at 20. Rejecting that proposition, Director Comey testified, “Our best information is that she set it up as a matter of convenience.” Ex. C at 20. Judicial Watch has provided no basis to conclude that a deposition of Secretary Clinton in this case would produce information different than what she and others have already provided, and discovery in a FOIA case is not available to “afford[] [the plaintiff] an opportunity to pursue a bare hope of falling upon something” that might support its claim. *Military Audit Project v. Casey*, 656 F.2d 724, 751–52 (D.C. Cir. 1981) (quotation marks omitted).

## 2. *Secretary Clinton’s continued use of the system*

Judicial Watch also claims that it needs to know why Secretary Clinton continued using the clintonemail.com system despite supposed problems and disruptions. Its underlying assumption—that the clintonemail.com system had more problems than the state.gov system—is not supported by the record. Ms. Abedin has testified that there were just as many technical issues with the state.gov system as with the clintonemail.com system. *See* Ex. B at 175; *see also* Abedin Dep. at 84:10–22 (“[I]t was both Clinton e-mail and State.gov having the communications challenges.”).

Ms. Abedin also testified that Secretary Clinton did not switch to a state.gov e-mail account because the technical issues with clintonemail.com were resolved. Abedin Dep. at 193:21–194:6.

Judicial Watch points to a series of e-mails related to technical difficulties. Secretary Clinton, however, was not a party to most of those e-mails, and Judicial Watch has deposed many of the persons who were. Although Judicial Watch highlights an e-mail to Ms. Abedin mentioning that a State-issued Blackberry would be subject to FOIA, *see* Mot. at 7, Ms. Abedin testified that she did not “remember discussing this with the Secretary.”<sup>5</sup> Abedin Dep. at 167:10–170:8. Judicial Watch has no need to depose Secretary Clinton about other people’s e-mails.

Judicial Watch identifies only one communication involving Secretary Clinton, but that document disproves any intent to thwart FOIA. When Ms. Abedin suggested that Secretary Clinton obtain a state.gov e-mail address in 2010, the Secretary did not express concern that her work-related e-mails would be subject to FOIA. *See* Dkt. 97-2, Doc. B. She stated only that she did not want her “personal” e-mails to be accessible. *Id.*; *see* Abedin Dep. at 188:17–193:9. Judicial Watch’s suggestion that it needs to depose Secretary Clinton to find out what she meant is not credible. Judicial Watch has already deposed Ms. Abedin about this exchange, *see* Abedin Dep. at 180:19–194:6, and the meaning of Secretary Clinton’s statement is obvious on its face.

### 3. *Secretary Clinton’s claim over the records on the clintonemail.com system*

Citing *Competitive Enterprise Institute v. Office of Science and Technology Policy*, No. 15-5128, --- F.3d ---, 2016 WL 3606551 (D.C. Cir. July 5, 2016), Judicial Watch argues that it needs to determine whether Secretary Clinton “claimed any personal right or exclusive control

---

<sup>5</sup> Moreover, Ms. Abedin explained that, when she stated that the proposed State Blackberry arrangement did not make sense, she was referring not to FOIA but to the fact that State was proposing to add “not just one but two additional devices.” Abedin Dep. at 176:6–177:17.

over the emails on the clintonemail.com system.” Mot. at 8. *Competitive Enterprise Institute*, however, involves a FOIA request for the records of a current agency head. See 2016 WL 3606551, at \*1. This case involves a request for the e-mails of a *former* agency head. *Competitive Enterprise Institute* thus does not govern this case. See *id.* at \*5 (Srinivasan, J., concurring) (explaining that the case does not “involve[] records held by someone having no present affiliation with the agency at the time of the FOIA request”). Moreover, even if it did, the Court of Appeals expressly pointed out that it was not deciding what relief was appropriate. See *id.* at \*4 (“We make clear that we are not ordering the specific disclosure of any document.”). It did not order that the agency head was required to give her agency unfettered access to all of her personal e-mails (as opposed to reviewing her e-mails herself), as Judicial Watch requests here.

Even if relevant, *Competitive Enterprise Institute* would not warrant discovery. The relief Judicial Watch seeks is an order requiring the State Department to obtain Secretary Clinton’s *entire* e-mail account to search for any additional e-mails. That e-mail account, which was hosted on private server equipment, was possessed privately under a claim of right, and has never been the property of or in the possession or control of the State Department.

Judicial Watch further claims that it needs to know whether Secretary Clinton deleted work-related e-mails during her tenure as Secretary—*i.e.*, before Judicial Watch submitted its FOIA request. That question is irrelevant to this FOIA case. FOIA does not obligate agencies to retain records; the obligation to retain records arises from the Federal Records Act, which does not confer a private right of action. See *Kissinger v. Reporters Committee for Freedom of the Press*, 445 U.S. 136, 152 (1980); see also *infra* Part III. Finally, Judicial Watch claims that it needs to know Secretary Clinton’s understanding of her FOIA obligations, but Secretary Clinton has already testified to that very issue. See *supra* pp.3-4.

**4. Secretary Clinton's inventorying of records upon completion of her tenure as secretary**

Judicial Watch further argues that it needs information about Secretary Clinton's "inventorying of records" at the end of her tenure. Mot. at 9. It highlights a "meeting between [Clarence] Finney, Ms. Abedin and other personnel from the Office of the Secretary about what records Secretary Clinton and her staff were allowed to take with them when they left the State Department." Mot. at 9. But Secretary Clinton was not at that meeting. *See* Abedin Dep. at 141:5–7. Moreover, Secretary Clinton was not the person inventorying her records. Her staff was performing that task. *See* Abedin Dep. at 141:8–143:10. Ms. Abedin has already explained why "record management officials apparently were not advised about official, government records on the clintonemail.com system when the secretary transitioned out of the department." Mot. at 10. She testified:

Q Do you know why nobody informed Mr. Finney about the State-related e-mails on Secretary Clinton's Clintonemail.com account? . . .

A I – as I think I've mentioned earlier, it is not anything that occurred to us. We all wish we could go back and that not be the case. It did not occur to those of us who were involved.

Q And is that the same answer? I'm specifically asking for the time period during the transition process prior to leaving the State Department.

A Yes, ma'am. I understand. It did not – it did not occur to us.

Abedin Dep. at 145:1–16; *see also* Abedin Dep. at 219:5–14; Ex. B at 138, 188. Similarly, Ms.

Mills testified:

Q So you never thought about how were the federal records that were stored on her e-mail account, how would the State Department have access to that after she left? . . .

A I assumed, I now know inaccurately, that records that were on a State system were ones that were kept forever. Obviously I've come to learn that that's not the case. And I thought since the Secretary's practice was to e-mail people on their State [accounts], that there was resident in the department a set of records with respect to her work at the department. And I thought they would have been there.



Q But what about – but what about the federal records that were the e-mails between the Secretary and other people outside of the State Department; what about those e-mails?

A I wish I had thought about that subset. . . . I didn't think about that.

Mills Dep. at 239:7–240:17.

**5. *Secretary Clinton's choice of type of e-mail system to conduct official government business***

Judicial Watch next argues that it needs to know why Secretary Clinton switched from a supposedly “archived” commercial AT&T e-mail account to the “non-archived” clintonemail.com account early in her tenure as Secretary of State. Mot. at 11. This argument is both factually unfounded and wholly irrelevant. Secretary Clinton produced to the State Department 55,000 pages of e-mails from her clintonemail.com account. As Judicial Watch knows, she was unable to retrieve or produce e-mails from the supposedly “archived” AT&T account that she used early in her tenure. See Dkt. 43; Ex. H (Letter from David Kendall to Patrick Kennedy (Oct. 8, 2015)).

**6. *Bryan Pagliano's role in creating and operating the clintonemail.com system***

Finally, Judicial Watch claims that it needs to know how Bryan Pagliano received a job at the State Department and what work he performed on the clintonemail.com system. Mot. at 12. It makes no attempt to explain how this information is in any way relevant to the question of intent to thwart FOIA. Even if this topic were relevant, Judicial Watch fails to establish that Secretary Clinton has any relevant knowledge. Ms. Mills testified that to her knowledge Secretary Clinton did *not* request that Mr. Pagliano receive a job at the Department. See Mills Dep. at 154:20–22. Moreover, Judicial Watch has identified documents related to Mr. Pagliano's hiring at the Department, see Mills Ex. 8, and none of them suggests that Secretary Clinton had any involvement. There is no basis to conclude that she has any information on these (irrelevant) questions.

**C. This Court Should Not Permit a Deposition of Secretary Clinton.**

On this record, Judicial Watch's request for more discovery under Rule 56(d) is an improper "fishing expedition[]." *Doe v. U.S. DOJ*, 660 F. Supp. 2d 31, 54 (D.D.C. 2009) (quotation marks omitted); *see also Exxon Corp. v. FTC*, 663 F.2d 120, 128 (D.C. Cir. 1980) ("It is not the intent of Rule 56 to preserve purely speculative issues of fact . . ."). Judicial Watch has answers to the questions that are relevant to the disputed issue of fact in this case. The fact that Judicial Watch does not like those answers does not warrant more discovery.

This Court should be especially wary of Judicial Watch's claim that it needs to depose Secretary Clinton, a former Cabinet Secretary. As a general matter, "subjecting a cabinet officer to oral deposition is not normally countenanced." *Peoples v. U.S. Dep't of Agriculture*, 427 F.2d 561, 567 (D.C. Cir. 1970); *see also Simplex Time Recorder Co. v. Sec'y of Labor*, 766 F.2d 575, 586 (D.C. Cir. 1985); *In re Papandreou*, 139 F.3d 247, 253 (D.C. Cir. 1998). For that reason, the Court of Appeals requires a litigant to show "extraordinary circumstances" before permitting a deposition of a high-ranking government official. *See In re United States*, No. 14-5146, 2014 U.S. App. LEXIS 14134, at \*2 (D.C. Cir. July 24, 2014) (per curiam) (granting a writ of mandamus to quash the deposition of the Secretary of Agriculture absent a showing of "extraordinary circumstances"); *see also, e.g., Lederman v. N.Y.C. Dep't of Parks & Recreation*, 731 F.3d 199, 203 (2d Cir. 2013); *In re United States*, 624 F.3d 1368, 1374 (11th Cir. 2010). This Court has extended this requirement to requests to depose former high-ranking government officials. *See, e.g., FDIC v. Galan-Alvarez*, No. 1:15-mc-00752(CRC), 2015 WL 5602342, at \*4 (D.D.C. Sept. 4, 2015); *Willingham v. Ashcroft*, 226 F.R.D. 57, 65 (D.D.C. 2005); *see also In re United States*, 542 F. App'x 944, 949 (Fed. Cir. 2013) (suggesting that the requirement would apply in the case of former high-ranking officials).

Litigants are not typically permitted to depose high-ranking government officials if the requested information can be obtained elsewhere, including from lower-ranking government officials. *See, e.g., In re Cheney*, 544 F.3d 311, 314 (D.C. Cir. 2008) (per curiam); *In re United States*, 197 F.3d 310, 314 (8th Cir. 1999). For all the reasons already set forth, Judicial Watch has obtained the requested information from other current and former government officials, as well as from Secretary Clinton's prior testimony to the Benghazi Select Committee. A deposition of Secretary Clinton in this case would be entirely cumulative and unnecessary.<sup>6</sup>

## II. THE REQUESTED DISCOVERY IS FUTILE.

The requested deposition is inappropriate for an independent reason. FOIA authorizes courts to grant only limited relief: a court can "enjoin the agency from withholding agency records and . . . order the production of any agency records improperly withheld from the complainant." 5 U.S.C. § 552(a)(4)(B). Judicial Watch sought discovery to determine whether the Department should be required to search Secretary Clinton's e-mail account to identify and produce work-related e-mails, if any, responsive to Judicial Watch's request. *See* Dkt. 48, at 3–5; Feb. 23, 2016 Hr'g Tr. at 47:1–6. Even if this Court had authority to order Secretary Clinton to produce her clintonemail.com e-mails or her private e-mail server equipment to the Department (it does not),<sup>7</sup>

---

<sup>6</sup> At a minimum, if the Court decides, notwithstanding the arguments herein, that further discovery is necessary, counsel to Secretary Clinton respectfully urge this Court to allow Secretary Clinton to provide information in writing. Secretary Clinton has already testified or spoken about some of the topics for which Judicial Watch claims to need discovery and has virtually no knowledge of others. Requiring her to sit for a deposition for the purpose of repeating her prior statements or stating that she has no knowledge of certain topics would serve no useful purpose.

<sup>7</sup> Although a court may have authority under FOIA to compel nonparties to return documents responsive to a FOIA request where an agency transferred those documents to evade a preexisting FOIA request, *see Judicial Watch, Inc. v. U.S. Dep't of Commerce*, 34 F. Supp. 2d 28, 44 (D.D.C. 1998), Judicial Watch has identified no authority for the altogether different proposition that FOIA authorizes courts to compel nonparties to produce to an agency entire personal e-mail accounts that may or may not contain responsive documents. As the Department has explained, the obligation to determine whether an e-mail is a federal record requiring preservation remains with the

that relief is impossible as a practical matter. In connection with the FBI investigation, Secretary Clinton voluntarily provided to the FBI the server equipment that housed her clintonemail.com account for the proper purpose of facilitating the FBI's security-related investigation. *See* Dkt. 24-1, at Ex. E. She does not have access to her clintonemail.com account. Even if this Court were to issue a subpoena to Secretary Clinton, she has nothing in her possession or custody to produce. Judicial Watch itself has acknowledged that its request for discovery could be "a moot point" in precisely this circumstance. Feb. 23, 2016 Hr'g Tr. at 11:5–16.

Judicial Watch has represented that it has filed a FOIA request with the FBI. *See* Oct. 6, 2015 Hr'g Tr. at 39:2–7. That request is the only avenue by which Judicial Watch can request the documents it seeks. *See DiBacco v. U.S. Army*, 795 F.3d 178, 192 (D.C. Cir. 2015) (holding that where documents are transferred to another agency after receipt of a FOIA request for a proper reason, FOIA "does not compel the agency [that received the FOIA request] to take further action in order to produce that document" (quotation marks omitted)); *see also* Dkt. 47-1 at 16–17.

### **III. THIS COURT LACKS JURISDICTION TO ORDER DISCOVERY RELATED TO SECRETARY CLINTON'S USE OF PRIVATE E-MAIL IN THIS CASE.**

Finally, counsel to Secretary Clinton, who have not previously had the chance to address this Court, respectfully urge the Court to reconsider its ruling granting discovery as a general matter. We submit that the Court lacks jurisdiction to order production of documents from Secretary Clinton's private e-mail server equipment, which was not in the Department's possession or control when Judicial Watch submitted its FOIA request. Judicial Watch's allegation of an intent to "thwart" FOIA, even if true, would not alter that fact.

---

employee. *See* Dkt. 49 at 8–11. At Secretary Clinton's direction, her counsel made that determination with respect to her e-mails and provided 55,000 pages of e-mails to the Department.

**A. *Kissinger Controls This Case.***

A court has jurisdiction to “devise remedies and enjoin agencies” under FOIA only if the agency has (1) “improperly”; (2) “withheld”; (3) “agency records.” *Kissinger*, 445 U.S. at 150 (1980) (quotation marks omitted). These requirements are jurisdictional. *See id.*; *see also Bureau of Nat’l Affairs, Inc. v. U.S. DOJ*, 742 F.2d 1484, 1488 (D.C. Cir. 1984).

The Supreme Court construed the statutory term “withheld” in *Kissinger*. In that case, Secretary of State Henry Kissinger had removed transcriptions of his telephone conversations from the State Department and deeded them to the Library of Congress under terms that prohibited public access for 25 years. 445 U.S. at 139–42. The plaintiffs requested the transcriptions under FOIA after Kissinger had deeded them to the Library of Congress. *Id.* at 143. Kissinger and the Library of Congress were “holding the documents under a claim of right.” *Id.* at 155. The Court held that, even assuming that Kissinger’s removal of the records violated the Federal Records Act, the district court lacked authority to order their return to the State Department. *Id.* at 148, 155.

The Supreme Court observed that FOIA “does not obligate agencies to create or retain documents; it only obligates them to provide access to those which it in fact has created and retained.” *Id.* at 152. The Federal Records Act—not FOIA—governs an agency’s obligation to retain records, “even though the agency’s failure to do so deprives the public of information which might have otherwise been available to it.” *Id.* As the Court explained, “[i]f the agency is not required to create or to retain records under the FOIA, it is somewhat difficult to determine why the agency is nevertheless required to retrieve documents which have escaped its possession, but which it has not endeavored to recover.” *Id.* It concluded: “Congress did not mean that an agency improperly withholds a document which has been removed from the possession of the agency prior to the filing of the FOIA request. In such a case, the agency has neither the custody or control

necessary to enable it to withhold.” *Id.* at 150–51. An agency’s “refusal to resort to legal remedies to obtain possession” is not a “withholding” of the record. *Id.* at 151.

The Court thus held that “a ‘withholding’ must . . . be gauged by the time at which the request is made since there is no FOIA obligation to retain records prior to that request.” *Id.* at 155 n.9. Applying this standard, the Court readily found that the State Department had not “withheld” Kissinger’s transcriptions because it did not have “possession or control of the documents at the time the requests were received.” *Id.* at 155. Both the Court of Appeals and this Court have repeatedly applied *Kissinger* to hold that an agency “withholds” agency records only if the records are in its possession or control at the time a FOIA request is made. *See, e.g., Founding Church of Scientology v. Regan*, 670 F.2d 1158, 1163–64 (D.C. Cir. 1981) (reversing a district court order compelling agency to retrieve documents transferred to a third party); *Piper v. U.S. DOJ*, 294 F. Supp. 2d 16, 22 (D.D.C. 2003) (holding that an agency is not required to reconstruct deleted records because “FOIA is triggered by agencies having actual possession of the requested documents”), *aff’d per curiam*, 222 F. App’x 1 (D.C. Cir. 2007); *Judicial Watch, Inc. v. Dep’t of Commerce*, 34 F. Supp. 2d 28, 44 (D.D.C. 1998) (“[T]he status of a particular document *at the time the FOIA request is submitted* determines whether the unreasonable failure to produce that document is an unlawful withholding.”); *see also Competitive Enter. Inst.*, 2016 WL 3606551, at \*5 (Srinivasan, J., concurring) (suggesting that an agency does not have possession or control of documents “held by a person unaffiliated with the agency at the time of the request”).

