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

OIG HIGHLIGHTS

ESP-16-03

May 2016

OFFICE OF EVALUATIONS AND SPECIAL PROJECTS

Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements

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.

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

CONTENTS

OBJECTIVES AND METHODOLOGY

In April 2015, the Office of Inspector General (OIG) initiated an evaluation to address concerns identified during recent audits and inspections[1] and to respond to requests from the current Secretary of State and several Members of Congress involving a variety of issues, including the use of non-Departmental systems[2] to conduct official business, records preservation requirements, and Freedom of Information Act (FOIA) compliance. This report, which is the fourth and final to document OIG's findings in these areas,[3] addresses efforts undertaken by the Department of State (Department) to preserve and secure electronic records and communications involving the Office of the Secretary. Specifically, this report (1) provides an overview of laws, regulations, and policies related to the management of email records; (2) assesses the effectiveness of electronic records management practices involving the Office of the Secretary; (3) evaluates staff compliance with records management requirements; and (4) examines information security requirements related to the use of non-Departmental systems.

As part of the current evaluation, OIG reviewed laws, policies, and practices from (and, in some cases, prior to) 1997 through the present, covering the tenures of five Secretaries: Madeleine Albright (January 23, 1997–January 20, 2001); Colin Powell (January 20, 2001–January 26, 2005); Condoleezza Rice (January 26, 2005–January 20, 2009); Hillary Clinton (January 21, 2009–February 1, 2013); and John Kerry (February 1, 2013–Present).

OIG reviewed the requirements of the Federal Records Act[4] and the Federal Information Security Management Act (FISMA)[5] and related regulations; circulars and directives issued by the President, the National Archives and Records Administration (NARA), the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB); applicable

[1] OIG has identified the following issues: inconsistencies across the Department in identifying and preserving records, hacking incidents and other issues affecting the security of Department electronic communication, delays and other processing problems related to FOIA requests, and concerns about an Ambassador's use of private email to conduct official business. *See* OIG, *Review of State Messaging and Archive Retrieval Toolset and Record Email* (ISP-I-15-15, March 2015); OIG, *Audit of the Department of State Information Security Program* (AUD-IT-15-17, October 2014); OIG, *Management Alert: OIG Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program* (AUD-IT-14-03, November 2013); OIG, *Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services* (ISP-I-12-54, September 2012); and OIG, *Inspection of Embassy Nairobi, Kenya* (ISP-I-12-38A, August 2012).

[2] For purposes of this work, OIG uses the term "non-Departmental systems" to mean hardware and software that is not owned, provided, monitored, or certified by the Department of State.

[3] Previous reports include the following: OIG, *Potential Issues Identified by the Office of the Inspector General of the Intelligence Community Concerning the Department of State's Process for the Review of Former Secretary Clinton's Emails under the Freedom of Information Act* (ESP-15-04, July 2015), OIG, *Evaluation of the Department of State's FOIA Processes for Requests Involving the Office of the Secretary* (ESP-16-01, January 2016), and OIG, *Classified Material Discovered in Unclassified Archival Material* (ESP-16-02, March 2016).

[4] 44 U.S.C. chapters 21, 29, 31, and 33.

[5] Pub. L. No. 107-347, title III, 116 Stat. 2946 (2002). In 2014, FISMA was replaced by the Federal Information Security Modernization Act, 44 U.S.C. § 3551 (2014).

Department directives issued in the *Foreign Affairs Manual* (FAM) and the *Foreign Affairs Handbook* (FAH);[6] and guidance and policies in cables and memoranda. Appendix A summarizes the relevant laws and policies that OIG reviewed during this evaluation.

OIG employed a number of strategies to test compliance with email records preservation requirements applicable to each Secretary's tenure, including (1) sending questionnaires to current and former staff of the Office of the Secretary requesting information about email usage and preservation practices; (2) reviewing records and public statements related to email usage; (3) comparing stated practices against applicable laws and policies; and (4) searching available hard-copy and electronic files to identify and analyze email records and assess staff practices. OIG faced a number of challenges in conducting this testing, which will be discussed in greater detail throughout the report.

OIG also interviewed dozens of former and current Department employees, including the Deputy Secretary for Management and Resources (D-MR); the Under Secretary for Management (M); the Assistant Secretary and other staff in the Bureau of Administration (A); and various staff in the Office of the Secretary and its Executive Secretariat (S/ES), the Office of the Legal Adviser (L), the Bureau of Information Resource Management (IRM), and the Bureau of Diplomatic Security (DS). In conjunction with the interviews, OIG reviewed paper and electronic records and documents associated with these offices. OIG also consulted with NARA officials. Finally, OIG interviewed Secretary Kerry and former Secretaries Albright, Powell, and Rice. Through her counsel, Secretary Clinton declined OIG's request for an interview. [7]

OIG conducted this work in accordance with quality standards for evaluations as set forth by the Council of the Inspectors General on Integrity and Efficiency.

BACKGROUND

The Federal Records Act requires the head of each agency to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the

[6] The Department articulates official guidance, including procedures and policies, on matters relating to Department management and personnel in the *Foreign Affairs Manual* and *Handbook.* 2 FAM 1111.1 (July 3, 2013).

[7] In addition to Secretary Clinton, eight former Department employees declined OIG requests for interviews: (1) the Chief of Staff to Secretary Powell (2002-05); (2) the Counselor and Chief of Staff to Secretary Clinton (2009-13); (3) the Deputy Chief of Staff for Policy to Secretary Clinton (2009-11) and the Director of Policy Planning (2011-13); (4) the Deputy Chief of Staff for Operations to Secretary Clinton (2009-13); (5) the Deputy Assistant Secretary for Strategic Communication (2009-13); (6) the Director of the S/ES Office of Information Resources Management (2008-13); (7) a Special Advisor to the Deputy Chief Information Officer (2009-13) who provided technical support for Secretary Clinton's personal email system; and (8) a Senior Advisor to the Department, who supervised responses to Congressional inquiries (2014-15). Two additional individuals did not respond to OIG interview requests: the Deputy Secretary of State for Management and Resources (2011-13) and an individual based in New York who provided technical support for Secretary Clinton's personal email system but who was never employed by the Department.

information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities."[8] Effective records management is critical for ensuring that sufficient documentation of an agency's business is created, that an agency can efficiently locate and retrieve records needed in the daily performance of its mission, and that records of historical significance are identified, preserved, and made available to the public.[9]

Citing its responsibilities under the Federal Records Act, the Department sent letters in October and November 2014 to the representatives of former Secretaries Albright, Powell, Rice, and Clinton requesting that they make available copies of any Federal records in their possession, such as emails sent or received on a personal email account while serving as Secretary of State. In response, Secretary Albright's representative advised that Secretary Albright did not use a Department or personal email account during her tenure, and Secretary Rice's representative advised that Secretary Rice did not use a personal email account to conduct official business.[10] Representatives for Secretaries Powell and Clinton acknowledged that the Secretaries used personal email accounts to conduct official business.

Secretary Powell has publicly stated that, during his tenure as Secretary, he "installed a laptop computer on a private line" and that he used the laptop to send emails via his personal email account to his "principal assistants, individual ambassadors, and foreign minister colleagues."[11] Secretary Powell's representative advised the Department in 2015 that he did not retain those emails or make printed copies.[12] Secretary Powell has also publicly stated that he generally sent emails to his staff via their State Department email addresses but that he personally does not know whether the Department captured those emails on its servers.[13]

Secretary Clinton employed a personal email system to conduct business during her tenure in the United States Senate and her 2008 Presidential campaign. She continued to use personal email throughout her term as Secretary, relying on an account maintained on a private server, predominantly through mobile devices. Throughout Secretary Clinton's tenure, the server was located in her New York residence.[14]

---

[8] 44 U.S.C. § 3101. The FAM assigns these recordkeeping responsibilities to officials within the Bureau of Administration. 1 FAM 214 (May 1, 2009); 1 FAM 214.2 (November 25, 1998); 1 FAM 216.4 (January 17, 1997).

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

[10] Letter from Margaret P. Grafeld, Deputy Assistant Secretary for Global Information Systems, Bureau of Administration, U.S. Department of State, to Paul M. Wester, Jr., Chief Records Officer for the U.S. Government, NARA (April 2, 2015) [hereinafter Grafeld Letter].

[11] Colin Powell, *It Worked For Me: In Life and Leadership* 109 (2012).

[12] Grafeld Letter. Secretary Powell did not provide his emails to the Department in any form.

[13] ABC News, *This Week Transcript: Former Secretary of State Colin Powell* (March 5, 2015), available at http://abcnews.go.com/Politics/week-transcript-secretary-state-colin-powell/story?id=29463658.

[14] A March 17, 2009 memorandum prepared by S/ES-IRM staff regarding communications equipment in the Secretary's New York residence identified a server located in the basement.

In December 2014, in response to Department requests, Secretary Clinton produced to the Department from her personal email account approximately 55,000 hard-copy pages, representing approximately 30,000 emails that she believed related to official business. In a letter to the Department, her representative stated that it was the Secretary's practice to email Department officials at their government email accounts on matters pertaining to the conduct of government business. Accordingly, the representative asserted, to the extent that the Department retained records of government email accounts, the Department already had records of the Secretary's email preserved within its recordkeeping systems.[15]

PRESERVATION REQUIREMENTS HAVE GENERALLY REMAINED CONSISTENT AS LAWS AND POLICIES RELATED TO THE USE OF EMAILS HAVE EVOLVED

The requirement to manage and preserve emails containing Federal records has remained consistent since at least 1995, though specific policies and guidance related to retention methods have evolved over time. In general, the Federal Records Act requires appropriate management, including preservation, of records containing adequate and proper documentation of the "organization, functions, policies, decisions, procedures, and essential transactions of the agency."[16] Although emails were not explicitly mentioned in the Federal Records Act or FAM until the mid-1990s, the law has stated since 1943 that a document can constitute a record "regardless of physical form or characteristics."[17]

NARA promulgates regulations providing guidance to agencies on implementation of the Federal Records Act and recordkeeping obligations more generally.[18] Since 1990, the regulations issued by NARA have explained that the medium of the record may be "paper, film, disk, or other physical type or form" and that the method of recording may be "manual, mechanical, photographic, electronic, or any other combination of these or other technologies."[19] These regulations also have stated that a record can be made "by agency personnel in the course of their official duties, regardless of the method(s) or the medium involved."[20] See Appendix A for a compilation of preservation laws and policies that were in effect during the tenures of each Secretary, from Secretary Albright through Secretary Kerry. Figure 1 shows the evolution of management and preservation requirements related to emails containing Federal records.

[15] Letter from Cheryl Mills, cdmills Group, to Patrick F. Kennedy, Under Secretary of State for Management (December 5, 2014).

[16] 44 U.S.C. § 3101.