*Kissinger* squarely governs this case. When Judicial Watch submitted its FOIA request in May 2013, Secretary Clinton was not employed by the State Department. Secretary Clinton held her privately owned server equipment under “a claim of right” and later voluntarily provided that equipment to the FBI for a proper purpose. *Kissinger*, 445 U.S. at 155. Judicial Watch has not

offered any colorable argument that the equipment or e-mail account was under the Department's possession or control at the time of the FOIA request, and the Department has disclaimed that it was. *See* Lang 30(b)(6) Dep. at 108:21–109:11; Dkt. 97-1, at 5–6. This Court lacks jurisdiction to compel production of Secretary Clinton's e-mails.

**B. A General Intent To “Thwart” FOIA Does Not Render *Kissinger* Inapplicable.**

Judicial Watch has argued that *Kissinger* is inapplicable when an agency official seeks to thwart FOIA as a general matter. Dkt. 48, at 4–5. Counsel to Secretary Clinton respectfully submit that this reading of *Kissinger* is incorrect.

In footnote nine of *Kissinger*, the Supreme Court “raised but did not decide whether the ‘possession or control’ requirement ‘might be displaced in the event that it was shown that an agency official purposefully routed a document out of agency possession in order to circumvent a FOIA request.’” *Nat’l Sec. Archive v. Archivist of the U.S.*, 909 F.2d 541, 546 (D.C. Cir. 1990) (per curiam) (quoting *Kissinger*, 445 U.S. at 155 n.9). That footnote does not mean that the “possession or control” test is displaced when an agency official removes agency records to prevent their release to *future* FOIA requesters as a general matter. That reading of the footnote is incompatible with the rest of the *Kissinger* decision. As *Kissinger* recognizes, FOIA “does not obligate agencies to create or retain documents.” 445 U.S. at 152; *see also Whitaker v. CIA*, 31 F. Supp. 3d 23, 46 (D.D.C. 2014) (holding that a failure to retain documents “does not create liability . . . under FOIA”). Except with respect to certain categories of documents not applicable here, an agency's obligation under FOIA arises only *once it receives a FOIA request*. *See* 5 U.S.C. § 552(a)(3)(A). Because FOIA imposes no obligations until receipt of a FOIA request, an agency official cannot “thwart” FOIA by removing agency records *before* the agency receives a request.

Judicial Watch's expansive reading of footnote nine also conflicts with the Supreme Court's decision in *U.S. DOJ v. Tax Analysts*, 492 U.S. 136 (1989). In that case, the Supreme Court observed that materials are "agency records" for purposes of FOIA only if they are "in the agency's control at the time the request is made." *Id.* at 145–46. Invoking *Kissinger* footnote nine, the Court explained that disputes about whether an agency controls requested materials could arise where requested materials are "'purposefully routed . . . out of agency possession in order to circumvent [an impending] FOIA request,'" or are "'wrongfully removed by an individual after a request is filed.'" *Id.* at 146 n.6 (quoting *Kissinger*, 445 U.S. at 155 n.9) (alterations in original).

The Court thus clarified that the question left open by *Kissinger* is whether the "possession or control" standard should be displaced where an agency official removes materials that are the subject of an "impending" (*i.e.*, imminent) FOIA request. That standard requires a close temporal connection between an official's removal of records and a *specific* FOIA request. That standard cannot be satisfied here. Judicial Watch's FOIA request was submitted nearly four months after Secretary Clinton left the State Department, and there is no evidence that Secretary Clinton or anyone else at the Department knew that Judicial Watch would submit the request, let alone intended to circumvent it. Absent such evidence, *Kissinger* footnote nine is irrelevant.

### CONCLUSION

For the foregoing reasons, counsel to Secretary Clinton respectfully request that this Court deny Judicial Watch's motion for permission to depose Secretary Clinton.



Respectfully submitted,

/s/ David E. Kendall

---

David E. Kendall (D.C. Bar No. 252890)  
Katherine M. Turner (D.C. Bar No. 495528)  
Amy Mason Saharia (D.C. Bar No. 981644)  
WILLIAMS & CONNOLLY LLP  
725 Twelfth Street, N.W.  
Washington, DC 20005  
Telephone: (202) 434-5000  
Facsimile: (202) 434-5029  
dkendall@wc.com  
kturner@wc.com  
asaharia@wc.com

*Counsel for Non-Party Hillary Rodham  
Clinton*

July 12, 2016

**CERTIFICATE OF SERVICE**

I, David E. Kendall, counsel for Non-Party Hillary Rodham Clinton, certify that, on July 12, 2016, a copy of this Opposition to Plaintiff's Motion to Depose Hillary Rodham Clinton, Clarence Finney, and John Bentel was filed via the Court's electronic filing system, and served via that system upon all parties required to be served.

/s/ David E. Kendall

David E. Kendall

# EXHIBIT A

## HEARING 4

---

# HEARING 4

BEFORE THE  
SELECT COMMITTEE ON  
THE EVENTS SURROUNDING  
THE 2012 TERRORIST  
ATTACK IN BENGHAZI  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED FOURTEENTH CONGRESS  
FIRST SESSION

HELD IN WASHINGTON, DC, OCTOBER 22, 2015

Printed for the use of the Select Committee on the Events Surrounding the  
2012 Terrorist Attack in Benghazi



Available on the Internet:  
[www.fdsys.gov](http://www.fdsys.gov)

U.S. GOVERNMENT PUBLISHING OFFICE  
WASHINGTON : 2016

98-884

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

there, they seem to fall off your radar in 2012, and the situation is getting much worse in 2012. It was getting much worse.

And let me just share for you, in your records that we have reviewed, there is not one email to you or from you in 2012 when an explosive device went off at our compound in April. There's not a single email in your records about that explosive device.

So my question is: this was a very important mission in 2011. You sent Chris Stevens there, but yet when our compound is attacked in 2012, what kind of culture was created in the State Department that your folks couldn't tell you in an email about a bomb in April of 2012?

Mrs. CLINTON. Well, Congresswoman, I did not conduct most of the business that I did on behalf of our country on email. I conducted it in meetings. I read massive amounts of memos, a great deal of classified information. I made a lot of secure phone calls. I was in and out of the White House all the time. There were a lot of things that happened that I was aware of and that I was reacting to. If you were to be in my office in the State Department, I didn't have a computer. I did not do the vast majority of my work on email. And I bet there's a lot of Sid Blumenthal's emails in there from 2011 too.

Mrs. BROOKS. Well, we'll go into that later.

Mrs. CLINTON. And so I think that there were—I don't want you to have a mistaken impression about what I did and how I did it. Most of my work was not done on emails with my closest aides, with the officials in the State Department, officials in the rest of the government, as well as the White House, and people around the world.

Mrs. BROOKS. And thank you for sharing that because I'm sure that it's not all done on emails, Madam Secretary, and there are meetings, and there are discussions. And so then when our compound took a second attack on June 6, when a bomb blew a wall through the compound then, no emails, no emails at all, but I am interested in knowing who were you meeting with, who were you huddling with, how were you informed about those things, because there is nothing in the emails that talks about two significant attacks on our compounds in 2012?

Mrs. CLINTON. I was meeting—

Mrs. BROOKS. There is a lot of information in 2011 about issues in security posture and yet nothing in 2012.

Mrs. CLINTON. Well, I'd be happy to explain. Every morning when I arrived at the State Department, usually between 8:00 and 8:30, I had a personal one-on-one briefing from the representative of the Central Intelligence Agency, who shared with me the highest level of classified information that I was to be aware of on a daily basis. I then had a meeting with the top officials of the State Department every day that I was in town. That's where a lot of information, including threats and attacks on our facilities, was shared. I also had a weekly meeting every Monday with all of the officials, the Assistant Secretaries and others, so that I could be brought up-to-date on any issue that they were concerned about. During the day, I received hundreds of pages of memos, many of them classified, some of them so top secret that they were brought into my office in a locked briefcase that I had to read and immediately return

And while you are answering that, I want to inform and instruct why I am asking it. You have mentioned the ARB on a number of occasions again today. This was not the first ARB. We had one after Kenya and Tanzania. And that ARB could not have been more specific: The Secretary of State should personally review the security situation of our embassy facilities. That ARB put the responsibility squarely on you.

So, with respect to that previous ARB recommendation and, in contrast, what did make your inbox versus what did not, did you personally review our security situation, as the previous ARB required?

Mrs. CLINTON. Well, let me see if I can answer the many parts of your question, Mr. Chairman.

Yes, personal email came to my personal account. Work-related email did, as well. And I also relied on a number of my aides and staff members, as well as experienced Foreign Service officers and civil servants, who were similarly engaged in gathering information and sharing it.

And, as I said and I will repeat, Chris Stevens communicated with a number of people that I worked with on a daily basis in the State Department. So far as I know, he did not raise any issue of security with any of those people. He raised it where he knew it would be properly addressed. If he had raised it with me, I would be here telling you he had. He did not.

And so I think it's important to try to separate out the various elements of your question, Mr. Chairman, and I will do my best to continue to try to answer your questions.

But I have said before and I will repeat again: Sid Blumenthal was not my adviser, official or unofficial, about Libya. He was not involved in any of the meetings, conversations, other efforts to obtain information in order to act on it.

On occasion, I did forward what he sent me to make sure that it was in the mix so, if it was useful, it could be put to use. And I believe in response to the email you pointed out originally from Ambassador Stevens, he actually said it rang true and it was worth looking into.

So I think it's important that we separate out the fact that Mr. Blumenthal was not my adviser. He was not an official of the United States Government. He was not passing on official information. He, like a number of my friends, would hand me a newspaper article, would buttonhole me at a reception and say, what about this, or what about that, were trying to be helpful. Some of it was. A lot of it wasn't.

Chairman GOWDY. The chair will now recognize the gentlelady from California, Ms. Sanchez.

Ms. SANCHEZ. Thank you.

Secretary Clinton, I listened very carefully when Chairman Gowdy was questioning you in the first round of questioning. I have to say I was kind of surprised.

We waited more than a year to finally get you up here to testify. We spent almost \$5 million, and we interviewed about 54 witnesses. And when the chairman finally got his chance to question you, he asked you over—he quibbled, actually, over the definition of the word “unsolicited.”

401

more about the situation as well and the lack of getting the records.

Of course, this second statement, the revised statement, was after this committee had contacted Huma Abedin, Jake Sullivan, Philippe Reines, asking for their personal accounts, which of course you knew would mean we would get their emails, and that first statement in March was not accurate.

In March, you said no classified information was sent or received on your personal accounts. You later revised your statement and said no information marked classified was sent or received on your personal account. And, once again, your revised statement was after the Inspector General for the Intelligence Community had examined your emails and determined that, yes, some indeed were classified.

Secretary Clinton, it seems like there's a pattern, a pattern of changing your story. In March, you say one thing. The truth comes out. Weeks and months later, you say something else.

That's not being the most transparent person ever. That's not even being transparent. So if your story about your emails keeps changing, then how can we accept your statement that you've turned over all work-related emails and all emails about Libya?

Mrs. CLINTON. Well, Congressman, I have said repeatedly that I take responsibility for my use of personal email. I've said it was a mistake. I've said that it was allowed, but it was not a good choice. When I got to the Department, we were faced with a global financial crisis, major troop decisions on Afghanistan, the imperative to rebuild our alliances in Europe and Asia, an ongoing war in Iraq, and so much else.

Email was not my primary means of communication, as I have said earlier. I did not have a computer on my desk. I've described how I did work, in meetings, secure and unsecure phone calls, reviewing many, many pages of materials every day, attending—

Mr. JORDAN. I appreciate—

Mrs. CLINTON [continuing]. A great deal of meetings. And I provided the Department, which has been providing you, with all of my work-related emails, all that I had, approximately 55,000 pages, and they are being publicly released.

Mr. JORDAN. I appreciate that. And let's get into that. Those 55,000 pages, there were 62,000 emails, total emails on your system. You have stated that you used a multistep process to determine which ones are private, which ones are public, which ones belong to you and your family, which ones belonged to the taxpayer.

Who oversaw this multistep process in making that determination of which ones we might get and which ones that were personal?

Mrs. CLINTON. That was overseen by my attorneys, and they conducted a rigorous review of my emails and were—

Mr. JORDAN. And these are the folks sitting behind you there, Mr. Kendall, Ms. Mills, Ms. Samuelson?

Mrs. CLINTON. Yes. That's right.

Mr. JORDAN. All right. And you said "rigorous." What does that mean?

402

Mrs. CLINTON. It means that they were asked to provide anything that could be possibly construed as work-related. In fact, in my opinion, and that has been confirmed by both——

Mr. JORDAN. But I'm asking how——

Mrs. CLINTON [continuing]. The State Department and——

Mr. JORDAN. But I'm asking how it was done. Was—did someone physically look at the 62,000 emails, or did you use search terms, date parameters? I want to know the specifics.

Mrs. CLINTON. They did all of that. And I did not look over their shoulders because I thought it would be appropriate for them to conduct that search, and they did.

Mr. JORDAN. Will you provide this committee—or can you answer today, what were the search terms?

Mrs. CLINTON. The search terms were everything you could imagine that might be related to anything, but they also went through every single email.

Mr. JORDAN. But that's not answering the question. What were the search terms? Search terms means terms. What terms did you use——

Mrs. CLINTON. I did not——

Mr. JORDAN [continuing]. And what were the date parameters? With what date did you start? What was the end date and the emails in between they were going to look at?

Mrs. CLINTON. Well, Congressman, I asked my attorneys to oversee the process. I did not look over their shoulder, I did not dictate how they would do it. I did not ask what they were doing and how they——

Mr. JORDAN. So you don't know?

Mrs. CLINTON [continuing]. Made the decisions.

Mr. JORDAN. You don't know what terms they used to determine which ones were your emails and which ones the State Department got and therefore we might get?

Mrs. CLINTON. You know, the State Department had between 90 and 95 percent of all the ones that were work-related. They were already on the system. In fact, this committee got emails——

Mr. JORDAN. I'm not asking about those. I'm asking about the 62,000 that were exclusively on your system.

Mrs. CLINTON. Ninety to 95 percent of all work-related emails were already in——

Mr. JORDAN. Well, we know that the National Archivist—Secretary Clinton, we know the National Archivist said 1,250 were clearly personal, no way we should have—no way you should have sent them to the State Department. And then we also know that 15 you missed because we got those from Mr. Blumenthal when he came and was—for his deposition.

So if you missed 15 you should have given us and you gave us 1,250 that, not we say, but the National Archivist says you never should have turned over, you erred on both sides. So, again, that's why we want to know the terms because if you've made a mistake both ways, you might have made more mistakes we don't know.

Mrs. CLINTON. Well, first of all, you had nine hours with one of my attorneys. And since, I think, the Democrats just finally released the transcript——

Mr. JORDAN. And I——



Mrs. CLINTON. I haven't had a chance——

Mr. JORDAN. And I specifically asked Ms. Mills. I did.

Mrs. CLINTON. Well——

Mr. JORDAN. I did. I asked her about this, and she gave me basically the same kind of answer you're giving me.

Mrs. CLINTON. Well, she'll be happy to supplement the record if she——

Mr. JORDAN. Well, she's not on the witness stand today; you are, and I'm asking you.

Mrs. CLINTON. Well, but I asked my attorneys to do it. I thought that was the appropriate way to proceed.

Mr. JORDAN. Let me do one other statement. Let me do one other statement——

Mrs. CLINTON. Okay.

Mr. JORDAN [continuing]. Because it sounds like—I hope you'll turn those—I hope we'll know the terms. I think the American people would like to know what terms you used to determine what we might get so that we could get all the information on Libya and find out what happened where these four Americans gave their lives. I think that's critical.

In March you also said this: your server was physically located on your property, which is protected by the Secret Service. Now, I've had a hard time figuring this out, because this story's been all over the place, but there was one server on your property in New York and a second server hosted by a Colorado company and housed in New Jersey. Is that right? There were two servers?

Mrs. CLINTON. No.

Mr. JORDAN. Okay.

Mrs. CLINTON. There was a—there was a server——

Mr. JORDAN. Just one?

Mrs. CLINTON [continuing]. That was already being used by my husband's team, an existing system in our home that I used. And then, later, again, my husband's office decided that they wanted to change their arrangements, and that's when they contracted with the company in Colorado.

Mr. JORDAN. And so there's only one server, is that what you're telling me, and it's the one server that the FBI has?

Mrs. CLINTON. The FBI has the server that was used during the tenure of my State Department service.

Mr. JORDAN. Okay. In your statement, you say, which was protected by the Secret Service. Why'd you mention the Secret Service?

Mrs. CLINTON. Well, because——

Mr. JORDAN. And here's why I'm—could a Secret Service agent standing at the back door of your house protect someone in Russia or China from hacking into your system? Why did you mention the Secret Service agent?

Mrs. CLINTON. Out of just an abundance of being transparent.

Mr. JORDAN. Transparent? I—but—and how—what's the relevance to protecting from classified information?

Mrs. CLINTON. There was nothing marked classified on my emails, either sent or received. And I want to respond——

Mr. JORDAN. You used the right term there, you used "marked." That's the one—that's what you——

408

Mr. WESTMORELAND. Well, if they were gathering emails, you had to tell them that you had a private server——

Mrs. CLINTON. Well——

Mr. WESTMORELAND [continuing]. Because you were there.