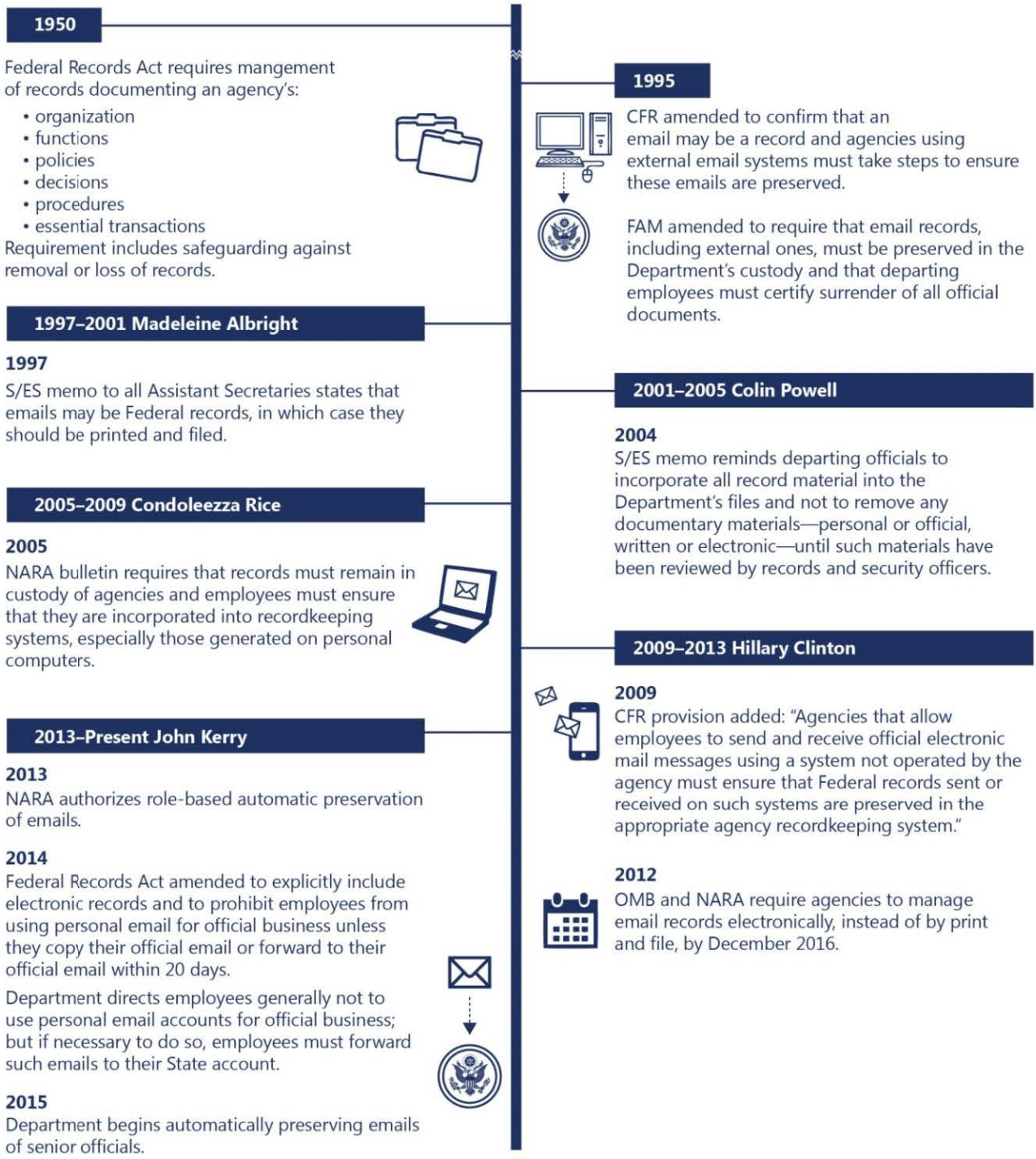
[17] H.R. 2943, Records Disposal Act of 1943, 57 Stat. 380 (July 7, 1943).

[18] 44 U.S.C. § 2904.

[19] 36 C.F.R. § 1222.12(b)(2) (1990).

[20] 36 C.F.R. § 1222.12(b)(3) (1990).

Figure 1: Timeline of Selected Records Management Requirements and Policies



Source: OIG analysis of laws and policies.

Email Records Equivalent to Other Records: In 1995, NARA amended the Code of Federal Regulations to confirm that "messages created or received on electronic mail systems may meet the definition of record."[21] The regulations also referenced the use of electronic communications systems external to the Government, indicating that "agencies with access to external electronic mail systems shall ensure that Federal records sent or received on these systems are preserved in the appropriate recordkeeping system."[22] A recordkeeping system is a manual or electronic system that captures, organizes, and categorizes records to facilitate their preservation, retrieval, use, and disposition.[23] The FAM adopted similar requirements in 1995, by providing in pertinent part that:

> all employees must be aware that some of the variety of the messages being exchanged on email are important to the Department and must be preserved; such messages are considered Federal records under the law.[24]

The FAM also included examples of emails that could constitute Federal records, including those providing key substantive comments on a draft action memorandum, documenting significant Department decisions and commitments reached orally, and conveying information of value on important Department activities.[25] The Department has frequently reminded employees of this requirement, including through a November 2009 announcement to all employees that noted that Federal records can be found in "any media, including email, instant messages, social media, etc."[26] However, the Department believes that the majority of the millions of emails sent to and from Department employees each year are non-permanent records with no long-term value.

In 2014, Congress amended the Federal Records Act explicitly to define Federal records to include "information created, manipulated, communicated, or stored in digital or electronic form."[27]

Methods of Preservation: According to NARA regulations, an agency "must ensure that procedures, directives and other issuances … include recordkeeping requirements for records in all media, including those records created or received on electronic mail systems."[28] These recordkeeping requirements include identifying specific categories of records to be maintained

---

[21] 36 C.F.R. § 1222.34(e) (1995).

[22] 36 C.F.R. § 1222.24(a)(4) (1995).

[23] 36 C.F.R. § 1220.18 (2009).

[24] 5 FAM 443.1(c) (October 30, 1995).

[25] 5 FAM 443.2(d) (October 30, 1995).

[26] *See, e.g.*, 09 STATE 120561; Department of State, Records Management Responsibilities, Announcement No. 2009_11_125, November 23, 2009.

[27] Presidential and Federal Records Act Amendments of 2014, Pub. L. No: 113-187, 128 Stat. 2003 (November 26, 2014) (amending 44 U.S.C. § 3301(a)).

[28] 36 C.F.R. § 1222.24 (October 2, 2009).

by agency personnel. Such maintenance includes ensuring that complete records are filed or otherwise identified and preserved, records can be readily found when needed, and permanent and temporary records are physically segregated from each other (or, for electronic records, segregable). Guidance issued by both NARA and the Department emphasize that every employee has records management responsibilities and must make and preserve records according to the law and Department policy.[29]

At the Department, compliance with this regulation and preservation of emails that constitute Federal records can be accomplished in one of three ways: print and file; incorporation into the State Messaging and Archive Retrieval Toolset (SMART); or the use of the NARA-approved Capstone program for capturing the emails of designated senior officials. Since 1995, the FAM has instructed employees, "until technology allowing archival capabilities for long-term electronic storage and retrieval of E-mail messages is available and installed," emails warranting preservation as records must be printed out and filed with related Department records.[30] NARA regulations codified in 2009 also specified that agencies must not use an electronic mail system to store the recordkeeping copy of electronic mail messages identified as Federal records unless that system contains specific features.[31] However, according to the Department, its technology has "lagged behind" this mandate.

---

[29] 5 FAM 414.8 (September 17, 2004). The prior version was located in 5 FAM 413.10 (October 30, 1995). *See also*, NARA, Frequently Asked Questions about Records Management in General, available at: http://www.archives.gov/records-mgmt/faqs/general.html#responsibility (January 20, 2001) (stating that "Federal employees are responsible for making and keeping records of their work.").

[30] 5 FAM 443.3 (October 30, 1995). S/ES-IRM reported to OIG that it has preserved email files numbering in the thousands for selected senior officials dating back at least as far as Secretary Powell's administration, although OIG found that these files are maintained in a format that makes them almost impossible to review or use.

[31] 36 C.F.R. § 1236.22 (2009). These required features are specified in 36 C.F.R. § 1236.20(b) as follows:

> (a) General. Agencies must use electronic or paper recordkeeping systems or a combination of those systems, depending on their business needs, for managing their records. Transitory email may be managed as specified in § 1236.22(c).
>
> (b) Electronic recordkeeping. Recordkeeping functionality may be built into the electronic information system or records can be transferred to an electronic recordkeeping repository, such as a DoD-5015.2 STD-certified product. The following functionalities are necessary for electronic recordkeeping:
>
> > (1) Declare records. Assign unique identifiers to records.
> >
> > (2) Capture records. Import records from other sources, manually enter records into the system, or link records to other systems.
> >
> > (3) Organize records. Associate with an approved records schedule and disposition instruction.
> >
> > (4) Maintain records security. Prevent the unauthorized access, modification, or deletion of declared records, and ensure that appropriate audit trails are in place to track use of the records.
> >
> > (5) Manage access and retrieval. Establish the appropriate rights for users to access the records and facilitate the search and retrieval of records.
> >
> > (6) Preserve records. Ensure that all records in the system are retrievable and usable for as long as needed to conduct agency business and to meet NARA-approved dispositions. Agencies must develop procedures to enable the migration of records and their associated metadata to new storage media or formats in order to avoid loss due to media decay or technology obsolescence.

In 2009, IRM introduced SMART throughout the Department, enabling employees to preserve a record copy of emails through their Department email accounts without having to print and file them.[32] However, the Office of the Secretary elected not to use SMART to preserve emails, in part because of concerns that the system would allow overly broad access to sensitive materials. As a result, printing and filing remained the only method by which emails could properly be preserved within the Office of the Secretary in full compliance with existing FAM guidance.

In August 2012, OMB and NARA issued a memorandum requiring agencies to eliminate paper recordkeeping and manage all email records in an electronic format by December 31, 2016.[33] Subsequently, in August 2013, NARA published a bulletin authorizing agencies to use the Capstone approach to manage emails based upon the sender or recipient's role within the agency (rather than the content of the email), which "allows for the capture of records that should be preserved as permanent from the accounts of officials at or near the top of an agency or an organizational subcomponent."[34] In February 2015, S/ES began retaining the emails of senior Department officials within its purview using the Capstone approach, a practice that was broadened to approximately 200 senior officials across the Department in September 2015.[35] However, if an employee is not a senior official under Capstone, he or she would still be responsible for preserving emails in an appropriate agency recordkeeping system, such as through the use of SMART or printing and filing.

Requirements for Email Records in Personal Accounts: As previously stated, documents can qualify as Federal records regardless of the location, method of creation, or the medium involved. Consequently, records management requirements have always applied to emails

---

(7) Execute disposition. Identify and effect the transfer of permanent records to NARA based on approved records schedules. Identify and delete temporary records that are eligible for disposal. Apply records hold or freeze on disposition when required.

(c) Backup systems. System and file backup processes and media do not provide the appropriate recordkeeping functionalities and must not be used as the agency electronic recordkeeping system.

[32] Prior OIG reports have observed that that use of the SMART system to create record emails has varied widely across Department offices. OIG, *Review of State Messaging and Archive Retrieval Toolset and Record Email* (ISP-I-15-15, March 2015) and OIG, *Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services* (ISP-I-12-54, September 2012).

[33] OMB and NARA, *Memorandum for The Heads of Executive Departments and Agencies and Independent Agencies: Managing Government Records Directive* (OMB Memorandum M-12-18) (August 24, 2012).

[34] NARA, *Guidance on a New Approach to Managing Email Records*, Bulletin No. 2013-02 (August 29, 2013), available at https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html.

[35] On January 29, 2015, the Executive Secretary notified the covered officials in the offices of the Secretary (S), the Deputy Secretaries of State (D), the Under Secretary for Political Affairs (P), and the Counselor of the Department (C) that on February 1, 2015, S/ES-IRM would begin permanently retaining all email activity in their State Department accounts. This notice also stated: "You should not use your private email accounts (e.g., Gmail) for official business." Later in 2015, the Under Secretary for Management notified all Assistant Secretaries and equivalents and Principal Deputies that all their email will be permanently stored and indexed beginning September 1, 2015. See *Memorandum To All Assistant Secretaries, Assistant Secretary Equivalents, And Principal Deputies: Email Retention* (July 29, 2015).

exchanged on personal email accounts, provided their content meets the definition of a record. In 2004, NARA issued a bulletin noting that officials and employees "must know how to ensure that records are incorporated into files or electronic recordkeeping systems, especially records that were generated electronically on personal computers." In 2009, NARA amended its regulations explicitly to address official emails on personal accounts:

> Agencies that allow employees to send and receive official electronic mail messages using a system not operated by the agency must ensure that Federal records sent or received on such systems are preserved in the appropriate agency recordkeeping system.[36]

In the 2014 amendments to the Federal Records Act, Congress added a provision prohibiting agency employees from creating or sending a record using "a non-official electronic messaging account" unless they copy their official electronic messaging account in the original creation or transmission of the record or forward a complete copy of the record to their official electronic messaging account within 20 days.[37] Shortly before the enactment of the 2014 amendments, the Department issued an interim directive with similar requirements[38] and subsequently updated the FAM in October 2015 as follows:

> Under the Presidential and Federal Records Act Amendments of 2014, employees are prohibited from creating or sending a record using a non-official email account unless the employee (1) copies the employee's official email account in the original creation or transmission, or (2) forwards a complete copy of record (including any attachments) to the employee's official email account not later than 20 days after the original creation or transmission….The U.S. National Archives and Records Administration has advised that "personal accounts should only be used in exceptional circumstances." Therefore, Department employees are discouraged from using private email accounts (e.g., Gmail, AOL, Hotmail, etc.) for official business. However, in those very limited circumstances when it becomes necessary to do so, the email messages covering official business sent from or received in a personal account must be captured and managed in a Department email system in a manner described above in accordance with the Presidential and Federal Records Act Amendments of 2014. If an employee has any emails (regardless of age) on his or her private email account(s) that have not already been forwarded to the employee's official email account, then such emails need to be forwarded to the employee's state.gov account as soon as possible. Employees are reminded that private email accounts should not be used to transmit or receive classified information.[39]

---

[36] 36 C.F.R. § 1236.22(b).

[37] 44 U.S.C. § 2911(a).

[38] Department of State, *A Message from Under Secretary for Management Patrick F. Kennedy regarding State Department Records Responsibilities and Policy*, Announcement No. 2014_10_115, October 17, 2014.

[39] 5 FAM 443.7 (October 23, 2015). Furthermore, the Consolidated Appropriations Act of 2016, which became Public Law 114-113 on December 18, 2015, requires, at Section 7077, that the Department update policies and directives needed to comply with Federal statutes, regulations, and presidential executive orders and memoranda concerning

However, forwarding to or copying an employee's official email account alone is not sufficient to fully meet records management requirements unless an employee's email is being captured under the Capstone approach. If such an email qualifies as a record, employees are still responsible for preserving it in an appropriate agency recordkeeping system, such as through the use of SMART or printing and filing.

Safeguards for Loss or Removal of Records: Both the Federal Records Act and NARA regulations also focus on preventing the removal, loss, or alienation of Federal records. The Act requires the head of each agency to establish safeguards against the removal or loss of records, including making it known to officials and employees of the agency (1) that records in the custody of the agency are not to be alienated or destroyed and (2) the penalties provided by law for the unlawful removal or destruction of records.[40] Although the FAM itself does not contain any explicit administrative penalties for removal or destruction of records, it does advise employees that such penalties exist and cites the Federal Records Act for this assertion.[41]

NARA regulations require each agency to have procedures to ensure that departing officials and employees do not remove Federal records from agency custody.[42] The Department has implemented these requirements through various FAM and FAH provisions that prohibit employees from removing, retiring, transferring, or destroying Department records; prohibit departing employees from removing any records; require each departing employee to sign a separation statement certifying that he or she has surrendered all documentation related to the official business of the Government; and require a review of documents proposed for removal by a departing employee. [43] For example, since 1982, the Department has given the

---

the preservation of all records made or received in the conduct of official business, including record emails, instant messaging, and other online tools. The Act also required the Department to direct departing employees that their records belong to the Federal government and to report within 30 days on the steps required to implement the recommendations issued by OIG in the March 2015 Review of State Messaging and Archive Retrieval Toolset and Record Email (ISP-1-15-15) and any recommendations from the OIG review of the records management practices of the Department of State. Section 7077 also contains a prohibition from the use of certain appropriated funds to support the use or establishment of email accounts or email servers created outside the .gov domain or not fitted for automated records management as part of a Federal government records management program in contravention of the Presidential and Federal Records Act Amendments of 2014 and a provision for withholding $10,000,000 from the Capital Investment Fund until the records management reports required under Section 7077 are submitted to Congress.

[40] 44 U.S.C. § 3105.

[41] 5 FAM 413(a)(6) (September 17, 2004). NARA's regulations interpreting the Federal Records Act refer to the criminal penalties in 18 U.S.C. §§ 641, 2071, but do not cite to any administrative penalties. 36 C.F.R. § 1230.12.

[42] 36 C.F.R. § 1222.24(a)(6) (October 2, 2009).

[43] 5 FAM 431.5(d) (July 31, 2012); 5 FAM 432.4(d) (July 31, 2012); 5 FAM 414.7 (June 19, 2015); 12 FAM 564.4 (July 10, 2015); 5 FAH-4 H-217.2 (August 13, 2008). These are the most current versions of these provisions, but the requirements have existed at least since 1995. *See also* 5 FAH-4 H-218a (April 15, 1997). For related discussions of agency responsibilities concerning removal of agency documents by senior officials upon departure, see also GAO, *Federal Records: Removal of Agency Documents by Senior Officials Upon Leaving Office* (GAO/GGD-89-91, July 1989), and GAO, *Document Removal by Agency Heads Needs Independent Oversight* (GAO/GGD-91-117, August 1991).

responsibility to the management section of each bureau, office, or post to ensure that every departing employee has signed a separation statement (form DS-109) that includes the following certification: "I have surrendered to responsible officials all unclassified documents and papers relating to the official business of the Government acquired by me while in the employ of the Department."[44] Numerous Department cables and announcements have emphasized the responsibility of every employee to sign a separation statement before she or he departs.[45]

Since 2004, both the Department and NARA have issued multiple notices emphasizing the need to preserve emails that constitute Federal records and to surrender all Federal records prior to departing government employment.[46] These include an August 2004 memorandum from the Executive Secretary that reminded departing officials not to remove any documentary materials, whether personal or official and whether in written or electronic form, until such materials have been reviewed by records and security officers. The memorandum also required departing officials to ensure that all record material they possess is incorporated in the Department's official files. The Department reiterated this guidance in April, June, and October 2008.[47] S/ES conducts annual workshops with the Agency Records Officer on records management for departing senior officials and their staffs. Such workshops were held in February 2007, September 2008, June 2009, April 2010, October 2011, October 2012, October 2013, October 2014, and June 2015.

[44] 5 FAM 417.2 (March 16, 1982); 5 FAM 413.9 (October 30, 1995); 5 FAM 414.7 (September 17, 2004).

[45] *See, e.g.*, *Procedures for the Removal of Personal Papers and Non-Record Material – 5 FAM 400, 5 FAH-4*, Announcement No. 2000_01_021, January 14, 2000; *Procedures for the Removal of Personal Papers and Non-Record Material,* Announcement No. 2005_02_017, February 3, 2005; 05 STATE 00018818 (February 1, 2005); 14 STATE 56010 (May 09, 2014).

[46] *See*, *e.g.*, NARA, *Protecting Federal records and other documentary materials from unauthorized removal*, Bulletin No. 2005-03 (December 22, 2004); NARA, *NARA Guidance for Implementing Section 207(e) of the E-Government Act of 2002*, Bulletin No. 2006-02 (December 15, 2005); Department of State, Records Management Procedures, Announcement No. 2007_02_147, February 28, 2007; Department of State, Preserving Electronic Message (E-mail) Records, Announcement No. 2009_06_090, June 17, 2009; 14 STATE 111506 (September 15, 2014); Department of State, *Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material*, Announcement No. 2008_04_089, April 17, 2008; Department of State, *Reminder – Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material*, Announcement No. 2008_06_095, June 16, 2008; Department of State, *Reminder – Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material*, Announcement No. 2008_10_087, October 16, 2008 ("The willful and unlawful removal or destruction of records is punishable by a fine or imprisonment of up to three years, or both (18 U.S.C. § 2071)."); 09 STATE 120561 (November 23, 2009); Department of State, *Records Management Responsibilities*, Announcement No. 2009_11_125, November 23, 2009; NARA, *Continuing Agency Responsibilities for Scheduling Electronic Records*, Bulletin No. 2010-02 (February 5, 2010); Department of State, *A Message from Under Secretary for Management Patrick F. Kennedy regarding State Department Records Responsibilities and Policy*, Announcement No. 2014_10_115, October 17, 2014.

[47] Memorandum from Karl Hoffman, Executive Secretary, to all Under Secretaries and Assistant Secretaries, *Refresher on Records Responsibilities and Review* (August 9, 2004).

MANAGEMENT WEAKNESSES CONTRIBUTE TO LOSS OF EMAIL RECORDS

As discussed above, the Federal Records Act and related NARA regulations impose records management responsibilities on both Federal agencies and individual employees. For agencies, these responsibilities include establishing "effective controls" to manage the creation, maintenance, use, and disposition of records in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government.[48] According to NARA, an effective records disposition program depends on scheduling[49] all records, regardless of location and regardless of physical form or characteristics (paper or electronic).[50] Therefore, agencies must implement a records maintenance program so that complete records are filed or otherwise identified and preserved, records can be readily found when needed, and permanent and temporary records are physically segregated or are segregable from each other.[51]

According to a 2010 U.S. Government Accountability Office (GAO) report, most agencies do not prioritize records management, as evidenced by lack of staff and budget resources, absence of up-to-date policies and procedures, lack of training, and lack of accountability.[52] In its most recent annual assessment of records management, NARA identified similar weaknesses across the Federal Government with regard to electronic records in particular. NARA reported that 80 percent of agencies had an elevated risk for the improper management of electronic records, reflecting serious challenges handling vast amounts of email, integrating records management functionality into electronic systems, and adapting to the changing technological and regulatory environments.[53]

In an effort to develop solutions to its own electronic records management challenges and to comply with NARA and OMB requirements, in 2013 the Department established the Electronic Records Management Working Group (ERMWG).[54] The Under Secretary for Management[55]

[48] 44 U.S.C. §§ 3101, 3102.

[49] A records schedule identifies records as either temporary or permanent. All records schedules must be approved by NARA. A records schedule provides mandatory instructions for the disposition of the records (including the transfer of permanent records and disposal of temporary records) when they are no longer needed by the agency. As part of the ongoing records life cycle, disposition should occur in the normal course of agency business. 44 U.S.C. §§ 3303, 3303a.

[50] *See* http://www.archives.gov/records-mgmt/publications/disposition-of-federal-records/chapter-2.html

[51] 36 C.F.R. § 1222.34.

[52] GAO, *Information Management: The Challenges of Managing Electronic Records* (GAO-10-838T, July 17, 2010).

[53] NARA, *Records Management Self-Assessment 2014* (November 6, 2015).

[54] The ERMWG is chaired by the Director of the Office of Management Policy, Rightsizing and Innovation, and its members include the Chief Information Officer (CIO) and representatives from L, IRM, and A.