Mrs. CLINTON. Well, the server is not the point; it's the account. And I made it a practice to send emails that were work-related to people on their government accounts. In fact——

Mr. WESTMORELAND. Ma'am——

Mrs. CLINTON [continuing]. You know, Secretary Kerry is the first Secretary of State to rely primarily on a government account. So——

Mr. WESTMORELAND. But I'm not talking about the account; I'm talking about the server. But one last point. Let me just—I'll close with this, and then the chairman can give you time to answer. You want me to tell you what I thought? I think that your attorneys sat down with the State Department, and they said: We've got a problem, and so we've got to come up with something that this is not just the secretary having these emails in a private server, so I tell you what let's do. Let's go back and ask Madeleine Albright, who was Secretary of State in 1997, that never even had an email account, or let's go back and ask, you know, Colin Powell, Condoleezza Rice, and me to provide all this information.

Ms. SANCHEZ. Regular order, Mr. Chairman.

Mr. WESTMORELAND. I'm just telling you, it smells, it doesn't smell right.

And so I yield back.

Mrs. CLINTON. Well, if I could respond, I think in the course of trying to answer and archive information, the State Department determined that they did have gaps in their record-keeping, and it was much more than about me. They had gaps with respect to others, both other Secretaries and others within the State Department. And the technology in the State Department, indeed, throughout our entire government, is notoriously difficult and often unreliable. And I think it was the State Department's efforts to try to fill some of those gaps. So I didn't know at the time that there had been such a meeting. I learned of it subsequently.

And when I received a copy of the letter that was sent by the State Department to me and the other three preceding secretaries of state, I immediately said, "Well, let's help them fill the gaps," even though I believed that the vast majority of my emails were already in their system, and we did. We conducted the investigation, the survey that I have described to you, and turned over more than 30,000 work-related emails, 55,000 pages, to the State Department; 90 to 95 percent were already there. We sent so many that some were going to be returned because they were clearly not work-related.

We did our best. I did my best to make sure that if there were gaps in record-keeping, at least my materials would be there to help fill any gaps above and beyond the 90 to 95 percent of emails that were already in the system.

Mr. WESTMORELAND. Well, I'm not an attorney, but I think Ms. Mills is a good attorney——

Ms. SANCHEZ. Regular order, Mr. Chairman.

Mr. WESTMORELAND [continuing]. And she never told you——

425

Mrs. CLINTON. Well, one is a shorthand, Mr. Chairman.

Chairman GOWDY. Well, why not just tell the court, "I turned over everything"?

Mrs. CLINTON. Well, you know how lawyers are. They use more words, perhaps, than they need.

Chairman GOWDY. Trust me, I know that. And they charge you for every one of them.

Mrs. CLINTON. Yes. I'm well aware of that, Mr. Chairman. And the clock is ticking.

Chairman GOWDY. Well, one more. One more. And I will pay Mr. Kendall's fee for the last question. How's that?

Mrs. CLINTON. Oh, I don't think you want to do that, Mr. Chairman.

Chairman GOWDY. I probably can't do it.

You see my point, though? You are very definitive when you are talking to the American people that you turned over everything.

Mrs. CLINTON. That's right.

Chairman GOWDY. But there are those kind of lawyerly fudge words when you are talking to court, "on information and belief."

Mrs. CLINTON. Well—

Chairman GOWDY. And the reality is, even tonight, you cannot tell us that you turned over everything, because you didn't think you missed the 15.

Mrs. CLINTON. Well, I didn't have them. I turned over everything I had. Everything I had—

Chairman GOWDY. Which means the system you had—

Mrs. CLINTON [continuing]. Has been turned over to the State Department.

Chairman GOWDY [continuing]. Somehow missed those 15.

Mrs. CLINTON. Well—

Chairman GOWDY. Last question on your system. Mr. Cummings said that your email arrangement was inappropriate. I think the President may have said it was a mistake. You have said that it was a mistake.

My question to you, Madam Secretary, is, was it a mistake for the four years that you had that email arrangement? Was it a mistake for the almost two years that you kept the public record to yourself? Or has it manifested itself as a mistake in just the last six months?

Mrs. CLINTON. Well, since I believed that all of my work-related emails to dot-gov accounts were being captured and preserved, it wasn't until I was asked to help the State Department to fill in what they saw as some recordkeeping gaps, not just with me but with others.

I did the best I could during those four years and thought that everything that I was emailing that was work-related was being preserved.

Chairman GOWDY. If you can find the source for the 90 to 95 percent, I would be grateful for it, and we would probably have fewer questions. If there is a source that you can provide that 90 to 95 percent were on the State Department system, then I will know that I need to ask the State Department what took them so long.

# EXHIBIT B

SELECT COMMITTEE ON BENGHAZI,  
U.S. HOUSE OF REPRESENTATIVES,  
WASHINGTON, D.C.

---

INTERVIEW OF: HUMA ABEDIN

FRIDAY, OCTOBER 16, 2015

Washington, D.C.

The interview in the above matter was held in Room HVC-205,  
Capitol Visitor Center, commencing at 10:07 a.m.

Present: Representatives Westmoreland, Pompeo, and Cummings.

Q Okay. Was there a memo that went out to all staff from Under Secretary Kennedy requesting that anybody who had information to provide it to the ARB? Do you recall that?

A I don't. If there was one, I don't remember receiving it.

Q Do you recall if the Secretary provided any documents to the ARB?

A I'm not aware of what she provided.

Q Okay. Who would have played a role in that if she were to provide documents to the ARB?

A It would have been our chief of staff, Cheryl Mills.

Q Okay. During the time that you worked with the Secretary, were you ever part of or privy to a conversation regarding complying with FOIA requests that particularly involved the Secretary's records?

A No, I wasn't aware that had ever happened. No.

Q Okay. So you were unaware that there had ever been a FOIA request regarding records of the Secretary individually?

A While we were at State or post State?

Q Let's start with while you were at the State Department.

A Not at all that I remember.

Q Okay. What about after you left the State Department?

A That was not something -- no, that wasn't something that happened outside her attorneys.

Q Okay. During the time that you were at the State Department, you were aware that the Secretary was using a personal email address; is that correct?

Q They did not?

A No.

Q Do you know how many did? How many people did? Obviously the Secretary did and you did.

A I think the only additional person was Chelsea.

Q What if any discussions did you have with the Secretary regarding the use of this new email address as her exclusive means of electronic communication as Secretary of State?

A I don't recall having many conversations. It was a natural progression from what she was doing previously, and she continued to do so.

---

Q And I just want to be precise here. You said you don't remember many conversations. Were there any conversations?

A I don't remember any conversations. I think those of us who were part of her senior leadership at the State Department all regret that we didn't think about it more, but we really didn't.

Q When she went in as Secretary of State, had they set up a state.gov account for her in anticipation of her arrival?

A Not that I'm aware of.

Q Did you or did anyone, to your knowledge, communicate with the State Department that she would not be using -- did you or others tell the IT department or the executive secretary or the executive assistant that she did not want one?

A I don't remember anyone discussing it with us. You know, we were coming into a bureaucracy. I don't know that they

A Do I know if he was consulted?

Q Uh-huh.

A I don't.

Q At any time, did he raise any concerns about her use of a personal email account?

A Not to me, that I remember.

Q Of all of the people that we've talked about, the deputy secretaries, the select under secretaries, a few assistant secretaries, at any time did anyone raise any type of concern about the Secretary exclusively use -- let me state that differently.

At any time did any of these individuals voice any type of concern over the secretary's use of a personal email account?

A No.

Q Okay. Did any of these individuals know that the Secretary was exclusively using a personal email account?

A Not that I'm aware of.

Q Okay. Do you know whether the Secretary or anyone on her behalf consulted with the National Archives and Record Administration regarding the exclusive use of a personal email?

A I don't believe so.

Q Do you believe that did not happen?

A I certainly did not do it on her behalf.

Q Okay. Do you know whether she told officials at the White House that it was going to be her exclusive means of electronic communication?



details, did you feel that your ability to just communicate in terms of the reliability was reasonably good on the account that the Secretary was using on her personal email account?

A From -- you know, from my memory, it was -- it was fairly reliable. There -- it was -- you know, there were instances where it wasn't working for a period; there was a delay by a couple of hours or something. I'm not saying there was never any technical issues at all in the 4 years, but it felt like we had just as many, if not many more instances, with State.gov going down for a period. So it wasn't exclusive to one email or another.

Q Right. I mean, I recall you talking a little bit about a particular problem and difficulty you had had with a fax machine --

A Yes.

Q -- and that --

A Yes.

Q -- seemed to me that that was a State Department fax setup, because it sounded like it was the secure fax.

A That's correct.

Q It's not that the State system would have been perfect either. Is that fair to say?

A That is fair to say, in my opinion, yes.

Q And in either case, if you encountered a problem, you were not going to be the technology person to solve the problem. Is that fair?

A That's fair.

your own email practices and usage, you had indicated that you used the account that the State Department had provided for you when you were there.

A Yes.

Q And you said that, I think in just explaining to us, you said, you know, I do try always to do the right thing. And I just wanted to explore that with you a little bit, because I think that some could read that as you having then said that you believed that at the time she did it and made the decisions, that the Secretary wasn't trying to do the right thing, and I just wanted to get a sense as to whether or not that's what you were trying to convey.

A Oh, no. I mean, not at all. I was only speaking on -- I was only speaking on my own behalf in terms of my own practices. I think, you know, she has said it, you know, I will repeat it again, I know other members of our senior team probably feel the same way, we all regret that we didn't -- we weren't more conscious about her email practices or the device or the account that she used when she joined the State Department. It just wasn't anything that we gave much thought to. She has publicly said she did it as a matter of convenience. In hindsight, none of us would have made the same choice, but it was -- you know, it was a mistake, she's clearly said it. And I -- I wasn't comparing that to my own -- my own email practices.

Q And certainly, you were not conveying your belief that what she did was in any way against the law or unlawful to have used personal email for work-related purposes?

# EXHIBIT C

## NewsRoom

7/7/16 CQ-RollCall Pol. Transcriptions 23:57:00

CQ-RollCall Political Transcriptions  
Copyright (c) 2016 Roll Call, Inc.

July 7, 2016

### REP. JASON CHAFFETZ HOLDS A HEARING ON THE FBI RECOMMENDATION REGARDING HILLARY CLINTON'S PRIVATE EMAIL SERVER

(CORRECTED COPY)

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOLDS A HEARING ON THE FBI  
RECOMMENDATION REGARDING HILLARY CLINTON'S PRIVATE E-MAIL SERVER, PANEL 1

JULY 7, 2016

SPEAKERS: REP. JASON CHAFFETZ, R-UTAH. CHAIRMAN REP. JOHN L. MICA, R-FLA. REP. MICHAEL  
R. TURNER, R-OHIO REP. JOHN J. DUNCAN JR., R-TENN. REP. KEN BUCK, R-COL. REP. JIM JORDAN,  
R-OHIO REP. JODY B. HICE, R-GA. REP. TIM WALBERG, R-MICH. REP. GLENN GROTHMAN, R-  
WISC. REP. JUSTIN AMASH, R-MICH. REP. PAUL GOSAR, R-ARIZ. REP. BUDDY CARTER, R-GA. REP.  
SCOTT DESJARLAIS, R-TENN. REP. TREY GOWDY, R-S.C. REP. STEVE RUSSELL, R-OK. REP. WILLIAM  
HURD, R-TEXAS REP. BLAKE FARENTHOLD, R-TEXAS REP. GARY PALMER, R-AL. REP. CYNTHIA M.  
LUMMIS, R-WYO. REP. MARK WALKER, R-N.C. REP. THOMAS MASSIE, R-KY. REP. MICK MULVANEY,  
R-S.C. REP. ROD BLUM, R-IND. REP. RON DESANTIS, R-FLA. REP. MARK MEADOWS, R-N.C.

REP. ELIJAH E. CUMMINGS, D-MD. RANKING MEMBER REP. CAROLYN B. MALONEY, D-N.Y. DEL.  
ELEANOR HOLMES NORTON, D-D.C. REP. WILLIAM LACY CLAY, D-MO. REP. STEPHEN F. LYNCH,  
D-MASS. REP. JIM COOPER, D-TENN. REP. GERALD E. CONNOLLY, D-VA. REP. MATT CARTWRIGHT,  
D-PA. REP. TAMMY DUCKWORTH, D-ILL. REP. MICHELLE LUJAN GRISHAM, D-N.M. REP. PETER  
WELCH, D-VT. REP. ROBIN KELLY, D-ILL. REP. BRENDA L. LAWRENCE, D-MICH. REP. BRENDAN F.  
BOYLE, D-PA. REP. MARK DESAULNIER, D-CALIF. REP. TED LIEU, D-CALIF. DEL. STACEY PLASKETT,  
D-VIRGIN IS. REP. BONNIE WATSON COLEMAN, D-N.J.

WITNESSES: FBI DIRECTOR JAMES COMEY

[\*] 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.

CHAFFETZ: My -- I have the greatest admiration for the FBI. My grandfather was a career FBI agent.

COMEY: I believe so.

DESANTIS: And she knowingly clearly set up her own private server in order to -- let me ask you that, was the reason she set up her own private server in your judgment was because she wanted to shield communications from Congress and the public?

COMEY: I can't say that.

Our best information is that she set it up as a matter of convenience. It was an existing system her husband had and she decided to have a domain on that system.

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?

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

DESANTIS: Isn't she in an original classification of authority?

COMEY: Yes, sir.

DESANTIS: Good grief.

Well, I appreciate you coming. I yield back the balance of my time.

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. I now recognize the gentleman from Missouri, Mr. Clay, for five minutes.

CLAY: Thank you, Mr. Chairman. 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 first hand 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 two 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's 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.

CHAFFETZ: Thank the gentleman. I will now recognize the gentleman from Arizona, Mr. -- Mr. Goshar. Oh, let's go ahead and go to the gentleman from South Carolina, Mr. Mulvaney first.

MULVANEY: Thank you gentleman. Director Comey, earlier today you heard a long list of statements that Ms. 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?

COMEY: I'm not equipped sitting here without the 302 in front of me to answer in that broad...

MULVANEY: But it's your -- it's your testimony...

COMEY: But I have no basis -- we do not have a basis for concluding she lied to the FBI.

MULVANEY: Gotcha. Did anybody ask her on Saturday, why she told y'all one thing and told us another?

COMEY: I don't know as I sit here. I mean, I can -- I'll figure that out.

MULVANEY: Would that have been of interest to you in helping to establish intent?

COMEY: It could have been, sure.

MULVANEY: More importantly I think, did anybody ask her why she set up the email system as she did in the first place?

COMEY: Yes.

MULVANEY: And the answer was convenience?

COMEY: Yeah, it was already there. It was a system her husband had and so she just jumped on to it.

MULVANEY: Were you aware that just earlier this week, her -- her assistant actually said it was for an entirely different reason? It was to -- it was to keep emails from being accessible, and that it was for concealment purpose. So she was -- Huma Abedin was asked in her deposition why it was set up.

And it was said, to keep her personal emails from being accessible. To the question, to whom? To anybody. Where you aware of that testimony?

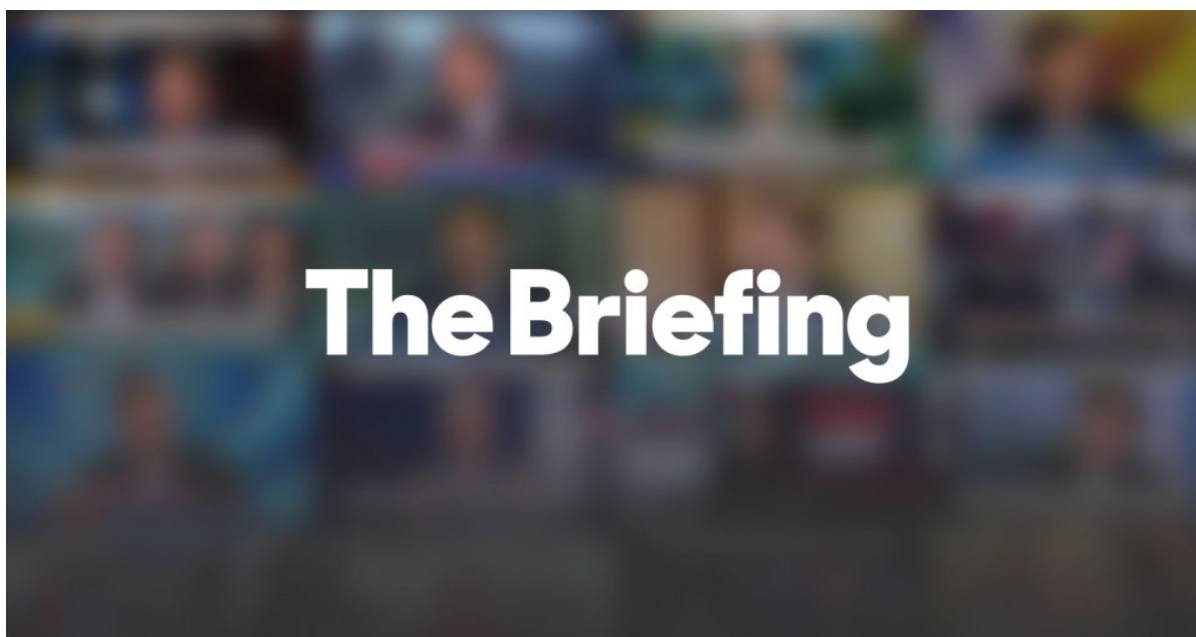
COMEY: Generally, yes.

MULVANEY: OK. So here's -- 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 -- to your testimony, your findings, she was careless regarding its technical security.

I think you 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.

# EXHIBIT D

## THE BRIEFING

**Factsheets**

## Updated: The Facts About Hillary Clinton's Emails

We've put all of the information about Hillary Clinton's State Department emails here. Just the facts, all in one place.

### ***Why did Clinton use her own email account?***

When Clinton got to the Department, she opted to use her personal email account as a matter of convenience. It enabled her to reach people quickly and keep in regular touch with her family and friends more easily given her travel schedule.

That is the only reason she used her own account.

Her usage was widely known to the over 100 State Department and U.S. government colleagues she emailed, consistent with the practice of prior Secretaries of State and permitted at the time.

As Clinton has said, in hindsight, it would have been better to just have two accounts. While she thought using one account would be easier, obviously, that has not been the case.



***Was it allowed?***

Yes. The laws, regulations, and State Department policy in place during her tenure permitted her to use a non-government email for work.

The 2009 National Archives regulation in place during her tenure required that "[a]gencies 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." The regulation recognizes the use of non-government email accounts.

As she has stated, Clinton's practice was to email government officials on their ".gov" accounts, so her work emails were immediately captured and preserved. In fact, more than 90% of those emails should have already been captured in the State Department's email system before she provided them with paper copies.

A Politifact analysis also confirmed that Clinton's practices complied with laws and regulations, including support from the former director of a prominent government accountability organization: "In Clinton's defense, we should note that it was only after Clinton left the State Department, that the National Archives issued a recommendation that government employees should avoid conducting official business on personal emails (though they noted there might be extenuating circumstances such as an emergency that require it). Additionally, in 2014, President Barack Obama signed changes to the Federal Records Act that explicitly said federal officials can only use personal email addresses if they also copy or send the emails to their official account. Because these rules weren't in effect when Clinton was in office, 'she was in compliance with the laws and regulations at the time,' said Gary Bass, founder and former director of OMB Watch, a government accountability organization."

***Clinton said she did not use her email to send or receive classified information, but the State Department and two Inspectors General said some of these emails do contain classified information. Was her statement inaccurate?***

Clinton only used her account for unclassified email. No information in Clinton's emails was marked classified at the time she sent or received them.

When information is reviewed for public release, it is common for information previously unclassified to be upgraded to classified if the State Department or another agency believes its public release could cause potential harm to national security, law enforcement or diplomatic relations.

After reviewing a sampling of the 55,000 pages of emails, the Inspectors General have proffered that a small number of emails, which did not contain any classified

markings and/or dissemination controls, should have been classified at the time they were sent. The State Department has said it disagrees with this assessment.

Clinton hopes the State Department and the agencies involved in the review process will sort out as quickly as possible which of the 55,000 pages of emails are appropriate to share with the public.

***How did Clinton receive and consume classified information?***

The Secretary's office was located in a secure area. Classified information was viewed in hard copy by Clinton while in the office. While on travel, the State Department had rigorous protocols for her and traveling staff to receive and transmit information of all types.

A separate, closed email system was used by the State Department for the purpose of handling classified communications, which was designed to prevent such information from being transmitted anywhere other than within that system.

***Is Department of Justice conducting a criminal inquiry into Clinton's email use?***

No. As the Department of Justice and Inspectors General made clear, the IGs made a security referral. This was not criminal in nature as misreported by some in the press. The Department of Justice is now seeking assurances about the storage of materials related to Clinton's email account.

***Is it true that her email server and a thumb drive were recently turned over to the government? Why?***

Again, when information is reviewed for public release, it is common for information previously unclassified to be upgraded to classified if the State Department or another agency believes its public release could cause potential harm to national security, law enforcement or diplomatic relations.

Clinton hopes that State and the other agencies involved in the review process will sort out as quickly as possible which emails are appropriate to share with the public, and that the release will be as timely and as transparent as possible.

When the Department upgraded some of the previously unclassified email to classified, her team worked with the State Department to ensure copies of her emails were stored in a safe and secure manner. She also directed her team to give her server that hosted her email account while she was Secretary to the Department of Justice, as well as a thumb drive containing copies of her emails that already had been provided to the State Department. Clinton has pledged to cooperate with the government's security inquiry.

***Would this issue not have arisen if she used a state.gov email address?***

Even if Clinton's emails had been on a government email address and government device, these questions would be raised prior to public release.

While the State Department's review of her 55,000 emails brought the issue to the Inspectors General's attentions, the emails that recently were upgraded to classified prior to public release were on the unclassified .gov email system. They were not on the separate, closed system used by State Department for handling classified communications.

***Have Clinton's State Department aides also been asked to provide the Department and Congress with emails from their personal accounts?***

We understand that members of her State Department staff were recently asked to assist the Department in its record-keeping by providing any work-related emails they may have on personal accounts. They have received requests from Rep. Gowdy as well.

Clinton is proud of the work of all the dedicated public servants that were part of her team at the State Department. She was proud of her aides then and is proud of them now, as they have committed - as she has - to being as helpful as possible in responding to requests.

***Press reports say she used multiple devices – a Blackberry and an iPad – is that true?***

Clinton relied on her Blackberry for emailing. This was easiest for her. When the iPad came out in 2010, she was as curious as others and found it great for shopping, browsing, and reading articles when she traveled. She also had access to her email account on her iPad and sometimes used it for that too.

***Was she ever provided guidance about her use of a non-".gov" email account?***

The State Department has and did provide guidance regarding the need to preserve federal records. To address these requirements, it was her practice to email government employees on their ".gov" email address. That way, work emails would be immediately captured and preserved in government record-keeping systems.

***What did Clinton provide to the State Department?***

On December 5, 2014, 30,490 copies of work or potentially work-related emails sent and received by Clinton from March 18, 2009, to February 1, 2013, were provided to the State Department. This totaled roughly 55,000 pages. More than 90% of her work or potentially work-related emails provided to the Department were already in

the State Department's record-keeping system because those e-mails were sent to or received by "state.gov" accounts.

Early in her term, Clinton continued using an att.blackberry.net account that she had used during her Senate service. Given her practice from the beginning of emailing State Department officials on their state.gov accounts, her work-related emails during these initial weeks would have been captured and preserved in the State Department's record-keeping system. She, however, no longer had access to these emails once she transitioned from this account.

***Why did the Select Committee announce that she used multiple email addresses during her tenure?***

In fairness to the Committee, this was an honest misunderstanding. Clinton used one email account during her tenure at State (with the exception of her initial weeks in office while transitioning from an email account she had previously used). In March 2013, a month after she left the Department, Gawker published the email address she used while Secretary, and so she had to change the address on her account.

At the time the printed copies were provided to the Department in 2014, because it was the same account, the new email address established after she left office appeared on the printed copies as the sender, and not the address she used as Secretary. In fact, this address on the account did not exist until March 2013. This led to understandable confusion that was cleared up directly with the Committee after its press conference.

***Why didn't Clinton provide her emails to the State Department until December 2014?***

In 2014, after recognizing potential gaps in its overall recordkeeping system, the State Department asked for the help of the four previous former Secretaries in meeting the State Department's obligations under the Federal Records Act.

Clinton responded to this request by providing the State Department with over 55,000 pages of emails. As it was Clinton's practice to email U.S. government officials on their .gov accounts, the overwhelming majority of these emails should have already been preserved in the State Department's email system.

In providing these emails to the Department, Clinton included all she had that were even potentially work-related—including emails about using a fax machine or asking for iced tea during a meeting—errring on the side of over-inclusion, as confirmed by the Department and National Archives' determination that over 1250 emails were "personal" records (which they have indicated will be returned to her).

After providing her work and potentially work-related emails, she chose not to keep her personal, non-work related emails, which by definition, are not federal records and were not requested by the Department or anyone else.

***Why did the State Department ask for assistance in collecting records? Why did the State Department need assistance in further meeting its requirements under the Federal Records Act?***

The State Department formally requested the assistance of the four previous former Secretaries in a letter to their representatives dated October 28, 2014, to help in further meeting the Department's requirements under the Federal Records Act.

The letter stated that in September 2013, the National Archives and Records Administration (NARA) issued new guidance clarifying records management responsibilities regarding the use of personal email accounts for government business.

While this guidance was issued after all four former Secretaries had departed office, the Department decided to ensure its records were as complete as possible and sought copies of work emails sent or received by the Secretaries on their own accounts.

***Why did Clinton decide not to keep her personal emails?***

As Clinton has said before, these were private, personal messages, including emails about her daughter's wedding plans, her mother's funeral services and condolence notes, as well as emails on family vacations, yoga routines, and other items one would typically find in their own email account, such as offers from retailers, spam, etc.

***Did Clinton delete any emails while facing a subpoena?***

No. As noted, the emails that Clinton chose not to keep were personal emails—they were not federal records or even work-related—and therefore were not subject to any preservation obligation under the Federal Records Act or any request. Nor would they have been subject to the subpoena—which did not exist at the time—that was issued by the Benghazi Select Committee some three months later.

Rep. Gowdy's subpoena issued in March 2015 did not seek, and had nothing to do with, her personal, non-work emails nor her server nor the request by State Department last year for her help in their own record-keeping. Indeed in his March 19th letter, Rep. Gowdy expressly stated he was not seeking any emails that were "purely personal in nature."

In March 2015, when Rep. Gowdy issued a subpoena to Clinton, the State Department had received all of Clinton's work-related emails in response to their

2014 request, and indeed, had already provided Clinton's relevant emails to Rep. Gowdy's committee.

Rep. Gowdy, other Republicans, and some members of the media have seized on a CNN interview with Clinton to question her on this point. Rep. Gowdy has even gone so far as to say Clinton is lying. But he and the others are clearly mistaken.

As Vox reported, "[S]he didn't lie about the subpoena. ... Clinton clearly wasn't responding to the question of whether she'd ever been subpoenaed by the Benghazi Committee but whether she'd been subpoenaed before she wiped the emails from her server." Additionally, Factcheck.org said in its analysis, "Clinton's denial came in response to a question about deleting emails 'while facing a subpoena,' and Clinton objected to Keilar's 'assumption.' Clinton's campaign said that the emails were deleted before she received the subpoena and that was the point Clinton was making." Politifact added, "Suggesting that Clinton deleted emails while facing a subpoena contradicts what we know about the controversy so far."

Vox went on to further decry Rep. Gowdy's reaction, saying, "[T]his one's a particularly absurd gimmick, even for a committee that is selectively leaking from depositions and documents to justify its existence. If there was a more extreme category of dissembling than 'pants on fire,' now would be the time for Politifact to roll it out on the House Republicans."

***Why was the State Department given printed copies?***

That is the requirement. The instructions regarding electronic mail in the Foreign Affairs Manual (the Department's policy manual) require that "until technology allowing archival capabilities for long-term electronic storage and retrieval of email 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." [5 FAM 443.3].

***Were any work items deleted in the course of producing the printed copies?***

No.

***How many emails were in her account? And how many of those were provided to the State Department?***

Her email account contained a total of 62,320 sent and received emails from March 2009 to February 2013. Based on the review process described below, 30,490 of these emails were provided to the Department, and the remaining 31,830 were private, personal records.

### ***How and who decided what should be provided to the State Department?***

The Federal Records Act puts the obligation on the government official to determine what is and is not a federal record. The State Department Foreign Affairs Manual outlines guidance "designed to help employees determine which of their e-mail messages must be preserved as federal records and which may be deleted without further authorization because they are not Federal record materials." [5 FAM 443.1 (c)].

Following conversations with State Department officials and in response to the State Department's 2014 letter to former Secretaries, Clinton directed her attorneys to assist by identifying and preserving all emails that could potentially be federal records. This entailed a multi-step process to review each email and provide printed copies of Clinton's emails to the State Department, erring on the side of including anything that might be even potentially work-related.

A search was conducted on Clinton's email account for all emails sent and received from 2009 to her last day in office, February 1, 2013.

After this universe was determined, a search was conducted for a ".gov" (not just state.gov) in any address field in an email. This produced over 27,500 emails, representing more than 90% of the 30,490 printed copies that were provided to the State Department.

To help identify any potential non-".gov" correspondence that should be included, a search of first and last names of more than 100 State Department and other U.S. government officials was performed. This included all Deputy Secretaries, Under Secretaries, Assistant Secretaries, Ambassadors-at-Large, Special Representatives and Envoys, members of the Secretary's Foreign Policy Advisory Board, and other senior officials to the Secretary, including close aides and staff.

Next, to account for non-obvious or non-recognizable email addresses or misspellings or other idiosyncrasies, the emails were sorted and reviewed both by sender and recipient.

Lastly, a number of terms were specifically searched for, including: "Benghazi" and "Libya."

These additional three steps yielded just over another 2,900 emails, including emails from former Administration officials and long-time friends that may not be deemed by the State Department to be federal records. And hundreds of these emails actually had already been forwarded onto the state.gov system and captured in real-time.

With respect to materials that the Select Committee has requested, the State Department has stated that just under 300 emails related to Libya were provided by the State Department to the Select Committee in response to a November 2014 letter, which contained a broader request for materials than prior requests from the House Oversight and Government Reform Committee.

Given Clinton's practice of emailing State Department officials on their state.gov addresses, the State Department already had, and had already provided, the Select Committee with emails from Clinton in August 2014 – prior to requesting and receiving printed copies of her emails.

The review process described above confirmed Clinton's practice of emailing State Department officials on their .gov address, with the vast majority of the printed copies of work-related emails Clinton provided to the State Department simply duplicating what was already captured in the State Department's record-keeping system in real time.

***Did Clinton use this account to communicate with foreign officials?***

During her time at State, she communicated with foreign officials in person, through correspondence, and by telephone. The review of all of her emails revealed only one email with a foreign (UK) official.

***Did she withhold any work emails? What about the 15 emails that Sid Blumenthal provided to the Select Committee that she did not provide to the State Department?***

She provided the State Department with all work and potentially work-related emails that she had, including all of her correspondence with Sid Blumenthal. We understand that Mr. Blumenthal had some emails that Clinton did not have, and Clinton had some emails that Mr. Blumenthal did not have, but it is important to note that none of those emails provide any new insights on the attack on our facilities in Benghazi.

***Do you think a third party should have been allowed to review what was turned over to the State Department, as well as the remainder that was not?***

The Federal Records Act puts the obligation on the government official, not the agency or a third party, to determine what is and is not a federal record. The State Department Foreign Affairs Manual outlines guidance "designed to help employees determine which of their e-mail messages must be preserved as federal records and which may be deleted without further authorization because they are not Federal record materials." [5 FAM 443.1(c)].



Clinton responded to the State Department's request by providing approximately 55,000 pages of her work and potentially work-related emails. She has also taken the unprecedented step of asking that those emails be made public. In doing so, she has sought to support the State Department's efforts, fulfill her responsibility of record-keeping, and provide the chance for the public to assess the work she and officials at the State Department did during her tenure.

After her work-related emails were identified and preserved, Clinton chose not to keep her private, personal emails that were not federal records, including emails about her daughter's wedding plans, her mother's funeral service, family vacations, etc.

Government officials are granted the privacy of their personal, non-work related emails, including personal emails on .gov accounts. Clinton exercised her privilege to ensure the continued privacy of her personal, non-work related emails.

***Can't she release the emails she provided to the State Department herself?***

Because the printed copies of work-related emails she provided to the State Department include federal records of the Department, the Department needs to review these emails before they can be made public. She called for them to be made available as soon as possible, and is glad to see the Department has begun releasing them.

***Some of the emails released show Clinton emailed aides at times on their personal, rather than .gov accounts. Was she trying to hide these communications?***

As Clinton has said before, it was her practice to email U.S. government officials on their .gov accounts if it was work-related. This is evidenced in the emails released so far. In reviewing her emails in 2014, there was a fraction of emails with work-related information sent to U.S. government officials' personal accounts, and those were provided to the State Department. The overwhelming majority of her work-related emails were to .gov accounts.

***Where was the server for her email located?***

The server for her email was physically located on her property, which is protected by U.S. Secret Service.

***What level of encryption was employed? Who was the service provider?***

The security and integrity of her family's electronic communications was taken seriously from the onset when it was first set up for President Clinton's team. While the curiosity about the specifics of this set up is understandable, given what people

with ill intentions can do with such information in this day and age, there are concerns about broadcasting specific technical details about past and current practices. Suffice it to say, 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.

***Was the server ever hacked?***

No, there is no evidence there was ever a breach.

***Was there ever an unauthorized intrusion into her email or did anyone else have access to it?***

No.

***What was done after her email was exposed in February 2013 after the hacker known as "Guccifer" hacked Sid Blumenthal's account?***

While this was not a breach of Clinton's account, because her email address was exposed, steps were taken at that time to ensure the security and integrity of her electronic communications, including changing her email address.

***Was the State Department able to respond to requests related to FOIA or Congressional requests before they received printed copies of her work-related emails?***

Yes. As the Select Committee has said, the State Department provided the Committee with relevant emails it already had on the state.gov system before the State Department requested any printed copies from former Secretaries, and four months before the State Department received the printed copies.

For example, in the well-publicized hack of Sid Blumenthal's email account, a note he sent Clinton on September 12, 2012, was posted online. At first blush, one might not think this exchange would be captured on the state.gov system. But in fact, Clinton forwarded the email, that very same day, onto the state.gov system. And the email was produced by the State Department to the Select Committee, and acknowledged by the Select Committee, in August 2014.

This example illustrates: 1) when an email from a non-".gov" sender had some connection to work or might add to the understanding of State Department officials, it was Clinton's practice to forward it to officials at their "state.gov" address; and 2) the State Department was able to search and produce Clinton's emails when needed long before, and unrelated to, receiving the printed copies as they were already captured on state.gov accounts.