[55] OMB and NARA Memorandum M-12-18, *Memorandum for The Heads of Executive Departments and Agencies and Independent Agencies: Managing Government Records Directive,* requires each agency to designate a Senior Agency Official (SAO) at the Assistant Secretary level or its equivalent with "direct responsibility for ensuring the department or agency efficiently and appropriately complies with all applicable records management statutes, regulations, and NARA policy, and the requirements of this Directive. The SAO must be located within the organization so as to make

approved recommendations submitted by the ERMWG, which included updating guidance on preserving senior officials' emails, developing a pilot program for the Capstone approach to record email, and directing IRM to perform a cost-benefit analysis of upgrading SMART as opposed to obtaining other solutions for preserving the emails of senior officials.[56]

In September 2015, Secretary Kerry named a former career Senior Foreign Service Officer as the Department's Transparency Coordinator. The Transparency Coordinator has been tasked with leading the Department's efforts in conjunction with the ERMWG to meet the President's Managing Government Records directive, responding to OIG's recommendations, and working with other agencies and the private sector to explore best practices and new technologies.

While these are positive steps, OIG identified multiple email and other electronic records management issues during the course of this evaluation. In its technical comments on this report, the Department noted that its budget has been declining over the past years and has not kept pace with inflation at a time when its national security mission is growing. According to the Department, it did request additional resources for records management for fiscal year 2017, but additional funding will still be needed to fully address its records management challenges.

Insufficient Oversight of the Recordkeeping Process: During the 20-year period covered by this evaluation, S/ES has had day-to-day responsibility for the Secretary of State's records management responsibilities, and it relies upon guidance and records schedules promulgated by the Bureau of Administration. The Bureau of Administration "plans, develops, implements, and evaluates programs, policies, rules, regulations, practices, and procedures on behalf of the Secretary to ensure compliance with the letter and spirit of relevant statutes, executive orders, and guidelines."[57] The Office of Information Programs and Services (IPS) is the component of the Bureau specifically tasked with issuing records guidance and overseeing records management efforts of the Department. Upon request, IPS reviews the records management practices of Department offices. The Acting Co-Director of IPS currently serves as the Agency Records Officer with program management responsibility for all records Department-wide throughout their life cycle (creation, acquisition, maintenance, use, and disposition). IPS has provided briefings, in conjunction with S/ES, to Office of the Secretary staff and has issued Department-wide notices and cables about records retention requirements, some of which included requirements to save email records, including records contained in personal emails. According to the FAM, the Agency Records Officer is "responsible for seeing that the Department and all of its component elements in the United States and abroad are in compliance with Federal records statutes and

---

adjustments to agency practices, personnel, and funding as may be necessary to ensure compliance and support the business needs of the department or agency." The Under Secretary for Management has served as the Department's SAO since 2012. Action Memo for the Secretary, *Designating A Senior Agency Official (SAO) for Managing Government Records* (November 27, 2012).

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

[57] 5 FAM 414.3 (June 9, 2009).

regulations,"[58] yet IPS has not reviewed Office of the Secretary records retention practices during the current or past four Secretaries' terms.

Although NARA is responsible for conducting inspections or surveys of agencies' records and records management programs and practices,[59] it last reviewed the Office of the Secretary's records retention practices in 1991–a quarter century ago. Beginning in 2009, NARA has relied on annual records management self-assessments and periodic reports from the Department to gauge the need to conduct formal inspections. The Department's last two self-assessments did not highlight any deficiencies.

Print and File Requirements Not Enforced: S/ES staff have provided numerous trainings for the Office of the Secretary on records preservation responsibilities and the requirement to print and file email records. However, S/ES staff told OIG that employees in the Office of the Secretary have printed and filed such emails only sporadically. In its discussions with OIG, NARA stated that this lack of compliance exists across the government. Although the Department is aware of the failure to print and file, the FAM contains no explicit penalties for lack of compliance, and the Department has never proposed discipline against an employee for failure to comply. OIG identified one email exchange occurring shortly before Secretary Clinton joined the Department that demonstrated a reluctance to communicate the requirement to incoming staff. In the exchange, records officials within the Bureau of Administration wondered whether there was an electronic method that could be used to capture the Secretary's emails because they were "not comfortable" advising the new administration to print and file email records.

Limited Ability To Retrieve Email Records: Even when emails are printed and filed, they are generally not inventoried or indexed and are therefore difficult to retrieve. As an illustration, almost 3,000 boxes, each filled with hundreds of pages of documents, would have to be reviewed manually, on a page-by-page basis, in order to identify and review all printed and filed emails from the Office of the Secretary since 1997. To help alleviate this problem, the Office of the Secretary could have adopted an electronic email management system in 2009 with the introduction of SMART. SMART allows users to designate specific emails sent or received through the Department's email system as record emails; other SMART users can search for and access record emails, depending on the access controls set by the individual who originally saved the email. However, prior OIG reports have repeatedly found that Department employees enter relatively few of their emails into the SMART system and that compliance varies greatly across bureaus, in part because of perceptions by Department employees that SMART is not intuitive, is difficult to use, and has some technical problems.[60]

[58] 5 FAM 414.2 (June 9, 2009).

[59] 44 U.S.C. § 2906. For an in-depth assessment of NARA's oversight practices, see GAO, *National Archives and Records Administration: Oversight and Management Improvements Initiated, but More Action Needed* (GAO-11-15, October 2010).

[60] OIG, *Review of State Messaging and Archive Retrieval Toolset and Record Email* (ISP-I-15-15, March 2015) and OIG, *Inspection of the Bureau of Administration, Global Information Services, Office of Information Programs and Services*

In 2015, the Department began permanently retaining the emails of approximately 200 senior officials pursuant to the Capstone approach discussed previously. The Department also plans to purchase an off-the-shelf product to electronically manage its emails in keeping with OMB's and NARA's requirement that it do so by December 2016.[61] This product will be adapted to Department requirements to include an interface that requires users to determine the record value and sensitivity of an email with one click and an auto-tagging feature that will allow emails to be stored according to disposition schedules. The new system will also be able to process legacy email files, such as the Personal Storage Table (.pst) files of departed officials.[62] In addition, the Department expects that the product will improve the Department's ability to perform more comprehensive email searches.

No Inventory of Archived Electronic Files: The S/ES Office of Information Resources Management (S/ES-IRM), the unit that handles information technology for the Office of the Secretary, reported to OIG that it has maintained electronic copies of email records for selected senior officials dating back as far as Secretary Powell's tenure. These records consist of thousands of electronic files, principally saved as .pst files. During OIG's fieldwork, S/ES-IRM did not have an inventory of the .pst or other electronic files that consistently identified the former email account holder. However, in early 2016, S/ES-IRM began to create a comprehensive inventory of these files.[63]

Unavailable or Inaccessible Electronic Files: When OIG requested specific .pst files, it encountered difficulties in obtaining and accessing those files. S/ES-IRM was unable to produce all of the .pst files OIG requested, and some of the requested files were corrupted and their recovery required considerable resources. Some .pst files were password protected, and staff did not know the passwords needed to open those files. Other files contained no data at all. Of the .pst files OIG was able to review, many were incomplete in that they did not span the particular employee's entire term of service, were mislabeled, or were missing key files such as populated sent or inbox folders. According to S/ES-IRM, as part of the inventory process currently underway, it is moving all .pst files in its possession onto servers and clearly labeling them.

Failure To Transfer Email Records to IPS: All Department offices are required to retire, or transfer, records to IPS in accordance with the Department's records disposition schedules.[64] For records

(ISP-I-12-54, September 2012). As noted previously, the Office of the Secretary did not implement SMART in part because of concerns the system would allow users to access highly sensitive records.

[61] On November 30, 2015, the Department issued a Request for Information to determine the capabilities of the private sector to provide and support a system to satisfy recordkeeping requirements involving emails by December 31, 2016. Department of State Email Management, Solicitation No. SAQMMA16I0008 (November 30, 2015).

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

[63] According to NARA regulations, creating .pst files is not an approved method of preserving Federal records, because .pst files do not have the required controls of an electronic records system. 36 C.F.R. § 1236.10.

[64] 5 FAM 433 (July 31, 2012).

specific to the Office of the Secretary, the relevant schedules require transferring most records to IPS at the end of the tenure of the Secretary.[65] S/ES has regularly retired paper copies of such records throughout the Secretaries' terms. However, S/ES has not consistently retired electronic email records. In April 2015, S/ES retired nine lots of electronic records containing approximately 16 gigabytes of data, consisting of emails, memoranda, travel records, and administrative documents from the tenures of former Secretaries Powell, Rice, and Clinton. However, the only email accounts included in this material were those of six of former Secretary Powell's staff and two of former Secretary Rice's staff. No email accounts from Secretary Clinton's staff were in the retired material.

In addition to retiring records in accordance with disposition schedules, offices must comply with Department policy requiring them to electronically capture the email accounts of selected senior officials upon their departure. A January 2009 memorandum from the Under Secretary for Management required Executive Directors and Management Officers to notify their system administrators of the departure of Presidential and political appointees and directed the administrators to copy the email accounts of those officials to two sets of CDs. The memorandum instructed the office to keep one of the CDs and send the other to IPS for records preservation.[66] The memorandum included an attachment identifying all officials who were subject to these requirements, including 50 officials from the offices under the purview of S/ES.[67] In August 2014, the Under Secretary sent another memorandum reiterating the requirement to electronically capture the email accounts of senior officials and broadening the list of officials subject to the requirement.[68] The Director of S/ES-IRM told OIG that S/ES complied with this requirement by creating .pst files covering the email accounts of the specified officials upon their departure. However, S/ES has never sent any CDs to IPS. In its most recent self-assessments of its records management, the Department stated that it has "established a procedure for departing officials to have their emails sent to the Department's Records Officer for preservation," but it failed to note that it has not complied with that procedure for the most senior officials in the organization.[69]

Failure To Follow Department Separation Processes: As noted previously, NARA regulations require each agency to adopt procedures to ensure that departing officials and employees do

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

[66] Under Secretary Patrick F. Kennedy, *Memorandum for All Under Secretaries, Assistant Secretaries, Executive Directors and Post Management Officers: Preserving Electronically the Email of Senior Officials upon their Departure* (January 2009).

[67] The list of officials included the Secretary, Deputy Secretaries, Counselor, Chief of Protocol, Special Assistants to the Secretary, the Chief of Staff, and the Deputy Chief of Staff.

[68] Under Secretary Patrick F. Kennedy, *Memorandum: Senior Officials' Records Management Responsibilities* (August 28, 2014).

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

not remove Federal records from agency custody.[70] The Department has implemented these requirements through various FAM provisions, including one that requires every departing employee to sign a separation statement (DS-109) certifying that he or she has surrendered all documentation related to the official business of the Government.[71] This function is handled for the Office of the Secretary by the Office of the S/ES Executive Director (S/ES-EX). However, S/ES-EX told OIG that, as the head of the agency, the Secretary is not asked to follow the exit process. Consequently, Secretaries Albright, Powell, Rice, and Clinton did not sign a DS-109 at the end of their tenures.

Notwithstanding the failure to adhere to separation requirements, all departing Secretaries of State from Secretary Albright on have followed the procedures governing the removal of personal papers. The FAH specifies that departing officials who wish to remove any documents must prepare an inventory of these personal papers and any non-record materials for review by Department officials.[72] Once the reviewing official is satisfied that removal of the documents would comply with Federal law and regulations, the reviewing official completes and signs Form DS-1904 (Authorization for the Removal of Personal Papers and Non-Record Materials). As the form itself notes, this process is especially important to ensure that the "the official records of the Department" are not "diminish[ed]." S/ES officials signed DS-1904 forms after the departures of Secretaries Albright, Powell, Rice, and Clinton. OIG reviewed the completed forms for these four Secretaries; none listed email as proposed for removal. However, in contrast to the Form DS-109, the DS-1904 does not impose a specific requirement to surrender documents.