# EXHIBIT E

RELEASE IN PART B5,B6

**From:** Koh, Harold Hongju <KohHH@state.gov>  
**Sent:** Saturday, December 12, 2009 12:31 PM  
**To:** Feltman, Jeffrey D; H  
**Subject:** RE: Guinea

That sounds like a good menu. We are seeing if there are other options and will get back to you

-----Original Message-----

**From:** Feltman, Jeffrey D  
**Sent:** Saturday, December 12, 2009 11:56 AM  
**To:** Koh, Harold Hongju; 'HDR22@clintonemail.com'  
**Subject:** Re: Guinea

Harold, we told the Moroccans they have a couple of options.

Other ideas welcome!  
Jeffrey Feltman

----- Original Message -----

**From:** Koh, Harold Hongju  
**To:** 'HDR22@clintonemail.com' <HDR22@clintonemail.com>; Feltman, Jeffrey D  
**Sent:** Sat Dec 12 10:45:37 2009  
**Subject:** Re: Guinea

Will happily do. The French Legal adviser Edwidge Belliard was very excited to meet you at lunch in DC a few months ago and I just saw her in the Hague on Wed. So Jeff--will stand by for your instructions Harold Harold Hongju Koh The Legal Adviser U.S. Department of State Suite 6421  
2201 C St. NW  
Washington, DC 20520-6421  
202 647 9598 office  
202 647 7096 fax

----- Original Message -----

**From:** H <HDR22@clintonemail.com>  
**To:** Feltman, Jeffrey D; Koh, Harold Hongju  
**Sent:** Sat Dec 12 10:32:03 2009

Subject: Guinea

Jeff/Harold--

I spoke w Kouchener who will be meeting in Paris tomorrow night w Moroccan FM Faris-Firri. I told him we had offered ideas to help them out of their current standoff re returning the passport.

Jeff, can you call your French counterpart to explain and connect w Harold if we need L to contact the French legal advisor? Thanks-iand let me know what unfolds. Hillary

RELEASE IN PART  
B6

---

**From:** Koh, Harold Hongju <KohHH@state.gov>  
**Sent:** Sunday, September 30, 2012 10:53 PM  
**To:** H  
**Subject:** Re: OMAR KHADR: Omar Khadr is going home to Canada from Guantánamo

So glad we got this done. After spending the last 10 years on GTMO, at least this young man finally has another chance.

---

**From:** H [mailto:HDR22@clintonemail.com]  
**Sent:** Sunday, September 30, 2012 09:41 PM  
**To:** Koh, Harold Hongju  
**Subject:** Re: OMAR KHADR: Omar Khadr is going home to Canada from Guantánamo

And, thank you for all you did to get this resolved.

---

**From:** Koh, Harold Hongju [mailto:KohHH@state.gov]  
**Sent:** Saturday, September 29, 2012 08:47 AM  
**To:** Sullivan, Jacob J <SullivanJJ@state.gov>; H; Mills, Cheryl D <MillsCD@state.gov>  
**Subject:** Fw: OMAR KHADR: Omar Khadr is going home to Canada from Guantánamo

Hooray! Thanks for the call to FM Baird!

---

**From:** Fried, Daniel  
**Sent:** Saturday, September 29, 2012 08:46 AM  
**To:** Koh, Harold Hongju; Conklin, Maeqan L; Gahan, Kimberly A; Bridgeman, Theresa; Perina, Alexandra H; McLeod, Mary; ringber [redacted] <ringber [redacted]>  
**Subject:** Re: OMAR KHADR: Omar Khadr is going home to Canada from Guantánamo

B6

Good work all around.

---

**From:** Koh, Harold Hongju  
**Sent:** Saturday, September 29, 2012 08:43 AM  
**To:** Conklin, Maeqan L; Gahan, Kimberly A; Bridgeman, Theresa; Perina, Alexandra H; McLeod, Mary; 'ringber [redacted] <ringber [redacted]> Fried, Daniel  
**Subject:** Fw: OMAR KHADR: Omar Khadr is going home to Canada from Guantánamo

Gtmo is 1 down!! Yayy!

---

**From:** Alan.Kessel [redacted]  
**Sent:** Saturday, September 29, 2012 08:40 AM  
**To:** Koh, Harold Hongju  
**Subject:** Fw: OMAR KHADR: Omar Khadr is going home to Canada from Guantánamo

Alan H. Kessel  
The Legal Adviser/  
Le Jurisconsulte (JFM)  
Department of Foreign Affairs and International Trade/  
Ministère des Affaires étrangères et du Commerce international  
125 Sussex Drive  
Ottawa, Ontario K1A 0G2



Canada

e-mail: alan.kessel

B6

---

**From:** Media Monitoring / Surveillance Médias (BCM)  
**Sent:** Saturday, September 29, 2012 07:11 AM  
**Subject:** OMAR KHADR: Omar Khadr is going home to Canada from Guantánamo

## Omar Khadr is going home to Canada from Guantánamo;

The Toronto-born man who got to Guantánamo as a teenager was en route to more prison time in his native Canada as of 4:30 a.m. Saturday under a 2010 plea deal, a U.S. military source tells The Miami Herald

By CAROL ROSENBERG, crosenberg@miamiherald.com, 29 September 2012, The Miami Herald  
<http://www.miamiherald.com/2012/09/29/3025662/omar-khadr-is-going-home-to-canada.html>

The United States sent Guantánamo's youngest captive home to a prison in his native Canada early Saturday morning, according to a U.S. military source, ending the decade-long detention of the young Muslim militant who grew from a teenager into adulthood at the Pentagon's prison camps in Cuba.

Omar Khadr, 26, born in Toronto, pleaded guilty to war crimes charges in 2010 in exchange for an eight-year sentence. Under the deal, he was to serve all but a year of it in Canada, where he will be eligible for early release because he was a juvenile, just 15, when he committed his crimes in war-torn Afghanistan.

But the Obama administration was slow to sign off on his transfer and the Canadian government was even slower to design a plan to hold him at home.

Saturday, a military source told The Miami Herald that Khadr was en route to his native Canada as of 4:30 a.m., a secret transfer under way just days after Khadr passed his 26th birthday with a visit from a Canadian diplomat behind the prison's barbed wire. It was not immediately known where he'd be imprisoned but defense lawyers had asked that he get special protections at the federal Canadian lockup because of his notoriety.

U.S. troops captured Khadr, who was near death, in a July 27, 2002 firefight at a suspected al Qaida compound near Khost, Afghanistan.

U.S. air strikes had leveled the compound and as a Special Forces unit assaulted, Khadr admitted in his guilty plea, he hurled a grenade from inside the rubble that mortally wounded Army Sgt. 1st Class Christopher Speer, 28. Medics were able to save Khadr's life, and turned him over to what became a decade of on-again off-again interrogation.

The case of Khadr — Guantánamo's last Western captive — was a source of international debate.

Because he was captured at such a young age, just months into the U.S. invasion of Afghanistan, some called him a child soldier deserving of rehabilitation not interrogation. Psychiatrist Michael Welner, testifying at the Guantánamo war court for the prosecution and paid by the Pentagon, called Khadr a continuing danger and that, while in the U.S. prison camps in Cuba, Khadr was "marinating in a community of hardened and belligerent radical Islamists."

Khadr's lawyers countered with a Canadian-style college preparatory curriculum. While Khadr served his sentence in Guantánamo's cellblock for convicted war criminals, he filled his time with remedial studies designed by a Canadian college professor — literature, physics and videos of "Little Mosque on the Prairie," a popular Canadian TV show about a Muslim community in a fictional prairie town. He also read Shakespeare with his U.S. Army defense lawyer, a tall lieutenant colonel who read Juliet to Khadr's Romeo.



Under the terms of his plea agreement, Khadr admitted to planting landmines in Afghanistan meant to shred invading allied forces. Once captured, and interrogated, he directed U.S. troops back to their location to safely disarm them.

Testimony at pre-trial hearings showed U.S. interrogators saw the 15-year-old as a human intelligence treasure trove because as a child his family had spent time with the family of Osama bin Laden in Afghanistan. His father, killed in Pakistan in 2003, was seen in Canada as a high-level al Qaida functionary who moved his family to Pakistan and Afghanistan in the years before the Sept. 11, 2001, attacks.

One of Omar Khadr's elder brothers, Abdurahman, also spent a short time in Guantánamo as an informant but never saw his kid brother there. Abdurahman is now free in Toronto. With Saturday's transfer, the Pentagon was holding 166 detainees at Guantánamo.

The youngest is now believed to be a Yemeni named Hassan bin Attash, whose leaked detention records indicate he was born in Yemen in 1985. He's the younger brother of former CIA captive Walid bin Attash, an alleged al Qaida lieutenant now at Guantánamo facing war crimes charges in the five-man Sept. 11 death penalty trial.

The Khadr transfer could break a logjam in efforts to get other captives to plead guilty. Defense lawyers have characterized the Obama administration's inability to get Khadr back to Canada as an obstacle to negotiations with other alleged al Qaida foot soldiers whose testimony might be useful at the Guantánamo war court.

The Miami Herald

---

**Not for redistribution outside DFAIT / Document à distribution au sein de MAECI seulement.**

Contact **Media Monitoring / Surveillance des médias (BCM)** for distribution list adjustments or other requests.

Veuillez contacter **Media Monitoring / Surveillance des médias (BCM)** pour tout ajustement aux listes de distribution ou autres requêtes.

---

**Robin Dumont**

***Surveillant des médias / Media Monitor***

Bureau des relations avec les médias / Media Relations Office

Tel.: (613) 944-1284

Fax: (613) 995-1405



Before printing think about our Environment. Avant l'impression, il faut penser à notre Environnement



RELEASE IN  
FULL

---

**From:** Kennedy, Patrick F <KennedyPF@state.gov>  
**Sent:** Friday, February 25, 2011 9:53 AM  
**To:** H  
**Subject:** RE: Pls let me know as soon as possible when the last American has left Tripoli. Thx

Madame Secretary

We have Bill Burns and Jeff Feltman reaching out

Have provide talking points to Mike Morell to make call and for him to get Steve Kappas to do so as well

Regards

pat

---

**From:** H [mailto:HDR22@clintonemail.com]  
**Sent:** Friday, February 25, 2011 8:47 AM  
**To:** Kennedy, Patrick F  
**Subject:** Re: Pls let me know as soon as possible when the last American has left Tripoli. Thx

Will they let our plane land? How can we insure that?

---

**From:** Kennedy, Patrick F [mailto:KennedyPF@state.gov]  
**Sent:** Friday, February 25, 2011 08:41 AM  
**To:** H; Mills, Cheryl D <MillsCD@state.gov>  
**Subject:** RE: Pls let me know as soon as possible when the last American has left Tripoli. Thx

Madame Secretary

Will do

Ferry has sailed

Last official staff at Mitiga Military Airport  
Our charter flite has departed from Istanbul  
There was some small arms fire near Mitiga and now Libyans want us to move everyone to civilian airport miles away  
RSO says that is not best solution

We have pushing back at all levels

Will keep you advised

Regards

pat

---

**From:** H [mailto:HDR22@clintonemail.com]  
**Sent:** Friday, February 25, 2011 8:18 AM

**To:** Kennedy, Patrick F; Mills, Cheryl D

**Subject:** Pls let me know as soon as possible when the last American has left Tripoli. Thx

RELEASE IN FULL

---

**From:** Kennedy, Patrick F <KennedyPF@state.gov>  
**Sent:** Monday, December 12, 2011 7:14 AM  
**To:** H; Nides, Thomas R; Sullivan, Jacob J  
**Subject:** Re: Iraq travel warning

Madame Secretary

Do not know what he means

Reaching out now to both london and baghdad urgently

Back to you soonest

Regards

Pat

----- Original Message -----

**From:** H [mailto:HDR22@clintonemail.com]  
**Sent:** Sunday, December 11, 2011 10:07 PM  
**To:** Kennedy, Patrick F; Nides, Thomas R; Sullivan, Jacob J  
**Subject:** Re: Iraq travel warning

I understand, but when he raised it he had been told that it did not "apply" to business. When I explained that it applied to everyone but that businesses were better able to protect themselves, he said the Japanese and British had better standards for their businesses. Jim Jeffrey and I promised to look into that. Do you know what he means?

----- Original Message -----

**From:** Kennedy, Patrick F [mailto:KennedyPF@state.gov]  
**Sent:** Sunday, December 11, 2011 09:17 PM  
**To:** H; Nides, Thomas R <NidesTR@state.gov>; Sullivan, Jacob J <SullivanJJ@state.gov>  
**Subject:** Re: Iraq travel warning

Madame Secretary

The Travel Warning applies to all American citizens

But we work, thru Diplomatic Security's Overseas Security Advisory Committee, to the security officers of companies.

These security professionals understand how to mitigate risks, which the average American traveller would not be able to do

Regards

Pat

----- Original Message -----

**From:** H [mailto:HDR22@clintonemail.com]  
**Sent:** Sunday, December 11, 2011 08:36 PM

To: Kennedy, Patrick F; Nides, Thomas R; Sullivan, Jacob J  
Subject: Iraq travel warning

PM just asked me if the travel warning applied to companies because if so, they would be hard to recruit tomorrow.



RELEASE IN  
PART B5

---

**From:** Burns, William J <BurnsWJ@state.gov>  
**Sent:** Saturday, May 26, 2012 8:22 AM  
**To:** H; Sherman, Wendy R  
**Cc:** Sullivan, Jacob J  
**Subject:** Re: Update

Glad to join at 10. Will let Ops know.

----- Original Message -----

From: H [mailto:HDR22@clintonemail.com]  
Sent: Saturday, May 26, 2012 08:19 AM  
To: Sherman, Wendy R  
Cc: Burns, William J; Sullivan, Jacob J  
Subject: Re: Update

Ok. Let's do at 10am today. I will call into ops and ask that they connect you--and if others wish to join, pls advise ops.  
Thx.

----- Original Message -----

From: Sherman, Wendy R [mailto:ShermanWR@state.gov]  
Sent: Saturday, May 26, 2012 08:08 AM  
To: H  
Cc: Burns, William J <BurnsWJ@state.gov>; Sullivan, Jacob J <SullivanJJ@state.gov>  
Subject: Re: Update

All of them work. I will call ops and tell them to work out what is best for you.

----- Original Message -----

From: H [mailto:HDR22@clintonemail.com]  
Sent: Saturday, May 26, 2012 07:54 AM  
To: Sherman, Wendy R  
Cc: Burns, William J; Sullivan, Jacob J  
Subject: Re: Update

Wendy--I would like to talk secure. Best times for me are this morning or tomorrow morning btw 8-9:30am. Or this afternoon btw 1-3pm. Do those windows work for you? If so, what's best?

----- Original Message -----

From: Sherman, Wendy R [mailto:ShermanWR@state.gov]  
Sent: Saturday, May 26, 2012 07:25 AM  
To: H  
Cc: Burns, William J <BurnsWJ@state.gov>; Sullivan, Jacob J <SullivanJJ@state.gov>  
Subject: Update

Madam Secretary,

Just back at Dulles after excellent meetings in Tel Aviv following Baghdad meetings. Will get points to you through S-EX  
[redacted] but happy to talk with you by phone, probably secure, any time this weekend if  
you'd like update.

Best,

Wendy

# EXHIBIT F



# 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

~~SENSITIVE BUT UNCLASSIFIED~~

## OBJECTIVES AND METHODOLOGY

---

In April 2015, the Office of Inspector General (OIG) initiated an evaluation to address concerns identified during recent audits and inspections<sup>1</sup> 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<sup>2</sup> 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.<sup>3</sup> 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*.<sup>4</sup> 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

---

<sup>1</sup> 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).

<sup>2</sup> 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.

<sup>3</sup> 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.

<sup>4</sup> Government Accountability Office (GAO), *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014).

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

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.<sup>5</sup> 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."<sup>6</sup>

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.<sup>7</sup> 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.<sup>8</sup>

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.<sup>9</sup> 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

---

<sup>5</sup> 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.

<sup>6</sup> 5 U.S.C. § 552(f)(2)(A).

<sup>7</sup> 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).

<sup>8</sup> 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.

<sup>9</sup> 5 U.S.C. § 552(a)(6)(A). This includes a determination that no responsive records exist.

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

production of any agency records the requester believes the agency improperly withheld.<sup>10</sup> In addition, a requester who receives no response within 20 days has a right to file a complaint in district court immediately.<sup>11</sup>

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.<sup>12</sup> 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.<sup>13</sup> The Assistant Secretary for Administration reports to the Under Secretary for Management.<sup>14</sup>

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.<sup>15</sup> The Department's FOIA regulations specify that FOIA requests be sent to IPS.<sup>16</sup> 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.<sup>17</sup>

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

---

<sup>10</sup> 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).

<sup>11</sup> 5 U.S.C. § 552 (a)(6)(C)(i).

<sup>12</sup> 1 FAM 214.2.

<sup>13</sup> 1 FAM 211.2(ee). Executive Order 13392 requires the designation of a Chief FOIA Officer.

<sup>14</sup> 1 FAM 211.2(a)

<sup>15</sup> U.S. Department of State, *FOIA Guidance For State Department Employees* (2010), at 3.

<sup>16</sup> 22 C.F.R. § 171.5(a).

<sup>17</sup> 22 C.F.R. § 171.5(c).

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

(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.<sup>18</sup>

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.<sup>19</sup> 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.<sup>20</sup>

---

<sup>18</sup> *FOIA Guidance For State Department Employees*, at 8.

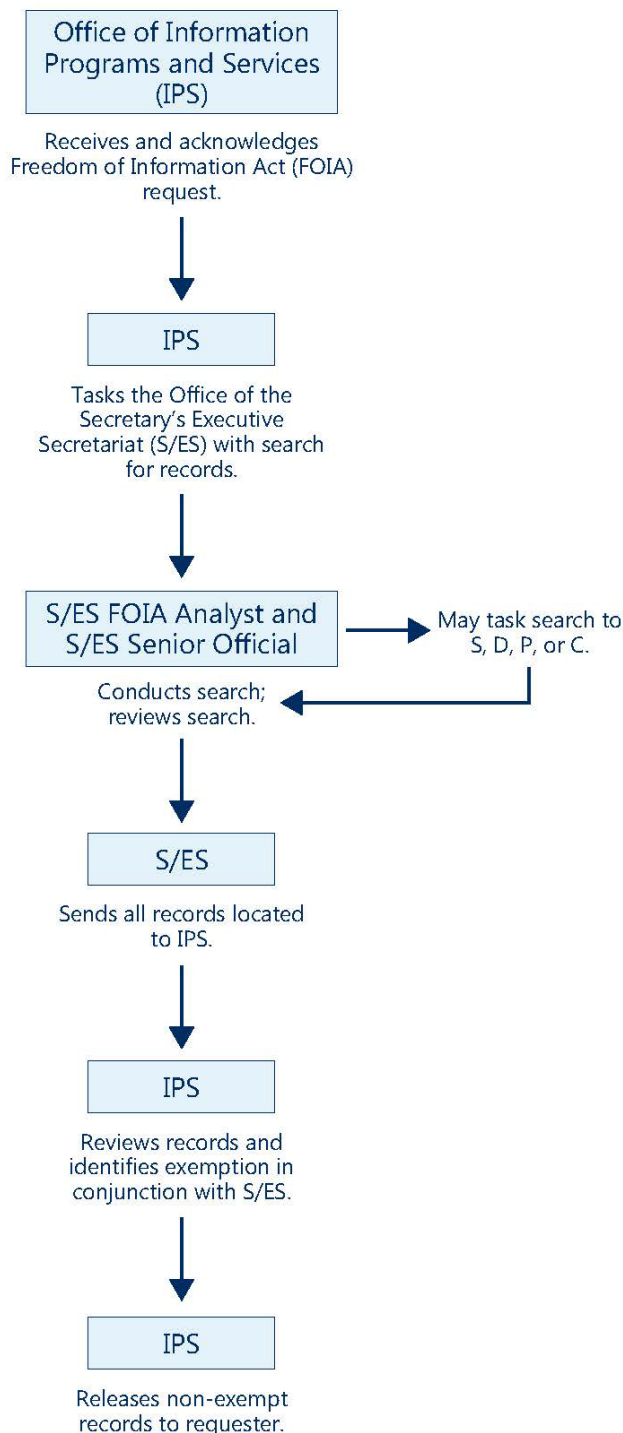
<sup>19</sup> Certain offices, including the Bureau of Diplomatic Security and the Office of Medical Services, are referred to as "decentralized offices" and review their own documents for exemptions. However, these offices must still forward a copy of their response to the request to IPS.

<sup>20</sup> 22 C.F.R. § 171.52.

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

**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.<sup>21</sup> S/ES employs one FOIA Analyst, who reports to the GS-14 Deputy Director of Correspondence, Records, & Staffing (Deputy Director).<sup>22</sup> 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.

<sup>21</sup> 1 FAM 022.2.

<sup>22</sup> A second S/ES employee occasionally assists with FOIA searches in addition to his regular duties.

~~SENSITIVE BUT UNCLASSIFIED~~



~~SENSITIVE BUT UNCLASSIFIED~~

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,<sup>23</sup> 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.<sup>24</sup> 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.<sup>25</sup>

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

---

<sup>23</sup> 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).

<sup>24</sup> U.S. Department of Justice, *Summary of Annual FOIA Reports For Fiscal Year 2014*, pp. 12–14.

<sup>25</sup> 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.

~~SENSITIVE BUT UNCLASSIFIED~~



~~SENSITIVE BUT UNCLASSIFIED~~

four Secretaries of State.<sup>26</sup> 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.

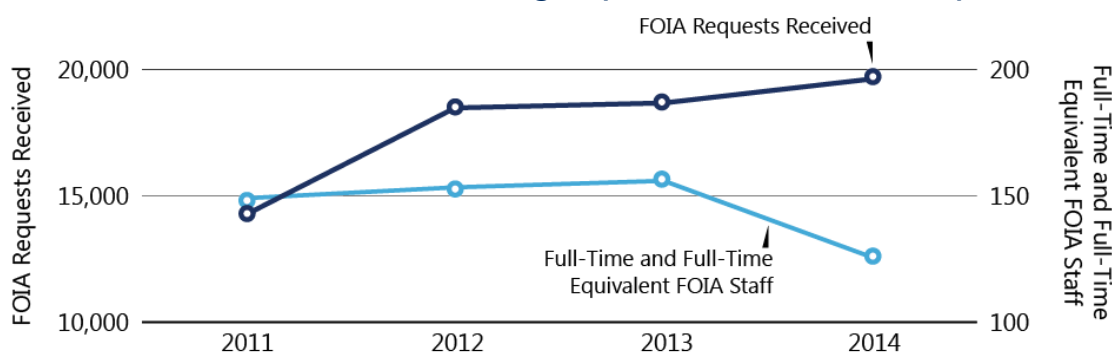
**Table 1: Processing Time for FOIA Requests Related to Recent Secretaries of State**

Secretary	Requests Completed Within Listed Times				Still Pending	Total Number of FOIA Requests
	Up to 20 Days	21–100 Days	101–500 Days	500+ Days		
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
<b>Total</b>	<b>14</b>	<b>28</b>	<b>77</b>	<b>55</b>	<b>243</b>	<b>417</b>

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.<sup>27</sup> 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.

<sup>26</sup> 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.

<sup>27</sup> 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).

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

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.<sup>28</sup>

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."<sup>29</sup> 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.<sup>30</sup> 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.<sup>31</sup>

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).<sup>32</sup> None

---

<sup>28</sup> The Department anticipates completing the court-ordered production in January 2016.

<sup>29</sup> *Weisberg v. U.S. Dep't of Justice*, 705 F.2d 1344, 1351 (D.C.Cir. 1983).

<sup>30</sup> 5 U.S.C. § 552(a)(3)(C)).

<sup>31</sup> *FOIA Guidance For State Department Employees*, at 8.

<sup>32</sup> 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

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

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.<sup>33</sup> 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.<sup>34</sup> S/ES-IRM reported to OIG that it has maintained files numbering in the thousands for selected senior officials<sup>35</sup> dating back at least as far as Secretary Powell's tenure, though OIG has determined that many of these are not easily accessible.<sup>36</sup> Moreover, as the Deputy Director noted, searching these files is difficult because searches are limited to those that can be undertaken using Microsoft Outlook.<sup>37</sup>

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).<sup>38</sup> 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.

<sup>33</sup> OIG did not evaluate the practices used by S, D, P, and C.

<sup>34</sup> 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.

<sup>35</sup> S/ES-IRM does not maintain an index or inventory of these files.

<sup>36</sup> In 2015, the Department began permanently retaining the emails of 102 senior officials.

<sup>37</sup> S/ES has begun testing software intended to enhance its ability to search and retrieve email records.

<sup>38</sup> 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).

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

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.<sup>39</sup> 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.<sup>40</sup>

## 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.<sup>41</sup> 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.<sup>42</sup> 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.<sup>43</sup> OIG's past and current

---

<sup>39</sup> 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.

<sup>40</sup> 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.

<sup>41</sup> OIG, *Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services* (ISP-I-12-54, September 2012).

<sup>42</sup> Center for Effective Government, *Making the Grade: Access to Information Scorecard 2015* (March 2015).

<sup>43</sup> GAO-14-704G, §§ 1.02 to 1.05.

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

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.<sup>44</sup> 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.<sup>45</sup> 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.<sup>46</sup> 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.<sup>47</sup> 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."<sup>48</sup>

***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.<sup>49</sup> Nonetheless, standards emphasize that monitoring should include regular management and supervisory

---

<sup>44</sup> U.S. Department of State Press Statement, *Transparency Coordinator* (Sept. 8, 2015), available at <http://www.state.gov/secretary/remarks/2015/09/246691.htm>.

<sup>45</sup> GAO-14-704G.

<sup>46</sup> See, e.g., GAO, *Social Security Disability: Management Controls Needed to Strengthen Demonstration Projects* (GAO-08-1053, September 2008).

<sup>47</sup> 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).

<sup>48</sup> DOE, Office of Inspector General, *Department's Freedom of Information Act Request Process* (OAS-SR-10-03, Sept. 2010).

<sup>49</sup> 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).

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

activities, comparisons, reconciliations, and other routine actions.<sup>50</sup> 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.<sup>51</sup> 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<sup>52</sup> 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,<sup>53</sup> and Department guidance specifically requires IPS to ensure that responses are timely, accurate, and complete.<sup>54</sup> 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

---

<sup>50</sup> GAO-14-704G, at §§ 16.04, 16.05.

<sup>51</sup> The Department agreed with these recommendations but has yet to take action.

<sup>52</sup> The performance standards for the current Director of Secretariat Staff were not yet available for review at the close of OIG's work.

<sup>53</sup> 1 FAM 214.2.

<sup>54</sup> U.S. Department of State, *FOIA Guidance For State Department Employees* (2010).

~~SENSITIVE BUT UNCLASSIFIED~~



~~SENSITIVE BUT UNCLASSIFIED~~

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.<sup>55</sup> 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.<sup>56</sup>

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.<sup>57</sup> 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.<sup>58</sup> The Department and its leadership could also be subject to contempt citations if they were found to

---

<sup>55</sup> According to S/ES, the FOIA Analyst also attended workshops at the Department of Justice.

<sup>56</sup> 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.

<sup>57</sup> GAO-14-704G, at §§ 17.01, 17.05.

<sup>58</sup> 5 U.S.C. § 552(a)(4)(E).

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

have violated rules requiring candor to the court.<sup>59</sup> 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.<sup>60</sup>

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.<sup>61</sup> 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."<sup>62</sup> On May 10, 2013, IPS replied to CREW, stating that "no records responsive to your request were located."<sup>63</sup> At the time the request was

<sup>59</sup> 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.

<sup>60</sup> 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).

<sup>61</sup> *The Associated Press v. U.S. Dept. of State*, Civil Action No. 1:15-cv-00345-RJL (D.D.C.).

<sup>62</sup> 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."

<sup>63</sup> The response also noted:

~~SENSITIVE BUT UNCLASSIFIED~~



~~SENSITIVE BUT UNCLASSIFIED~~

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.<sup>64</sup> Furthermore, it does not appear that S/ES searched any email records, even though the request clearly encompassed emails.<sup>65</sup>

- 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.

<sup>64</sup> 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.

<sup>65</sup> 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.

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

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.

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

**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.

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

## 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

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

-2-

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.

UNCLASSIFIED~~SENSITIVE BUT UNCLASSIFIED~~



~~SENSITIVE BUT UNCLASSIFIED~~


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 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

UNCLASSIFIED~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~UNCLASSIFIED

- 2 -

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~~SENSITIVE BUT UNCLASSIFIED~~



~~SENSITIVE BUT UNCLASSIFIED~~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 21<sup>st</sup> 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

~~SENSITIVE BUT UNCLASSIFIED~~



~~SENSITIVE BUT UNCLASSIFIED~~

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.

~~SENSITIVE BUT UNCLASSIFIED~~

## 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	<i>Foreign Affairs Manual</i>
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

~~SENSITIVE BUT UNCLASSIFIED~~



# HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926

[OIG.state.gov/HOTLINE](http://OIG.state.gov/HOTLINE)

If you fear reprisal, contact the  
OIG Whistleblower Ombudsman to learn more about your rights:

[OIGWPEAOmbuds@state.gov](mailto:OIGWPEAOmbuds@state.gov)

[oig.state.gov](http://oig.state.gov)

Office of Inspector General • U.S. Department of State • P.O. Box 9778 • Arlington, VA 22219

~~SENSITIVE BUT UNCLASSIFIED~~

# EXHIBIT G

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

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.

\_\_\_\_\_  
Office of Inspector General  
U.S. Department of State • Broadcasting Board of Governors

UNCLASSIFIED



# OIG

## HIGHLIGHTS

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

## 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

UNCLASSIFIED



## OBJECTIVES AND METHODOLOGY

---

In April 2015, the Office of Inspector General (OIG) initiated an evaluation to address concerns identified during recent audits and inspections<sup>1</sup> 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<sup>2</sup> 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,<sup>3</sup> 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<sup>4</sup> and the Federal Information Security Management Act (FISMA)<sup>5</sup> 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

---

<sup>1</sup> 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).

<sup>2</sup> 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.

<sup>3</sup> 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).

<sup>4</sup> 44 U.S.C. chapters 21, 29, 31, and 33.

<sup>5</sup> 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).

UNCLASSIFIED

Department directives issued in the *Foreign Affairs Manual* (FAM) and the *Foreign Affairs Handbook* (FAH);<sup>6</sup> 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.<sup>7</sup>

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

---

<sup>6</sup> 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).

<sup>7</sup> 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.

UNCLASSIFIED

information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities."<sup>8</sup> 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.<sup>9</sup>

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.<sup>10</sup> 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."<sup>11</sup> Secretary Powell's representative advised the Department in 2015 that he did not retain those emails or make printed copies.<sup>12</sup> 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.<sup>13</sup>

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.<sup>14</sup>

---

<sup>8</sup> 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).

<sup>9</sup> GAO, *National Archives and Records Administration: Oversight and Management Improvements Initiated, but More Action Needed* (GAO-11-15, October 5, 2010).

<sup>10</sup> 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].

<sup>11</sup> Colin Powell, *It Worked For Me: In Life and Leadership* 109 (2012).

<sup>12</sup> Grafeld Letter. Secretary Powell did not provide his emails to the Department in any form.

<sup>13</sup> 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>.

<sup>14</sup> 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.

UNCLASSIFIED

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.<sup>15</sup>

## 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."<sup>16</sup> 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."<sup>17</sup>

NARA promulgates regulations providing guidance to agencies on implementation of the Federal Records Act and recordkeeping obligations more generally.<sup>18</sup> 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."<sup>19</sup> 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."<sup>20</sup> 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.

---

<sup>15</sup> Letter from Cheryl Mills, cd Mills Group, to Patrick F. Kennedy, Under Secretary of State for Management (December 5, 2014).

<sup>16</sup> 44 U.S.C. § 3101.

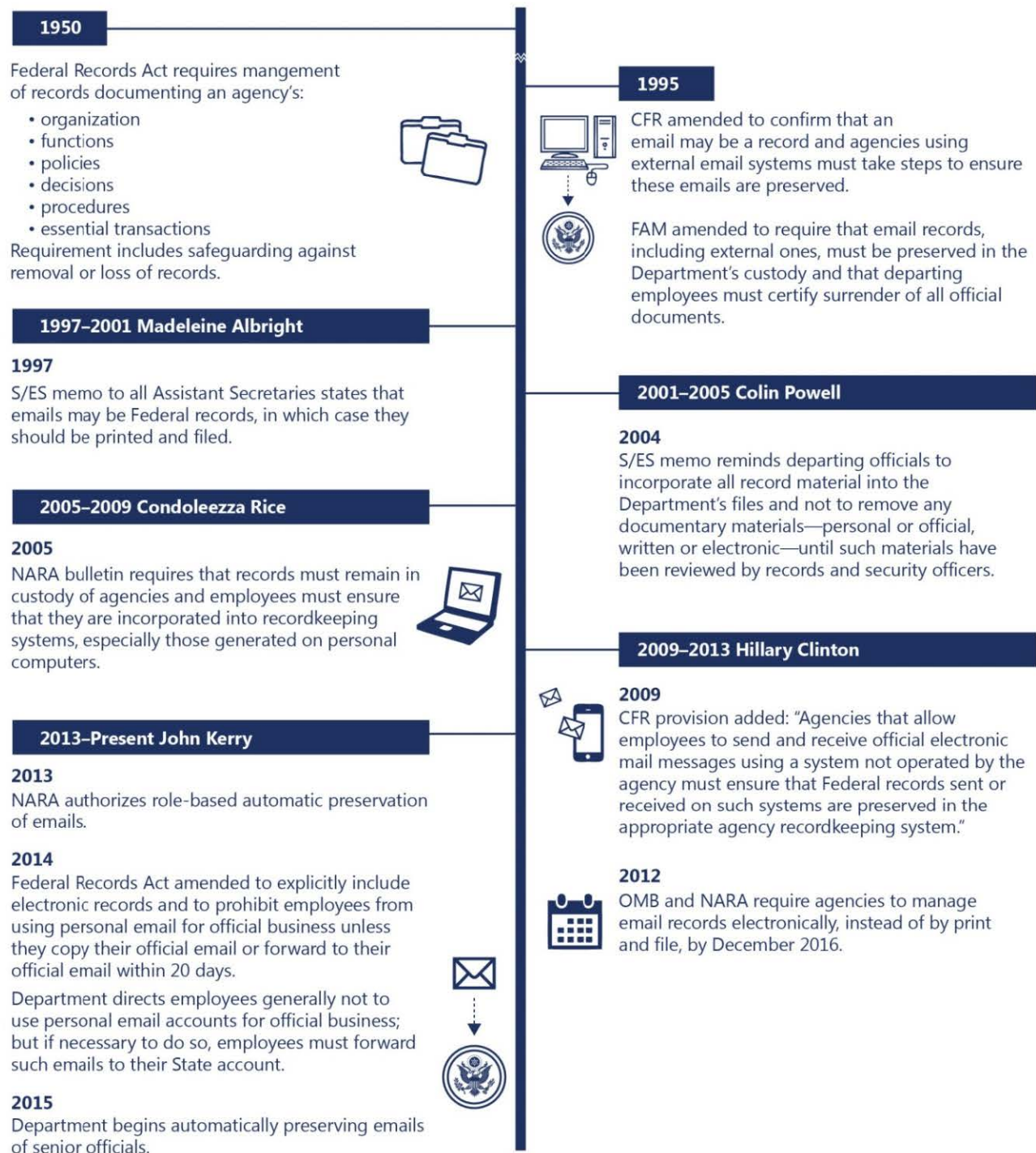
<sup>17</sup> H.R. 2943, Records Disposal Act of 1943, 57 Stat. 380 (July 7, 1943).