Failure To Notify NARA of Loss of Records: Federal laws and regulations require an agency head to notify NARA of any actual, impending, or threatened unlawful removal or loss of agency records.[73] Although numerous senior officials emailed Secretaries Powell and Clinton on their personal email accounts to conduct official business, the Department did not make a formal request to the former Secretaries for the Federal records contained within these personal accounts until October and November 2014.[74] The Department also did not promptly notify NARA about the potential loss of records.[75] NARA officials told OIG they learned of former

[70] 36 C.F.R. § 1222.24 (2009).

[71] 12 FAM 564.4 (July 10, 2015); 5 FAM 414.7 (June 9, 2015). These are the most current versions of these provisions, but the requirements have existed since at least 1995.

[72] 5 FAH-4 H-217.2 (August 13, 2008).

[73] 44 U.S.C. § 3106; 36 C.F.R. § 1230.14.

[74] In letters to the respective representatives of Secretaries Powell and Clinton, the Department asked that, should they "be aware or become aware in the future of a federal record, such as an email sent or received on a personal email account while serving as Secretary of State, that a copy of this record be made available to the Department." In addition, the Department advised that they should "note that diverse Department records are subject to various disposition schedules, with most Secretary of State records retained permanently." Therefore, the Department asked that "a record be provided to the Department if there is reason to believe that it may not otherwise be preserved in the Department recordkeeping system."

[75] In May 2014, the Department undertook efforts to recover potential Federal records from Secretary Clinton. Thereafter, in July 2014, senior officials met with former members of Secretary Clinton's immediate staff, who were then acting as Secretary Clinton's representatives. At the meeting, her representative indicated that her practice of

Secretary Clinton's email practices through media accounts in March 2015. Immediately thereafter, NARA requested that the Department provide a report concerning "the potential alienation of Federal email records" created by former Secretary Clinton and actions taken to recover such records.[76]

In April 2015, the Department informed NARA of the information it obtained from the former Secretaries concerning their email records.[77] NARA subsequently requested additional information about how the Department implements records management requirements with regard to senior officials.[78] NARA also requested that the Department contact the Internet service providers (ISPs) associated with the personal accounts of Secretaries Powell and Clinton to inquire if "it is still possible to retrieve the email records that may still be present on their servers." The Under Secretary for Management subsequently informed NARA that the Department sent letters to the representatives of Powell and Clinton conveying this request.[79]

Well before the disclosure in April 2015, Department officials discussed in 2011 whether there was an obligation to search personal email accounts for Federal records.[80] In 2013, this issue arose again. Specifically, in early June 2013, Department staff participating in the review of potential material for production to congressional committees examining the September 2012 Benghazi attack discovered emails sent by the former Policy Planning Director via his Department email account to a personal email address associated with Secretary Clinton. In ensuing weeks, partly as a result of the staff's discovery, Department senior officials discussed

---

using a personal account was based on Secretary Powell's similar use, but Department staff instructed Clinton's representatives to provide the Department with any Federal records transmitted through her personal system. On August 22, 2014, Secretary Clinton's former Chief of Staff and then-representative advised Department leadership that hard copies of Secretary Clinton emails containing responsive information would be provided but that, given the volume of emails, it would take some time to produce. Subsequently, in October 2014, the Department began making formal, written requests to the representatives of Secretaries Albright, Powell, Rice and Clinton to produce any Federal records maintained in personal accounts. Secretary Clinton produced emails in hard copy form in December 2014. Thereafter, in March 2015, the Department made a similar request to four of Secretary Clinton's immediate staff. They produced email from their personal accounts during the summer of 2015.

[76] Letter from Paul M. Wester, Jr., Chief Records Officer for the U.S. Government, NARA, to Margaret P. Grafeld, Deputy Assistant Secretary for Global Information Systems, Bureau of Administration, U.S. Department of State (March 3, 2015).

[77] Grafeld Letter.

[78] Letter from Paul M. Wester, Jr., Chief Records Officer for the U.S. Government, NARA, to Margaret P. Grafeld, Deputy Assistant Secretary for Global Information Systems, Bureau of Administration, U.S. Department of State (July 2, 2015).

[79] Letter from Patrick F. Kennedy, Under Secretary of State for Management, to Laurence Brewer, Acting Chief Records Officer for the U.S. Government, NARA (November 6, 2015). Secretary Clinton responded to the Department that she has provided it with all official emails in her possession and pledged to provide any other record emails if they become available. As of May 2016, the Department has not received a response from Secretary Powell.

[80] This was prompted by a FOIA matter, in which a plaintiff inquired about a document it received showing that a staff assistant in the Office of the Secretary had received a work-related email on her personal account from someone who was not a Federal employee; the staff assistant had forwarded the email to her official account. This matter was ultimately resolved without further litigation.

the Department's obligations under the Federal Records Act in the context of personal email accounts. As discussed earlier in this report, laws and regulations did not prohibit employees from using their personal email accounts for the conduct of official Department business. However, email messages regarding official business sent to or from a personal email account fell within the scope of the Federal Records Act if their contents met the Act's definition of a record. OIG found that the Department took no action to notify NARA of a potential loss of records at any point in time.[81]

STAFF EMAIL USAGE AND COMPLIANCE WITH RECORDS MANAGEMENT REQUIREMENTS VARY

As part of this evaluation, OIG sought to examine whether staff in the Office of the Secretary complied with relevant email records management requirements, including those associated with the use of personal email accounts. However, OIG was unable to systematically assess the extent to which Secretaries Albright, Powell, Rice, Clinton, and Kerry and their immediate staff managed and preserved email records. In particular, OIG could not readily retrieve and analyze email records, in part because of the previously discussed weaknesses in the Department's records management processes. Although hard-copy and electronic email records dating back to Secretary Albright's tenure exist, these records have never been organized or indexed. For example, the Department could not immediately retrieve and make available for review specific email accounts identified and requested by OIG, which led to 2- to 3-month-long delays in obtaining the requested records. In addition, OIG was unable to reconstruct many events because of staff turnover and current employees' limited recollections of past events. These problems were compounded by the fact that multiple former Department employees and other individuals declined OIG requests for interviews, and OIG lacks the authority to compel anyone who is not a current Department employee to submit to interviews or to answer questions.

Moreover, OIG was unable to assess the degree to which Federal records sent though personal email accounts have been appropriately managed by Secretaries of State and their immediate staffs. Emails sent from the personal accounts of these individuals to other Department employees may or may not exist in the Department email accounts of the recipients, but OIG has limited ability to determine which accounts might contain these records unless the sender of the emails provides detailed information about the recipients. The Department currently lacks the resources and technical means to systematically review electronic files in its possession for records.

Despite these issues, OIG discovered anecdotal examples suggesting that Department staff have used personal email accounts to conduct official business, with wide variations among

[81] The current Deputy Secretary for Management and Resources, who during the summer of 2013 served as Counselor to the Department, told OIG that she recalled conversations with Secretary Kerry about email usage, but the conversations focused only on Secretary Kerry's practices. In his interview with OIG, Secretary Kerry reported that he was not involved in any of the discussions regarding Secretary Clinton's emails and that he first became aware of her exclusive use of a personal email account when an aide informed him around the time the information became public.

Secretaries and their immediate staff members. For instance, OIG reviewed the Department email accounts (.pst files) of senior Department employees who served on the immediate staffs of Secretary Powell and Secretary Rice between 2001 and 2008. Within these accounts, OIG identified more than 90 Department employees who periodically used personal email accounts to conduct official business, though OIG could not quantify the frequency of this use.

OIG also reviewed an S/ES-IRM report prepared in 2010 showing that more than 9,200 emails were sent within one week from S/ES servers to 16 web-based email domains, including gmail.com, hotmail.com, and att.net.[82] S/ES-IRM told OIG that it no longer has access to the tool used to generate this particular report. In another instance, in a June 3, 2011, email message to Secretary Clinton with the subject line "Google email hacking and woeful state of civilian technology," a former Director of Policy Planning wrote: "State's technology is so antiquated that NO ONE uses a State-issued laptop and even high officials routinely end up using their home email accounts to be able to get their work done quickly and effectively."

Notwithstanding the limitations on its ability to conduct a systematic evaluation, the information available allowed OIG to establish that email usage and compliance with statutory, regulatory, and Department requirements varied across the past five Secretaries' tenures. The practices of each Secretary and their immediate staff are discussed below.

Secretary Albright (January 23, 1997 – January 20, 2001): During Secretary Albright's tenure, desktop unclassified email and access to the Internet were not widely available to Department employees. OIG searched selected hard-copy records from her tenure and did not find any evidence to indicate that Secretary Albright used either Department or personal email accounts during that period. OIG additionally interviewed Secretary Albright and current and former Department staff, who further confirmed that she did not use email while serving as Secretary. In her interview with OIG, Secretary Albright noted that email use was still in its early stages when she became Secretary, and at the time she had no familiarity with the practice.

With regard to Secretary Albright's immediate staff, OIG did not find any emails that appeared to be to or from personal accounts and only found a few emails from staff Department accounts related to the Secretary's schedule. Staff responses on OIG questionnaires also identified minimal email usage–though two staff noted retaining emails on "Department servers."[83] These responses suggest staff may not have consistently complied with the preservation requirement to print and file emails containing Federal records.[84]

[82] Not all of these emails may indicate the use of personal email to conduct official business. Some of these emails could be communications with individuals outside the Department. Others could be communications by employees on personal matters, which is permissible under the Department's limited-use policy.

[83] OIG sent 13 questionnaires to former Secretary Albright's staff and received 8 responses, of which 2 were anonymous. None of the respondents reported having a personal email account while employed with the Department, and most did not acknowledge using a Department account. Two noted that they retained their emails on Department servers and one recalled receiving training on the topic of email preservation.

[84] 5 FAM 443.3 (October 30, 1995).

Secretary Powell (January 20, 2001 – January 26, 2005): During Secretary Powell's tenure, the Department introduced for the first time unclassified desktop email and access to the Internet on a system known as OpenNet, which remains in use to this day. Secretary Powell did not employ a Department email account, even after OpenNet's introduction. He has publicly written:

> To complement the official State Department computer in my office, I installed a laptop computer on a private line. My personal email account on the laptop allowed me direct access to anyone online. I started shooting emails to my principal assistants, to individual ambassadors, and increasingly to my foreign-minister colleagues ….[85]

OIG identified emails sent from and received by Secretary Powell's personal account in selected records associated with Secretary Powell. During his interview with OIG, Secretary Powell stated that he accessed the email account via his personal laptop computer in his office, while traveling, and at his residence, but not through a mobile device. His representative advised the Department that Secretary Powell "did not retain those emails or make printed copies."[86] Secretary Powell also stated that neither he nor his representatives took any specific measures to preserve Federal records in his email account. Secretary Powell's representative told OIG that she asked Department staff responsible for recordkeeping whether they needed to do anything to preserve the Secretary's emails prior to his departure, though she could not recall the names or titles of these staff. According to the representative, the Department staff responded that the Secretary's emails would be captured on Department servers because the Secretary had emailed other Department employees.

However, according to records management requirements and OIG's discussion with NARA, sending emails from a personal account to other employees at their Department accounts is not an appropriate method of preserving emails that constitute Federal records.[87] Guidance issued by both NARA and the Department emphasize that all employees have records management responsibilities and must make and preserve records that they send and receive.[88] Moreover, in keeping with NARA regulations,[89] the Department's policies specifically acknowledged that its email system at the time did not contain features necessary for long-term preservation of Federal records.[90] Therefore, Secretary Powell should have preserved any Federal records he

---

[85] Colin Powell, *It Worked for Me*, at 109 (2012).