<sup>18</sup> 44 U.S.C. § 2904.

<sup>19</sup> 36 C.F.R. § 1222.12(b)(2) (1990).

<sup>20</sup> 36 C.F.R. § 1222.12(b)(3) (1990).

UNCLASSIFIED

**Figure 1: Timeline of Selected Records Management Requirements and Policies**

Source: OIG analysis of laws and policies.



UNCLASSIFIED

**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.”<sup>21</sup> 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.”<sup>22</sup> A recordkeeping system is a manual or electronic system that captures, organizes, and categorizes records to facilitate their preservation, retrieval, use, and disposition.<sup>23</sup> 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.<sup>24</sup>

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.<sup>25</sup> 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.”<sup>26</sup> 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.”<sup>27</sup>

**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.”<sup>28</sup> These recordkeeping requirements include identifying specific categories of records to be maintained

---

<sup>21</sup> 36 C.F.R. § 1222.34(e) (1995).

<sup>22</sup> 36 C.F.R. § 1222.24(a)(4) (1995).

<sup>23</sup> 36 C.F.R. § 1220.18 (2009).

<sup>24</sup> 5 FAM 443.1(c) (October 30, 1995).

<sup>25</sup> 5 FAM 443.2(d) (October 30, 1995).

<sup>26</sup> *See, e.g.*, 09 STATE 120561; Department of State, Records Management Responsibilities, Announcement No. 2009\_11\_125, November 23, 2009.

<sup>27</sup> 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)).

<sup>28</sup> 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.<sup>29</sup>

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.<sup>30</sup> 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.<sup>31</sup> However, according to the Department, its technology has "lagged behind" this mandate.

<sup>29</sup> 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.").

<sup>30</sup> 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.

<sup>31</sup> 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.

UNCLASSIFIED

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.<sup>32</sup> 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.<sup>33</sup> 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."<sup>34</sup> 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.<sup>35</sup> 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.

<sup>32</sup> 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).

<sup>33</sup> 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).

<sup>34</sup> 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>.

<sup>35</sup> 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).



UNCLASSIFIED

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.<sup>36</sup>

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.<sup>37</sup> Shortly before the enactment of the 2014 amendments, the Department issued an interim directive with similar requirements<sup>38</sup> 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.<sup>39</sup>

---

<sup>36</sup> 36 C.F.R. § 1236.22(b).

<sup>37</sup> 44 U.S.C. § 2911(a).

<sup>38</sup> 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.

<sup>39</sup> 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.<sup>40</sup> 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.<sup>41</sup>

NARA regulations require each agency to have procedures to ensure that departing officials and employees do not remove Federal records from agency custody.<sup>42</sup> 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.<sup>43</sup> 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.

<sup>40</sup> 44 U.S.C. § 3105.

<sup>41</sup> 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.

<sup>42</sup> 36 C.F.R. § 1222.24(a)(6) (October 2, 2009).

<sup>43</sup> 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).

UNCLASSIFIED

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."<sup>44</sup> Numerous Department cables and announcements have emphasized the responsibility of every employee to sign a separation statement before she or he departs.<sup>45</sup>

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.<sup>46</sup> 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.<sup>47</sup> 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.

---

<sup>44</sup> 5 FAM 417.2 (March 16, 1982); 5 FAM 413.9 (October 30, 1995); 5 FAM 414.7 (September 17, 2004).

<sup>45</sup> 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).

<sup>46</sup> 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.

<sup>47</sup> 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.<sup>48</sup> According to NARA, an effective records disposition program depends on scheduling<sup>49</sup> all records, regardless of location and regardless of physical form or characteristics (paper or electronic).<sup>50</sup> 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.<sup>51</sup>

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.<sup>52</sup> 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.<sup>53</sup>

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).<sup>54</sup> The Under Secretary for Management<sup>55</sup>

---

<sup>48</sup> 44 U.S.C. §§ 3101, 3102.

<sup>49</sup> 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.

<sup>50</sup> See <http://www.archives.gov/records-mgmt/publications/disposition-of-federal-records/chapter-2.html>

<sup>51</sup> 36 C.F.R. § 1222.34.

<sup>52</sup> GAO, *Information Management: The Challenges of Managing Electronic Records* (GAO-10-838T, July 17, 2010).

<sup>53</sup> NARA, *Records Management Self-Assessment 2014* (November 6, 2015).

<sup>54</sup> 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.

<sup>55</sup> 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

UNCLASSIFIED

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.<sup>56</sup>

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."<sup>57</sup> 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).

<sup>56</sup> ERMWG, *Action Memo for Under Secretary Kennedy: Preserving Electronically Senior Officials' Record Email Messages* (August 22, 2014).

<sup>57</sup> 5 FAM 414.3 (June 9, 2009).

regulations,”<sup>58</sup> 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,<sup>59</sup> 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.<sup>60</sup>

---

<sup>58</sup> 5 FAM 414.2 (June 9, 2009).

<sup>59</sup> 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).

<sup>60</sup> 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*



UNCLASSIFIED

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.<sup>61</sup> 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.<sup>62</sup> 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.<sup>63</sup>

**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.<sup>64</sup> 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.

<sup>61</sup> 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).

<sup>62</sup> The term ".pst" refers to the format used to store copies of email messages, calendar events, and other items within Microsoft software.

<sup>63</sup> 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.

<sup>64</sup> 5 FAM 433 (July 31, 2012).

UNCLASSIFIED

UNCLASSIFIED

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.<sup>65</sup> 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.<sup>66</sup> 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.<sup>67</sup> 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.<sup>68</sup> 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.<sup>69</sup>

**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

---

<sup>65</sup> The schedule for records specific to the Office of the Secretary is available at: [https://foia.state.gov/\\_docs/RecordsDisposition/A-01.pdf](https://foia.state.gov/_docs/RecordsDisposition/A-01.pdf)

<sup>66</sup> 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).

<sup>67</sup> 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.

<sup>68</sup> Under Secretary Patrick F. Kennedy, *Memorandum: Senior Officials' Records Management Responsibilities* (August 28, 2014).

<sup>69</sup> See, e.g., Department of State, *Senior Agency Official for Records Management FY 2014 Annual Report Template* (February 5, 2015).

UNCLASSIFIED



UNCLASSIFIED

not remove Federal records from agency custody.<sup>70</sup> 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.<sup>71</sup> 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.<sup>72</sup> 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.<sup>73</sup> 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.<sup>74</sup> The Department also did not promptly notify NARA about the potential loss of records.<sup>75</sup> NARA officials told OIG they learned of former

---

<sup>70</sup> 36 C.F.R. § 1222.24 (2009).

<sup>71</sup> 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.

<sup>72</sup> 5 FAH-4 H-217.2 (August 13, 2008).

<sup>73</sup> 44 U.S.C. § 3106; 36 C.F.R. § 1230.14.

<sup>74</sup> 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.”

<sup>75</sup> 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

UNCLASSIFIED

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.<sup>76</sup>

In April 2015, the Department informed NARA of the information it obtained from the former Secretaries concerning their email records.<sup>77</sup> NARA subsequently requested additional information about how the Department implements records management requirements with regard to senior officials.<sup>78</sup> 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.<sup>79</sup>

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.<sup>80</sup> 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.

<sup>76</sup> 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).

<sup>77</sup> Grafeld Letter.

<sup>78</sup> 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).

<sup>79</sup> 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.

<sup>80</sup> 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.<sup>81</sup>

## 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 through 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

---

<sup>81</sup> 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.

UNCLASSIFIED

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.<sup>82</sup> 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."<sup>83</sup> These responses suggest staff may not have consistently complied with the preservation requirement to print and file emails containing Federal records.<sup>84</sup>

<sup>82</sup> 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.

<sup>83</sup> 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.

<sup>84</sup> 5 FAM 443.3 (October 30, 1995).

UNCLASSIFIED

**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 ....<sup>85</sup>

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."<sup>86</sup> 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.<sup>87</sup> 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.<sup>88</sup> Moreover, in keeping with NARA regulations,<sup>89</sup> 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.<sup>90</sup> Therefore, Secretary Powell should have preserved any Federal records he

<sup>85</sup> Colin Powell, *It Worked for Me*, at 109 (2012).

<sup>86</sup> Grafeld Letter.

<sup>87</sup> 36 C.F.R. § 1234.24(b)(2) (August 28, 1995).

<sup>88</sup> 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.")

<sup>89</sup> 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.

<sup>90</sup> 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.<sup>91</sup>

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.<sup>92</sup> The Under Secretary for Management subsequently informed NARA that the Department sent a letter to Secretary Powell's representative conveying this request.<sup>93</sup> 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.<sup>94</sup> 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.<sup>95</sup> 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).

<sup>91</sup> 5 FAM 443.3 (October 30, 1995).

<sup>92</sup> 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).

<sup>93</sup> 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).

<sup>94</sup> 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.

<sup>95</sup> Grafeld Letter.



UNCLASSIFIED

accounts for official business.<sup>96</sup> 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.<sup>97</sup>

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.<sup>98</sup> 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

<sup>96</sup> 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.

<sup>97</sup> Letter from Cheryl Mills, cd Mills Group, to Patrick F. Kennedy, Under Secretary of State for Management (December 5, 2014).

<sup>98</sup> 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.<sup>99</sup> 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.<sup>100</sup>

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.<sup>101</sup> 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.<sup>102</sup> 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

<sup>99</sup> 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).

<sup>100</sup> 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).

<sup>101</sup> 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.

<sup>102</sup> The material was produced to the Department for the following individuals:

<b>Title</b>	<b>Production Dates</b>
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



UNCLASSIFIED

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.<sup>103</sup> 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.<sup>104</sup>

OIG received responses to questionnaires from most of Secretary Kerry's immediate staff, who reported occasional use of personal email accounts for official business.<sup>105</sup> A number of staff also reported that they follow current policy on forwarding emails containing Federal records from personal accounts to Department accounts.<sup>106</sup> 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

<sup>103</sup> 36 C.F.R. §1236.22(d) (October 2, 2009); 5 FAM 443.3 (October 30, 1995).

<sup>104</sup> 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>.

<sup>105</sup> 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.

<sup>106</sup> Eight stated that they forwarded or copied these emails to their Department accounts for records preservation purposes.

UNCLASSIFIED

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;<sup>107</sup> 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.<sup>108</sup> 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.<sup>109</sup> 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.<sup>110</sup>

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

---

<sup>107</sup> 36 C.F.R. § 1236.22 (October 2, 2009).

<sup>108</sup> 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).

<sup>109</sup> 1 FAM 271.1(4) (March 5, 2010).

<sup>110</sup> 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.<sup>111</sup> 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."<sup>112</sup> The FAM defines an AIS as an assembly of hardware, software, and firmware used to electronically input, process, store, and/or output data.<sup>113</sup> 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.<sup>114</sup> 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.<sup>115</sup> 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.<sup>116</sup> 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.

---

<sup>111</sup> See, e.g., 11 STATE 65111 (June 28, 2011).

<sup>112</sup> 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."

<sup>113</sup> 12 FAM 091 (January 11, 2016).

<sup>114</sup> 44 U.S.C. § 3554.

<sup>115</sup> 44 U.S.C. § 3552(b)(3).

<sup>116</sup> NIST, FIPS PUB 200: *Minimum Security Requirements for Federal Information and Information Systems* (March 2006).

UNCLASSIFIED

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.<sup>117</sup>

### **Restrictions Apply to the Use of Non-Departmental Systems**

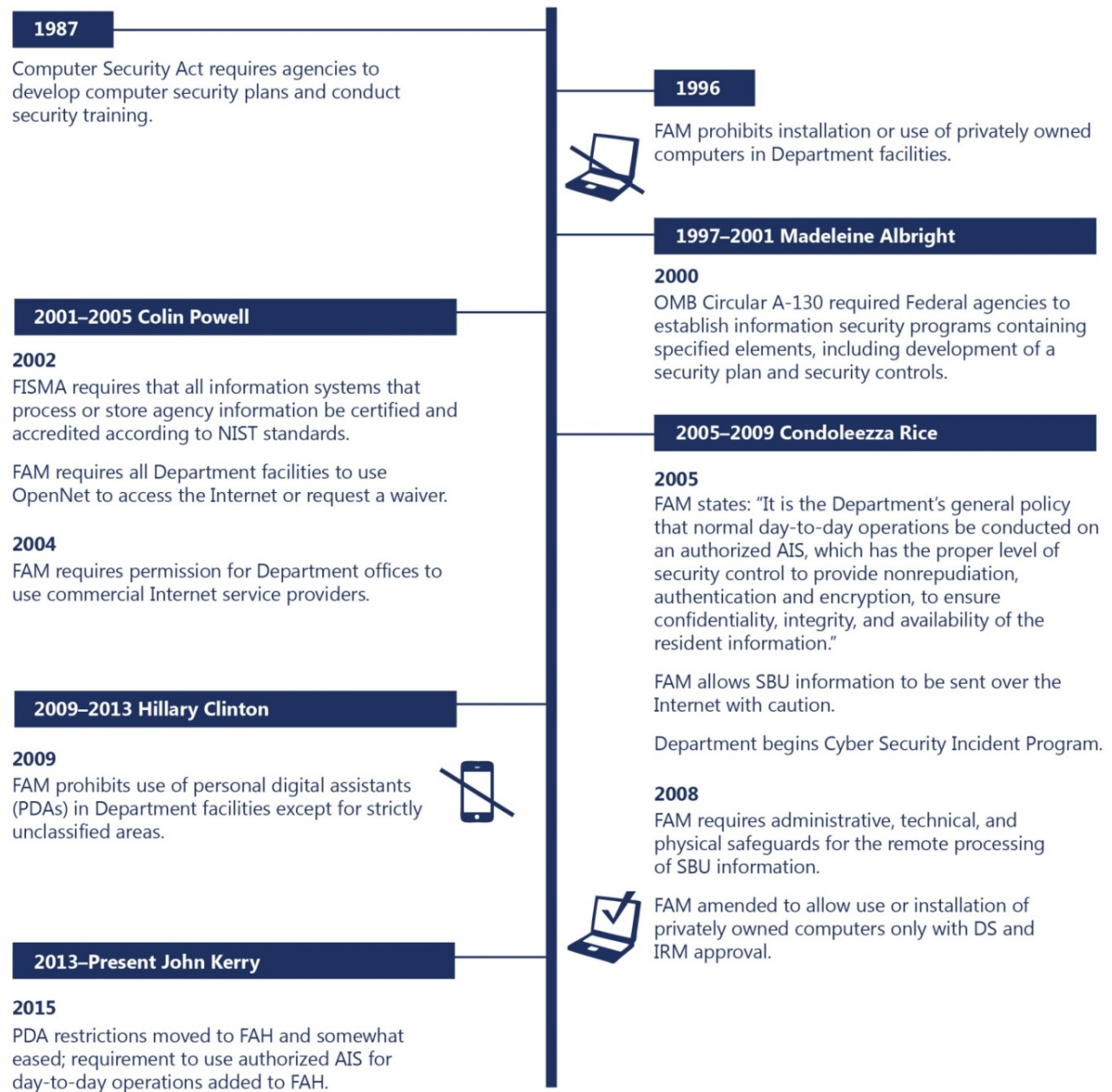
The FAM and FAH contain a number of restrictions regarding the use of non-Departmental computers, mobile devices, Internet connections, and personal email to transmit Department information. These provisions have evolved since 1996, but employees must implement safeguards or request approval before using such equipment. Figure 2 shows the evolution of these provisions and related statutes and regulations.

---

<sup>117</sup> 5 FAH-11 H-412.4(c)(4) (June 25, 2007).

UNCLASSIFIED

**Figure 2: Timeline of Selected Security Requirements and Policies**



**Source:** OIG analysis of laws and policies.

UNCLASSIFIED

**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.<sup>118</sup> 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.<sup>119</sup>

In 2009, the Department adopted policies addressing the specific requirements for use of non-Department-owned personal digital assistants (PDAs).<sup>120</sup> 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.<sup>121</sup> 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.<sup>122</sup>

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.<sup>123</sup> Under this policy, management and employees must exercise “particular care and judgment” when remotely processing SBU information.<sup>124</sup> Offices that allow employees to remotely process SBU information must ensure that appropriate administrative, technical, and physical safeguards are maintained to protect the

---

<sup>118</sup> 12 FAM 625.2-1 (April 12, 1996).

<sup>119</sup> 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.

<sup>120</sup> 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).

<sup>121</sup> 12 FAM 683.2-3 (December 2, 2009).

<sup>122</sup> 12 FAH-10 H-165.4 (May 20, 2015). These devices are referred to as Non-Department Owned Mobile Devices (NDOMDs).

<sup>123</sup> 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).

<sup>124</sup> 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.<sup>125</sup> 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.<sup>126</sup>

**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.<sup>127</sup> The Department further regulated access to the Internet by establishing rules in 2004 addressing the use of non-Departmental Internet connections in Department facilities.<sup>128</sup>

**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."<sup>129</sup>

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."<sup>130</sup> 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

<sup>125</sup> 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.

<sup>126</sup> 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).

<sup>127</sup> 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.

<sup>128</sup> 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).

<sup>129</sup> 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).

<sup>130</sup> 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.<sup>131</sup>

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."<sup>132</sup> 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.<sup>133</sup> 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.<sup>134</sup> 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.<sup>135</sup> Employees are also reminded of these issues through the Department's required annual Cybersecurity Awareness course.<sup>136</sup> 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

<sup>131</sup> 12 FAM 544.2 (November 4, 2005).

<sup>132</sup> 5 FAM 443.7 (October 23, 2015).