[86] Grafeld Letter.

[87] 36 C.F.R. § 1234.24(b)(2) (August 28, 1995).

[88] 5 FAM 414.8 (September 17, 2004). The prior version was located at: 5 FAM 413.10 (October 30, 1995). *See also*, NARA, Frequently Asked Questions about Records Management in General, available at: http://www.archives.gov/records-mgmt/faqs/general.html#responsibility (January 20, 2001) (stating that "Federal employees are responsible for making and keeping records of their work.")

[89] 36 C.F.R. §1234.24(d) (August 28, 1995). In 2009, this provision was moved to 36 C.F.R. §1236.22(d) (October 2, 2009). It states, "Agencies must not use an electronic mail system to store the recordkeeping copy of electronic mail messages identified as Federal records unless that system" has certain listed attributes.

[90] As noted previously, Department guidance explained that messages must be printed and filed until "until technology allowing archival capabilities for long-term electronic storage and retrieval of E-mail records is available

created and received on his personal account by printing and filing those records with the related files in the Office of the Secretary.[91]

NARA agrees that the records should have been printed and filed but also told OIG that any effort to transfer such records to the Department would have mitigated the failure to preserve these records. At a minimum, Secretary Powell should have surrendered all emails sent from or received in his personal account that related to Department business. Because he did not do so at the time that he departed government service or at any time thereafter, Secretary Powell did not comply with Department policies that were implemented in accordance with the Federal Records Act. In an attempt to address this deficiency, NARA requested that the Department inquire with Secretary Powell's "internet service or email provider" to determine whether it is still possible to retrieve the email records that might remain on its servers.[92] The Under Secretary for Management subsequently informed NARA that the Department sent a letter to Secretary Powell's representative conveying this request.[93] As of May 2016, the Department had not received a response from Secretary Powell or his representative.

Members of Secretary Powell's immediate staff who responded to OIG questionnaires described minimal email usage overall—two staff recalled printing and filing emails in Department recordkeeping systems.[94] While the limited number of respondents also asserted they did not use personal email accounts for official business, OIG discovered some personal email usage for official business by Secretary Powell's staff through its own review of selected records.

Secretary Rice (January 26, 2005 – January 20, 2009): Secretary Rice and her representative advised the Department and OIG that the Secretary did not use either personal or Department email accounts for official business.[95] OIG searched selected records and did not find any evidence to indicate that the Secretary used such accounts during her tenure.

OIG received limited responses on questionnaires sent to former Secretary Rice's staff. Two staff recalled printing and filing emails, and only one acknowledged the use of personal email

---

and installed" that will preserve messages for "periods longer than current E-mail systems routinely maintain them." 5 FAM 443.3 (October 30, 1995).

[91] 5 FAM 443.3 (October 30, 1995).

[92] Letter from Paul M. Wester, Jr., Chief Records Officer for the U.S. Government, NARA, to Margaret P. Grafeld, Deputy Assistant Secretary for Global Information Systems, Bureau of Administration, U.S. Department of State (July 2, 2015).

[93] Letter from Patrick F. Kennedy, Under Secretary of State for Management, to Laurence Brewer, Acting Chief Records Officer for the U.S. Government, NARA (November 6, 2015).

[94] OIG sent 18 questionnaires to former Secretary Powell's staff and received 6 responses, of which one was anonymous. Two respondents stated they created records by printing copies of emails from their Department accounts and filing them into the Department's records system. One respondent recalled receiving records retention training.

[95] Grafeld Letter.

accounts for official business.[96] OIG reviewed hard-copy and electronic records of Secretary Rice's immediate staff and discovered that other staff who did not reply to the questionnaire did use personal email accounts to conduct official business.

Secretary Clinton (January 21, 2009 – February 1, 2013): Former Secretary Clinton did not use a Department email account and has acknowledged using an email account maintained on a private server for official business. As discussed above, in December 2014, her representative produced to the Department 55,000 hard-copy pages of documents, representing approximately 30,000 emails that could potentially constitute Federal records that she sent or received from April 2009 through early 2013. Secretary Clinton's representative asserted that, because the Secretary emailed Department officials at their government email accounts, the Department already had records of the Secretary's email preserved within its recordkeeping systems.[97]

As previously discussed, however, sending emails from a personal account to other employees at their Department accounts is not an appropriate method of preserving any such emails that would constitute a Federal record. Therefore, Secretary Clinton should have preserved any Federal records she created and received on her personal account by printing and filing those records with the related files in the Office of the Secretary.[98] At a minimum, Secretary Clinton should have surrendered all emails dealing with Department business before leaving government service and, because she did not do so, she did not comply with the Department's policies that were implemented in accordance with the Federal Records Act.

NARA agrees with the foregoing assessment but told OIG that Secretary Clinton's production of 55,000 pages of emails mitigated her failure to properly preserve emails that qualified as Federal records during her tenure and to surrender such records upon her departure. OIG concurs with NARA but also notes that Secretary Clinton's production was incomplete. For example, the Department and OIG both determined that the production included no email covering the first few months of Secretary Clinton's tenure—from January 21, 2009, to March 17, 2009, for received messages; and from January 21, 2009, to April 12, 2009, for sent messages. OIG discovered multiple instances in which Secretary Clinton's personal email account sent and received official business email during this period. For instance, the Department of Defense provided to OIG in September 2015 copies of 19 emails between Secretary Clinton and General David Petraeus on his official Department of Defense email account; these 19 emails were not in the Secretary's 55,000-page production. OIG also learned that the 55,000-page production did

[96] OIG sent 23 questionnaires to Secretary Rice's former staff and received 9 responses. Only one respondent reported using personal email accounts to conduct official business when "Department accounts were down or inaccessible." Two respondents said they printed emails and filed them into the Department's records systems; another said he believed IRM "backed up" all emails. One respondent stated she did not recall any specific instructions about retaining emails but assumed all emails were captured electronically.

[97] Letter from Cheryl Mills, cdmills Group, to Patrick F. Kennedy, Under Secretary of State for Management (December 5, 2014).

[98] 5 FAM 443.3 (October 30, 1995).

not contain some emails that an external contact not employed by the Department sent to Secretary Clinton regarding Department business. In an attempt to address these deficiencies, NARA requested that the Department inquire with Secretary Clinton's "internet service or email provider" to determine whether it is still possible to retrieve the email records that might remain on its servers.[99] The Department conveyed this request to Secretary Clinton's representative and on November 6, 2015, the Under Secretary for Management reported to NARA that the representative responded as follows:

> With regard to her tenure as Secretary of State, former Secretary Clinton has provided the Department on December 5, 2014, with all federal e-mail records in her custody, regardless of their format or the domain on which they were stored or created, that may not otherwise be preserved, to our knowledge, in the Department's recordkeeping system. She does not have custody of e-mails sent or received during the first few weeks of her tenure as she was transitioning to a new address, and we have been unable to obtain these. In the event we do, we will immediately provide the Department with federal record e-mails in this collection. [100]

With regard to Secretary Clinton's immediate staff, OIG received limited responses to its questionnaires, though two of Secretary Clinton's staff acknowledged occasional use of personal email accounts for official business.[101] However, OIG learned of extensive use of personal email accounts by four immediate staff members (none of whom responded to the questionnaire). During the summer of 2015, their representatives produced Federal records in response to a request from the Department, portions of which included material sent and received via their personal email accounts.[102] The material consists of nearly 72,000 pages in hard copy and more than 7.5 gigabytes of electronic data. One of the staff submitted 9,585 emails spanning January 22, 2009, to February 24, 2013, averaging 9 emails per workday sent on a personal email account. In this material, there are instances where the four individuals sent or received emails

[99] Letter from Paul M. Wester, Jr., Chief Records Officer for the U.S. Government, NARA, to Margaret P. Grafeld, Deputy Assistant Secretary for Global Information Systems, Bureau of Administration, U.S. Department of State (July 2, 2015).

[100] Letter from Patrick F. Kennedy, Under Secretary of State for Management, to Laurence Brewer, Acting Chief Records Officer for the U.S. Government, NARA (November 6, 2015).

[101] OIG sent 26 questionnaires to Secretary Clinton's staff and received 5 responses. Three respondents reported that they did not use personal email accounts to conduct official business. Another reported occasionally using personal email accounts while traveling with the Secretary and when Department accounts were not working. Another said he occasionally used his personal laptop or desktop at home to access the Department's OpenNet and that he assumed all data processed on OpenNet would be available to the Department.

[102] The material was produced to the Department for the following individuals:

Title	Production Dates
Counselor and Chief of Staff	6/25/2015; 8/10/2015; 8/12/2015
Deputy Chief of Staff for Operations	7/9/2015; 8/7/2015
Deputy Chief of Staff/Director of Policy Planning	7/30/2015
Deputy Assistant Secretary, Strategic Communications	7/28/2015; 8/6/15

regarding Department business using only their personal web-based email accounts. Accordingly, these staff failed to comply with Department policies intended to implement NARA regulations, because none of these emails were preserved in Department recordkeeping systems prior to their production in 2015.[103] As noted above, NARA has concluded that these subsequent productions mitigated their failure to properly preserve emails that qualified as Federal records during their service as Department employees. However, OIG did not attempt to determine whether these productions were complete. None of these individuals are currently employed by the Department.

Secretary Kerry (February 1, 2013 – Present): Secretary Kerry uses a Department email account on OpenNet and stated that, while he has used a personal email account to conduct official business, he has done so infrequently. In his interview with OIG, Secretary Kerry stated that he used his personal email more frequently when he was transitioning from the U.S. Senate to the Office of the Secretary. However, after discussions with his aides and other Department staff, he began primarily using his Department email account to conduct official business. The Secretary stated he may occasionally use personal email for official business when responding to a sender who emailed him on his personal account. The Secretary also stated that he either copies or forwards such emails to his Department account and copies his assistant. OIG's limited review of electronic records shows some personal email account usage by Secretary Kerry. Secretary Kerry's emails are now being retained using the Capstone approach discussed previously, which complies with the Federal Records Act and email records management requirements.[104]

OIG received responses to questionnaires from most of Secretary Kerry's immediate staff, who reported occasional use of personal email accounts for official business.[105] A number of staff also reported that they follow current policy on forwarding emails containing Federal records from personal accounts to Department accounts.[106] OIG's limited review of electronic records shows some personal email account usage by these staff.

Other staff reported that their emails are being retained using the Capstone approach, and some mentioned preserving emails through printing and filing. Several staff mentioned preserving emails by saving them in their Department email accounts. However, as previously

[103] 36 C.F.R. §1236.22(d) (October 2, 2009); 5 FAM 443.3 (October 30, 1995).

[104] NARA, *Guidance on a New Approach to Managing Email Records*, Bulletin No. 2013-02 (August 29, 2013), available at https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html.

[105] OIG sent 36 questionnaires to Secretary Kerry's staff and received 30 responses (several of the non-respondents had departed or were departing the Office of the Secretary), as well as a completed questionnaire from Secretary Kerry. With regard to preservation of Department emails, many reported retaining files in Microsoft Outlook and others reported that the Department was permanently retaining their email as part of the new Capstone program for senior officials. Most staff reported receiving training or other guidance on records preservation requirements through a variety of means, including formal training sessions, briefings, memos, and Department notices. Eleven staff reported using personal email accounts or other devices for official business, usually because of Internet connectivity interruptions while traveling.

[106] Eight stated that they forwarded or copied these emails to their Department accounts for records preservation purposes.

noted, NARA regulations state that agencies may only use an electronic mail system to store the recordkeeping copy of electronic mail messages identified as Federal records if that system contains specific features;[107] the current Department email system does not contain these features. Given that the Office of the Secretary does not use the SMART system, staff whose emails are not being retained under the Capstone approach should still be preserving emails through printing and filing. However, as previously noted, the Department is in the process of adopting a new email records management system that will cover the Office of the Secretary with the goal of meeting the requirement to manage all email records in an electronic format by December 31, 2016.[108] The Department plans that this system will eventually capture some of the email currently saved in Department email accounts and all of the email of senior officials currently being preserved.

CYBERSECURITY RISKS RESULT FROM THE USE OF NON-DEPARTMENTAL SYSTEMS AND EMAIL ACCOUNTS

In addition to complying with records management and preservation requirements, Department employees, including those in the Office of the Secretary, must comply with cybersecurity policies. Department information must be secure and protected from threats.

DS and IRM are the two bureaus within the Department with primary responsibility for ensuring the security of Department electronic information.[109] IRM is responsible for establishing effective information resource management planning and policies; ensuring the availability of information technology systems and operations; and approving development and administration of the Department's computer and information security programs and policies. DS is responsible for providing a safe and secure environment for the conduct of U.S. foreign policy, including personal, physical, and information security.[110]

According to DS and IRM officials, Department employees must use agency-authorized information systems to conduct normal day-to-day operations because the use of non-Departmental systems creates significant security risks. Department policies have evolved considerably over the past two decades; but since 1996, the FAM and FAH have contained numerous provisions regulating the use of such outside systems, including computers, personal devices, Internet connections, and email. (See Appendix A for a compilation of related cybersecurity laws and policies that were in effect during the tenures of each Secretary, from Secretary Albright through Secretary Kerry.) These provisions do contemplate limited use of non-Departmental systems, but the exceptions are quite narrow. Among the risks is the

[107] 36 C.F.R. § 1236.22 (October 2, 2009).

[108] OMB and NARA, *Memorandum for The Heads of Executive Departments and Agencies and Independent Agencies: Managing Government Records Directive* (OMB Memorandum M-12-18) (August 24, 2012).

[109] 1 FAM 271.1(4) (March 5, 2010).

[110] 12 FAM 010 (December 21, 2004).

targeting and penetration of the personal email accounts of Department employees, which was brought to the attention of the most senior officials of the Department as early as 2011.[111] Another significant risk is the introduction of viruses and malware onto Department systems, which increases their vulnerability to intrusion.

Based on this evaluation and a previous OIG inspection, OIG identified three Department officials—Secretary Powell, Secretary Clinton, and a former U.S. Ambassador to Kenya—who exclusively used non-Departmental systems to conduct official business. As will be discussed in greater detail below, OIG acknowledges significant differences in the facts and circumstances surrounding each of these cases.

Employees Generally Must Use Department Information Systems To Conduct Official Business

The Department's current policy, implemented in 2005, is that normal day-to-day operations should be conducted on an authorized Automated Information System (AIS), which "has the proper level of security control to … ensure confidentiality, integrity, and availability of the resident information."[112] The FAM defines an AIS as an assembly of hardware, software, and firmware used to electronically input, process, store, and/or output data.[113] Examples include: mainframes, servers, desktop workstations, and mobile devices (such as laptops, e-readers, smartphones, and tablets).

This policy comports with FISMA, which was enacted in December 2002 and requires Federal agencies to ensure information security for the systems that support the agency's operations and assets, including information security protections for information systems used by a contractor of an agency or other organization on behalf of an agency.[114] FISMA defines information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide for the integrity, confidentiality, and availability of the information and systems.[115] In 2006, as required by FISMA, NIST promulgated minimum security requirements that apply to all information within the Federal Government and to Federal information systems.[116] Among these are requirements for certifying and accrediting information systems, retaining system audit records for monitoring purposes, conducting risk assessments, and ensuring the protection of communications.

---

[111] *See, e.g.,* 11 STATE 65111 (June 28, 2011).

[112] 12 FAM 544.3 (November 4, 2005). This provision also states that "The Department's authorized telework solution(s) are designed in a manner that meet these requirements and are not considered end points outside of the Department's management control."

[113] 12 FAM 091 (January 11, 2016).

[114] 44 U.S.C. § 3554.

[115] 44 U.S.C. § 3552(b)(3).

[116] NIST, FIPS PUB 200: *Minimum Security Requirements for Federal Information and Information Systems* (March 2006).

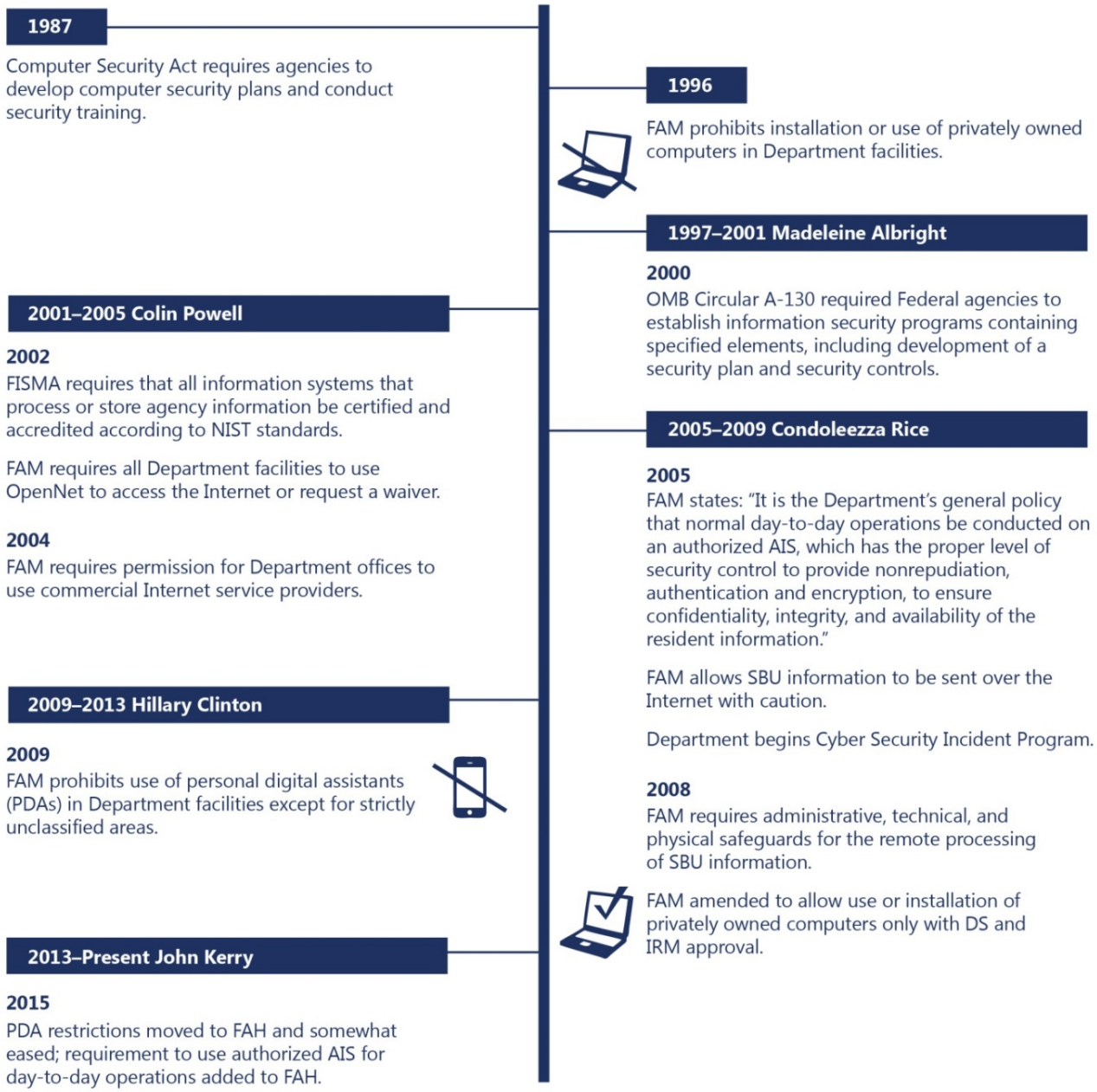
In 2007, the Department adopted additional policies to implement these requirements, including numerous provisions intended to ensure that non-Departmental information systems that process or store Department information maintain the same minimum security controls. Further, non-Departmental systems that are sponsored by the Department to process information on its behalf must be registered with the Department.[117]

Restrictions Apply to the Use of Non-Departmental Systems

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

[117] 5 FAH-11 H-412.4(c)(4) (June 25, 2007).

Figure 2: Timeline of Selected Security Requirements and Policies



Source: OIG analysis of laws and policies.

Privately Owned Computers and Mobile Devices: In 1996, the FAM directed Department systems managers to ensure that privately owned computers were not installed or used in any Department office building.[118] In 2008, the Department amended this provision to prohibit the use or installation of non-U.S. Government-owned computers in any Department facility without the written approval of DS and IRM, with certain exceptions.[119]

In 2009, the Department adopted polices addressing the specific requirements for use of non-Department-owned personal digital assistants (PDAs).[120] Under this policy, PDAs could only be turned on and used within Department areas that are strictly unclassified (such as the cafeteria) and could not connect with a Department network except via a Department-approved remote-access program, such as Global OpenNet.[121] In 2014, the Department amended this provision to authorize Department managers in domestic locations to allow non-Department-owned PDAs within their specific work areas, provided users maintain a minimum 10-foot separation between the PDA and classified processing equipment. In 2015, the Department replaced these provisions with a new FAH provision that included the domestic 10-foot-separation rule and the ban on connecting to a Department network except via a Department-approved remote-access program.[122]

Related to these provisions is the Department policy on "remote processing"—the processing of Department unclassified or sensitive but unclassified (SBU) information on non-Department-owned systems (such as a home computer or a tablet) or on Department-owned systems (such as a Department-issued laptop) at non-Departmental facilities (such as at an employee's home or a hotel)—which has been in place since 2008.[123] Under this policy, management and employees must exercise "particular care and judgment" when remotely processing SBU information.[124] Offices that allow employees to remotely process SBU information must ensure that appropriate administrative, technical, and physical safeguards are maintained to protect the

[118] 12 FAM 625.2-1 (April 12, 1996).

[119] 12 FAM 625.2-1 (July 28, 2008). This provision was removed from the FAM in 2015, but a FAH provision prohibits the installation of non-Department owned information systems within Department facilities without the written authorization of DS and IRM. 12 FAH-10 H-112.14-2 (September 19, 2014). Both the FAM and FAH provisions include an exception for a non-Department entity that has an approved dedicated space within a Department facility.

[120] The FAM defined PDAs as "hand-held computers" including "standard personal digital assistants; e.g., Palm devices, Win CE devices, etc., and multi-function automated information system (AIS) devices; e.g., BlackBerry devices, PDA/cell phones, etc." 12 FAM 683.1 (December 2, 2009).

[121] 12 FAM 683.2-3 (December 2, 2009).

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

[123] 12 FAM 682 (August 4, 2008). This subchapter was later removed from the FAM and moved to the FAH at 12 FAH-10 H-170 (as amended January 11, 2016).