<sup>133</sup> 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.

<sup>134</sup> 04 STATE 204864 (September 22, 2004).

<sup>135</sup> 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).

<sup>136</sup> 5 FAM 845 (July 12, 2013).



UNCLASSIFIED

notices from 2005 to 2011 addressed BlackBerry security vulnerabilities, generally citing mobile devices as a weak link in computer networks.<sup>137</sup> 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.<sup>138</sup> 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.<sup>139</sup> 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.<sup>140</sup> It concluded by noting, "We also urge Department users to minimize the use

<sup>137</sup> See, e.g., CTAD, *Cyber Security Awareness* (March 3, 2011).

<sup>138</sup> 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).

<sup>139</sup> OIG asked DS if it had sent memoranda warning of similar risks to other Secretaries, but it could not find any similar examples.

<sup>140</sup> 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

UNCLASSIFIED

UNCLASSIFIED

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.”<sup>141</sup> 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.”<sup>142</sup>

### 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.

<sup>141</sup> 11 STATE 65111 (June 28, 2011).

<sup>142</sup> 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).

UNCLASSIFIED

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."<sup>143</sup> 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.<sup>144</sup> He described his email usage as "daily," though OIG was unable to determine how many emails he actually sent and received during his tenure.

<sup>143</sup> *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>.

<sup>144</sup> 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).

UNCLASSIFIED

UNCLASSIFIED

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.<sup>145</sup> By 2002, the Department had established the requirement to connect to the Internet only on OpenNet.<sup>146</sup> 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

---

<sup>145</sup> 12 FAM 625.2-1 (April 12, 1996); 5 FAM 751.2 (February 27, 2002).

<sup>146</sup> 5 FAM 871 (December 30, 2002).

UNCLASSIFIED

should be conducted on an authorized AIS,<sup>147</sup> 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.<sup>148</sup> 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.<sup>149</sup> 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."<sup>150</sup> 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

---

<sup>147</sup> 12 FAM 544.3 (November 4, 2005).

<sup>148</sup> 12 FAM 544.2 (November 4, 2005).

<sup>149</sup> 12 FAM 682 (August 4, 2008).

<sup>150</sup> <https://www.hillaryclinton.com/briefing/factsheets/2015/07/13/email-facts/> (date last downloaded April 20, 2016).

UNCLASSIFIED

personal email address.<sup>151</sup> 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."<sup>152</sup>
- 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

---

<sup>151</sup>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.

<sup>152</sup> 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.



UNCLASSIFIED

been set up for the Secretary<sup>153</sup> and also stated that “you should be aware that any email would go through the Department’s infrastructure and subject to FOIA searches.”<sup>154</sup> 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.<sup>155</sup> The second, a Schedule C political appointee who worked in IRM as a Senior Advisor from May 2009 through February 2013,<sup>156</sup> provided technical support for BlackBerry communications during the Secretary’s 2008 campaign for President.<sup>157</sup> 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.<sup>158</sup>

<sup>153</sup> According to the Department, this account was only used by Secretary Clinton’s staff to maintain an Outlook calendar.

<sup>154</sup> The former Director of S/ES-IRM declined OIG’s request for an interview.

<sup>155</sup> 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.

<sup>156</sup> Schedule C appointments are those of a “confidential or policy-determining character” 5 C.F.R. § 6.2.

<sup>157</sup> 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.

<sup>158</sup> 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.



UNCLASSIFIED

- 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."<sup>159</sup>

**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.<sup>160</sup> 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

<sup>159</sup> 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.

<sup>160</sup> 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.<sup>161</sup> 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.

---

<sup>161</sup> 11 STATE 73417 (July 20, 2011).

UNCLASSIFIED

## 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.

UNCLASSIFIED

**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.

UNCLASSIFIED

**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.<sup>1</sup>

**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.<sup>2</sup> 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.”<sup>3</sup> 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.<sup>4</sup>

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

---

<sup>1</sup> 12 FAM 625.2-1 (April 12, 1996).

<sup>2</sup> Pub. L. No. 100-235 (January 8, 1988).

<sup>3</sup> 44 U.S.C. § 3101.

<sup>4</sup> 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.<sup>5</sup> 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.<sup>6</sup> 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.<sup>7</sup>

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;

---

<sup>5</sup> 44 U.S.C. § 3105.

<sup>6</sup> 44 U.S.C. § 3106.

<sup>7</sup> 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.<sup>8</sup>

The regulations explicitly noted that "messages created or received on electronic mail systems may meet the definition of record."<sup>9</sup> Furthermore, the regulations required agencies to develop procedures to ensure that departing officials do not remove Federal records from agency custody.<sup>10</sup> 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.<sup>11</sup>

The regulations issued by NARA included separate provisions on electronic records management, including email.<sup>12</sup> 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.<sup>13</sup> The management of email records had to include instructions on preservation of data regarding transmission, calendar and task lists, and acknowledgements.<sup>14</sup> Agencies were restricted from storing the recordkeeping copy of email messages solely on the electronic mail

<sup>8</sup> 36 C.F.R. § 1222.20 (1995).

<sup>9</sup> 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.

<sup>10</sup> 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.

<sup>11</sup> 36 C.F.R. § 1222.38 (1990).

<sup>12</sup> 36 C.F.R. part 1234 (1995).

<sup>13</sup> 36 C.F.R. § 1234.10 (1995).

<sup>14</sup> 36 C.F.R. § 1234.24(a) (1995).

system, unless the system was able to meet regulatory requirements.<sup>15</sup> If an agency used paper files as its recordkeeping system, it was required to print email records and the related transmission and receipt data.<sup>16</sup>

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.<sup>17</sup>

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.<sup>18</sup>

**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).<sup>19</sup> 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.<sup>20</sup> 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."<sup>21</sup>

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."<sup>22</sup> It gave examples of emails that could constitute agency records, such as email providing key substantive comments on a draft

<sup>15</sup> 36 C.F.R. § 1234.24(b)(2) (1995).

<sup>16</sup> 36 C.F.R. § 1234.24(d) (1995).

<sup>17</sup> 36 C.F.R. § 1234.24(a)(4) (1995).

<sup>18</sup> 36 C.F.R. § 1234.28 (1995).

<sup>19</sup> 5 FAM 413.1 (October 30, 1995).

<sup>20</sup> 5 FAM 422.1 (October 30, 1995); 5 FAM 423.1 (October 30, 1995).

<sup>21</sup> 5 FAM 413.10 (October 30, 1995).

<sup>22</sup> 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.<sup>23</sup> 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.<sup>24</sup>

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.<sup>25</sup> 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

---

<sup>23</sup> 5 FAM 443.2(d) (October 30, 1995).

<sup>24</sup> 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.

<sup>25</sup> 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.<sup>26</sup> 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.<sup>27</sup> 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.<sup>28</sup>

The Department established rules in May 2004 regulating the use of non-government information systems, called Dedicated Internet Networks (DINs), to access the Internet.<sup>29</sup> 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).<sup>30</sup> According to the IT CCB, it approved approximately 180 such waivers during the first year this provision was in effect.

---

<sup>26</sup> 00 STATE 228951.

<sup>27</sup> 5 FAM 871 (December 30, 2002). At the time, OpenNet was referred to as "OpenNet Plus."

<sup>28</sup> 5 FAM 872 (December 30, 2002).

<sup>29</sup> 5 FAM 874.2 (May 4, 2004).

<sup>30</sup> 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.<sup>31</sup>

**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."<sup>32</sup> 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.<sup>33</sup> This amendment also noted that "email sent or received as a Department official is not personal."<sup>34</sup> 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.<sup>35</sup>

**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.

<sup>31</sup> 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.

<sup>32</sup> 5 FAM 751.4 (February 27, 2002).

<sup>33</sup> 5 FAM 414.2 (September 17, 2004).

<sup>34</sup> 5 FAM 415.1 (September 17, 2004).

<sup>35</sup> 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.<sup>36</sup> 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.<sup>37</sup>

#### 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.<sup>38</sup> 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.<sup>39</sup>

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.<sup>40</sup> 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).<sup>41</sup> The FAM

<sup>36</sup> NARA, *Protecting Federal records and other documentary materials from unauthorized removal*, Bulletin No. 2005-03 (December 22, 2004).

<sup>37</sup> 05 STATE 013345 (January 24, 2005).

<sup>38</sup> 12 FAM 592.2 (November 1, 2005).

<sup>39</sup> 12 FAM 592.2 (January 10, 2007).

<sup>40</sup> 12 FAM 544.3 (November 4, 2005).

<sup>41</sup> 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.<sup>42</sup> All employees who possessed SBU information on personally owned computers must ensure adequate and appropriate security for the SBU information.<sup>43</sup>

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.<sup>44</sup> 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.<sup>45</sup> Employees are prohibited from storing or processing SBU information on non-Department-owned computers unless it is necessary in the performance of their duties.<sup>46</sup> 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.<sup>47</sup>

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.<sup>48</sup>

**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.<sup>49</sup> 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.<sup>50</sup> Cybersecurity incidents are defined as acts against, or failure to protect, the Department's unclassified cyber infrastructure.<sup>51</sup>

<sup>42</sup> 12 FAM 544.3 (November 4, 2005).

<sup>43</sup> 12 FAM 544.3 (November 4, 2005).

<sup>44</sup> 12 FAM 682.1 (August 4, 2008).

<sup>45</sup> 12 FAM 682.2-4 (August 4, 2008).

<sup>46</sup> 12 FAM 682.2-4 (August 4, 2008).

<sup>47</sup> 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.

<sup>48</sup> 12 FAM 625.2-1 (July 28, 2008).

<sup>49</sup> 12 FAM 591.1(a) (November 1, 2005).

<sup>50</sup> 12 FAM 591.1 (November 1, 2005).

<sup>51</sup> 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.<sup>52</sup> Employees must inform their Information Systems Security Office and their Regional or Bureau Security Officer when any improper cybersecurity practice comes to their attention.<sup>53</sup> 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.<sup>54</sup>

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.<sup>55</sup> 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

<sup>52</sup> 12 FAM 592.4 (January 10, 2007).

<sup>53</sup> 12 FAM 592.4 (January 10, 2007).

<sup>54</sup> 12 FAM 592.1 and 592.2 (January 10, 2007).

<sup>55</sup> 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.<sup>56</sup>

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.<sup>57</sup> 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.<sup>58</sup>

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.<sup>59</sup>

**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

<sup>56</sup> NIST, FIPS PUB 200: *Minimum Security Requirements for Federal Information and Information Systems* (March 2006).

<sup>57</sup> 5 FAM 1065.1-6 (February 22, 2007); 5 FAH-11 H-411.4 (June 25, 2007).

<sup>58</sup> 5 FAH-11 H-411.5 (June 25, 2007).

<sup>59</sup> 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.”<sup>60</sup>

**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.<sup>61</sup>

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.<sup>62</sup>

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.<sup>63</sup>

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.”<sup>64</sup>

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)

---

<sup>60</sup> 5 FAM 422.3 (October 11, 2005).

<sup>61</sup> 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.

<sup>62</sup> NARA, *NARA Guidance for Implementing Section 207(e) of the E-Government Act of 2002*, Bulletin No. 2006-02 (December 15, 2005).

<sup>63</sup> 07 STATE 024044; Department of State, *Records Management Procedures*, Announcement No. 2007\_02\_147, February 28, 2007.

<sup>64</sup> 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.<sup>65</sup>

**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.<sup>66</sup>

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.<sup>67</sup> 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.<sup>68</sup>

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.<sup>69</sup> The existing requirements were largely retained, but renumbered.<sup>70</sup> 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

<sup>65</sup> 12 FAM 683.2-3 (December 2, 2009).

<sup>66</sup> 13 FAM 331 (December 22, 2010).

<sup>67</sup> CTAD, *Security Checklist* (December 15, 2009); CTAD, *Cyber Security Awareness* (March 3, 2011).

<sup>68</sup> *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).

<sup>69</sup> 74 Fed. Reg. 51004 (Oct 2, 2009).

<sup>70</sup> 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.<sup>71</sup> The new section on managing email records required preservation of email attachments that are an integral part of the record.<sup>72</sup> 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.<sup>73</sup>

**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.<sup>74</sup> 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.<sup>75</sup> 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.<sup>76</sup>

---

<sup>71</sup> 36 C.F.R. § 1220.34 (2010).

<sup>72</sup> 36 C.F.R. § 1236.22(a)(2) (2010).

<sup>73</sup> 36 C.F.R. § 1236.22(b) (2010).

<sup>74</sup> Department of State, *Preserving Electronic Message (E-mail) Records*, Announcement No. 2009\_06\_090, June 17, 2009.

<sup>75</sup> 09 STATE 120561; Department of State, *Records Management Responsibilities*, Announcement No. 2009\_11\_125, November 23, 2009.

<sup>76</sup> *Presidential Memorandum – Managing Government Records* (November 28, 2011).



UNCLASSIFIED

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.<sup>77</sup>

**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.<sup>78</sup> 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.<sup>79</sup>

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.<sup>80</sup> Employees were prohibited from remotely processing classified or SBU/NOFORN (not releasable to foreign nationals) information.<sup>81</sup> 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.<sup>82</sup> 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-

<sup>77</sup> *Memorandum for the Heads of Executive Departments and Agencies and Independent Agencies: Managing Government Records Directive*, M-12-18 (August 24, 2012).

<sup>78</sup> 5 FAM 872 (May 1, 2014).

<sup>79</sup> 5 FAM 872.1 (May 1, 2014).

<sup>80</sup> 12 FAH-10 H-172.1 (September 25, 2014). These provisions are currently located at 12 FAH-10 H-173.1 (January 11, 2016).

<sup>81</sup> 12 FAH-10 H-172.4 (September 25, 2014). These provisions are currently located at 12 FAH-10 H-173.4 (January 11, 2016).

<sup>82</sup> 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.<sup>83</sup>

**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.<sup>84</sup> 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.<sup>85</sup> 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...<sup>86</sup>

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.<sup>87</sup>

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.<sup>88</sup> The directive noted that employees may delete personal emails, but that "the only e-mails that are personal or non-record are those that

<sup>83</sup> 12 FAH-10 H-165.4 (May 20, 2015).

<sup>84</sup> Pub. L. No. 113-283 (December 18, 2014).

<sup>85</sup> Pub. L. No. 113-187 (November 26, 2014).

<sup>86</sup> 44 U.S.C. § 3301(a).

<sup>87</sup> 44 U.S.C. § 2911(a).

<sup>88</sup> 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.<sup>89</sup>

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.<sup>90</sup>

**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.<sup>91</sup>

In August 2013, NARA published a bulletin authorizing agencies to use a “Capstone” approach to managing email records, in lieu of print and file.<sup>92</sup> 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

---

<sup>89</sup> 5 FAM 443.7 (October 23, 2015).

<sup>90</sup> 5 FAM 414.7 (June 19, 2015).

<sup>91</sup> Department of State, *Departing Senior Officials: Government Records and Personal Papers*, Announcement No. 2013\_02\_122, February 26, 2013.

<sup>92</sup> 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.”<sup>93</sup> In 2015, NARA issued guidance on managing other forms of electronic messaging, including social media and texts.<sup>94</sup>

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.<sup>95</sup>

---

<sup>93</sup> 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).

<sup>94</sup> NARA, *Guidance on Managing Electronic Messages*, Bulletin No. 2015-02 (July 29, 2015).

<sup>95</sup> The Under Secretary sent this same message to all Chiefs of Mission in September 2014. 14 STATE 111506 (September 15, 2014).

UNCLASSIFIED

## 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

UNCLASSIFIED

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](#)



UNCLASSIFIED

[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.)

UNCLASSIFIED

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.

UNCLASSIFIED



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

UNCLASSIFIED

- 2 -

**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



UNCLASSIFIED

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.

UNCLASSIFIED

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 21<sup>st</sup> 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	<i>Foreign Affairs Handbook</i>
FAM	<i>Foreign Affairs Manual</i>
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

UNCLASSIFIED

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**

**[oig.state.gov](http://oig.state.gov)**

Office of Inspector General • U.S. Department of State • P.O. Box 9778 • Arlington, VA 22219

UNCLASSIFIED

# EXHIBIT H



LAW OFFICES

**WILLIAMS & CONNOLLY LLP**

725 TWELFTH STREET, N.W.

WASHINGTON, D. C. 20005-5901

(202) 434-5000

FAX (202) 434-5029

DAVID E. KENDALL

(202) 434-5145

dkendall@wc.com

EDWARD BENNETT WILLIAMS (1920-1988)  
PAUL R. CONNOLLY (1922-1978)

October 8, 2015

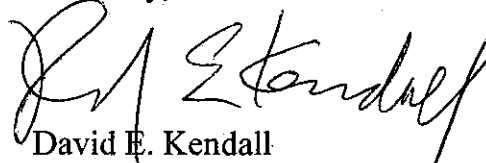
**BY EMAIL**

Mr. Patrick F. Kennedy  
Under Secretary of State for Management  
United States Department of State  
2201 C Street NW  
Washington, DC 20520-6421

Dear Mr. Kennedy:

Thank you for your letter dated October 2, 2015. I can confirm that, 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 in 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.

Sincerely,



David E. Kendall

DEK/bb

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

JUDICIAL WATCH, INC.,

Plaintiff,

v.

U.S. DEPARTMENT OF STATE,

Defendant.

No. 1:13-cv-01363-EGS

**[PROPOSED] ORDER**

Upon consideration of Plaintiff's Motion for Permission to Depose Hillary Clinton, Clarence Finney, and John Bentel, all oppositions thereto, and the entire record herein, it is hereby ORDERED that:

Plaintiff's motion to depose Hillary Clinton is DENIED.

SO ORDERED.

Date: \_\_\_\_\_

\_\_\_\_\_  
The Hon. Emmet G. Sullivan, U.S.D.J.