[124] 12 FAM 682.2-4 (August 4, 2008). This requirement is currently located at 12 FAH-10 H-173.4 (January 11, 2016). SBU information is defined in the FAM as information that is not classified for national security reasons but that warrants or requires administrative control and protection from public or other unauthorized disclosure for other reasons. Examples include personnel data, visa and asylum records, law enforcement information, privileged communications, and deliberative inter- or intra-agency communications. 12 FAM 541 (March 5, 2013).

confidentiality and integrity of records and to ensure encryption of SBU information with products certified by NIST. Employees must implement and regularly update basic home security controls, including a firewall, anti-spyware, antivirus, and file-destruction applications for all computers on the network.[125] In 2014, the Department added a provision to the FAH to require users who process SBU information on non-Department-owned storage media to encrypt it with products certified by NIST. [126]

Internet Connections: Since the end of 2002, the FAM has required all Department facilities to use the Department's primary Internet connection, OpenNet, to establish Internet connectivity.[127] The Department further regulated access to the Internet by establishing rules in 2004 addressing the use of non-Departmental Internet connections in Department facilities.[128]

Personal Email: Since 2002, Department employees have been prohibited from auto-forwarding their email to a personal email address "to preclude inadvertent transmission of SBU email on the Internet."[129]

The FAM also reminds employees that "transmissions from the Department's OpenNet to and from non-U.S. Government Internet addresses, and other .gov or .mil addresses, unless specifically directed through an approved secure means, traverse the Internet unencrypted."[130] The FAM further states that, with regard to SBU information, the Department is expected to provide, and employees are expected to use, approved secure methods to transmit such information when available and practical. However, if such secure methods are not available, employees with a valid business need may transmit SBU information over the Internet unencrypted so long as they carefully consider that unencrypted emails can pass through foreign and domestic controlled ISPs, placing the confidentiality and integrity of the information at risk. In addition, the FAM instructs employees transmitting SBU information outside the

[125] 12 FAM 682.2-5 (August 4, 2008). Currently, these requirements, as amended, are located at 12 FAH-10 H-173.4 (January 11, 2016). The amended provision requires NIST FIPS 140-2 encryption for SBU information in addition to the use of a firewall anti-spyware, anti-virus, and file destruction applications.

[126] 12 FAH-10 H-172.1 (September 25, 2014). Currently, this requirement is located at 12 FAH-10 H-173.4 (January 11, 2016). If the employee has a wireless home network, the FAH requires use of a NIST-validated product to secure the wireless connection. 12 FAH-10 H-173.4(9) (September 25, 2014).

[127] 5 FAM 871 (December 30, 2002). The language of this provision was amended in 2004, 2009, and 2013, but the basic requirement to use OpenNet has remained consistent.

[128] 5 FAM 874.2 (May 4, 2004). Currently, these rules are at 5 FAM 872 (May 1, 2014). Department facilities must seek authorization from the bureau Executive Director or post Management Officer to use such a connection. 5 FAM 872.1 (May 1, 2014). Such systems may not be used to process SBU information, except in limited amounts under exigent circumstances. 5 FAM 872.2 (May 1, 2014).

[129] 5 FAM 751.2 (February 27, 2002). This rule was amended in 2011 to incorporate a prohibition on including a personal email address in an auto-reply message. 5 FAM 752.1(e) (November 14, 2011).

[130] 12 FAM 544.3 (November 4, 2005). From 2002 to 2005, transmission of SBU information over the Internet was completely prohibited. 5 FAM 751.2 (February 27, 2002).

Department's OpenNet network on a regular basis to the same official or personal email address to request a solution from IRM.[131]

In 2015, the Department amended the FAM to incorporate NARA's guidance, which advises employees that "personal accounts should only be used in exceptional circumstances."[132] This provision also states that "Department employees are discouraged from using private email accounts (e.g., Gmail, AOL, Hotmail, etc.) for official business [except] in those very limited circumstances when it becomes necessary to do so." However, the FAM gives no further guidance about what type of circumstances would permit use of personal email.

The Department Has Issued Numerous Warnings About Cybersecurity Risks

One of the primary reasons that Department policy requires the use of Department systems is to guard against cybersecurity incidents. Threats and actual attacks against the Department have been on the rise for nearly a decade. For example, in May 2006, the Department experienced large-scale computer intrusions that targeted its headquarters and its East Asian posts.[133] Consequently, the Department has issued numerous announcements, cables, training requirements, and memos to highlight the various restrictions and risks associated with the use of non-Departmental systems, especially the use of personal email accounts.

As early as 2004, Department cables reminded staff that only Department-approved software should be installed on the Department's information systems because outside software may bypass firewall and anti-virus checks, creating an open channel for hackers and malicious code, thus placing Department networks at serious risk.[134] Since then, the Department has published prohibitions or warnings related to the use of instant messaging, PDAs and smartphones, thumb drives, CDs and DVDs, Internet browsers, and personally owned devices.[135] Employees are also reminded of these issues through the Department's required annual Cybersecurity Awareness course.[136] Further, in 2005 DS's Cyber Threat Analysis Division (CTAD) began issuing notices to Department computer users specifically highlighting cybersecurity threats. For example, CTAD's

[131] 12 FAM 544.2 (November 4, 2005).

[132] 5 FAM 443.7 (October 23, 2015).

[133] *See Cyber Insecurity: Hackers Are Penetrating Federal Systems And Critical Infrastructure: Hearing Before the House Committee on Homeland Security, Subcommittee On Emerging Threats, Cybersecurity And Science And Technology*, 110th Congress (2007) (statement of Donald Reid, Senior Coordinator for Security Infrastructure, Bureau of Diplomatic Security, U.S. Department of State), at 13-15.

[134] 04 STATE 204864 (September 22, 2004).

[135] *See e.g.,* 05 STATE 096534 (May 2005); *Prohibition Against Use of Privately Owned Software/Hardware on Department Automated Information Systems*, Announcement No. 2006_01_074 (January 24, 2006); *Use Of Unclassified/SBU Thumb Drives*, Announcement No. 2008_09_046 (September 9, 2008); *Using PEDs Abroad,* Announcement No. 2008_09_068 (September 12, 2008); *Remote Accessing and Processing*, Announcement No. 2008_11_061 (November 14, 2008); 09 STATE 130999 (December 24, 2009); *Use of Non-Department Owned Personal Digital Assistants (PDAs) and Smartphones in Department Facilities*, Announcement No. 2010_10_150 (October 26, 2010).

[136] 5 FAM 845 (July 12, 2013).

notices from 2005 to 2011 addressed BlackBerry security vulnerabilities, generally citing mobile devices as a weak link in computer networks.[137] CTAD warned that BlackBerry devices must be configured in accordance with the Department's security guidelines.

In July 2005, IRM introduced its BlackBerry service that provided domestic users access to their OpenNet email, calendar, and contacts.[138] From the beginning, the BlackBerry servers were required to be configured in accordance with the current DS Information Technology Security Guide, which contains an extensive list of security settings that lock down the devices. These security standards continue to apply to current Department BlackBerry devices.

In March 2009, after unsuccessful efforts to supply Secretary Clinton with a secure government smartphone, DS was informed that Secretary Clinton's staff had been asking to use BlackBerry devices inside classified areas. The Assistant Secretary of DS then sent a classified memorandum to Secretary Clinton's Chief of Staff that described the vulnerabilities associated with the use of BlackBerry devices and also noted the prohibition on the use of Blackberry devices in sensitive areas. According to a DS official, shortly after the memorandum was delivered, Secretary Clinton approached the Assistant Secretary and told him she "gets it."

The use of personal email accounts to conduct official business has been a particular concern over the past several years. For example, on March 11, 2011, the Assistant Secretary for Diplomatic Security sent a memorandum on cybersecurity threats directly to Secretary Clinton.[139] A portion of the unclassified version of this memorandum states:

> Threat analysis by the DS cyber security team and related incident reports indicate a dramatic increase since January 2011 in attempts by [redacted] cyber actors to compromise the private home e-mail accounts of senior Department officials. … Although the targets are unclassified, personal e-mail accounts, the likely objective is to compromise user accounts and thereby gain access to policy documents and personal information that could enable technical surveillance and possible blackmail. The personal e-mail of family members also is at risk.

The memorandum included as an attachment "a snapshot of affected Department personnel," noting that many of the email account owners play major roles in forming diplomatic and economic policy.[140] It concluded by noting, "We also urge Department users to minimize the use

[137] *See, e.g.,* CTAD, *Cyber Security Awareness* (March 3, 2011).

[138] Department of State, *Blackberry Wireless PDA Use in the Department of State*, Announcement No. 2005_07_018, July 7, 2005. This announcement also notes: "Personal Blackberry devices are not allowed." In September 2005, overseas posts were also authorized to procure, install, and operate their own BlackBerry Enterprise Server (BES) and BlackBerry devices. 05 STATE 172062 (September 2005).

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

[140] Spear phishing was one of the several types of threats included in the Memorandum. It is an attack on a single user or department within an organization, such as asking employees to update their username and passwords. Once

of personal web email for business, as some compromised home systems have been reconfigured by these actors to automatically forward copies of all composed emails to an undisclosed recipient."

Following the March 2011 memorandum, DS cybersecurity staff conducted two cybersecurity briefings of S/ES staff, the Secretary's immediate staff, and Bureau of Public Affairs staff in April and May 2011. OIG discovered in Secretary Clinton's retired paper files a copy of the classified presentation used during the briefing. It contains material similar to the type provided in the March 11, 2011, memorandum.

On June 28, 2011, the Department, in a cable entitled "Securing Personal E-mail Accounts" that was approved by the Assistant Secretary for Diplomatic Security and sent over Secretary Clinton's name to all diplomatic and consular posts, encouraged Department users "to check the security settings and change passwords of their home e-mail accounts because of recent targeting of personal email accounts by online adversaries."[141] The cable further elaborated that "recently, Google asserted that online adversaries are targeting the personal Gmail accounts of U.S. government employees. Although the company believes it has taken appropriate steps to remediate identified activity, users should exercise caution and follow best practices in order to protect personal e-mail and prevent the compromise of government and personal information." It then recommended best practices for Department users and their family members to follow, including "avoid conducting official Department business from your personal e-mail accounts."[142]

Three Officials Exclusively Used Non-Departmental Systems for Day-to-Day Operations

Cybersecurity risks demonstrate the need both for restrictions on the use of non-Departmental systems and for requirements to seek approval before using such systems. A senior IRM official

---

hackers obtain this information, they can easily access entry into secured networks. Another example of spear phishing is asking users to click on a link, which deploys spyware.

[141] 11 STATE 65111 (June 28, 2011).

[142] That portion of the cable reads in full as follows:

> 3. What can you and your family members do?
>
> (a) Follow the personal e-mail guides posted on the Awareness site to change your password, to ensure that messages are not auto-forwarding to an unintended address, and to verify that other security settings are properly configured.
>
> (b) Beware of e-mail messages that include links to password reset web pages. These can be easily faked.
>
> (c) Create strong passwords for all of your online accounts, change them often, and never use the same password for more than one account.
>
> (d) Avoid conducting official Department business from your personal e-mail accounts.
>
> (e) Do not reveal your personal e-mail address in your work "Out of Office" message.
>
> (f) Do not auto-forward Department e-mail to personal e-mail accounts, which is prohibited by Department policy (12 FAM 544.3).

reported to OIG that many Department employees have requested to use non-Departmental systems to conduct business; examples include requests to use outside video conferencing systems and file sharing software. According to this official, the Department typically refuses such requests. For instance, in 2012, Department staff submitted a request to IRM to use an Internet-based teleconference service. In response, IRM cited the 2005 FAM provision (12 FAM 544.3) requiring that normal day-to-day operations be conducted on an authorized AIS and further noted that the Department "expect[s] employees to use the tools provided by the Department to protect sensitive information from unauthorized access or disclosure" and only permits the use of non-Departmental systems "when absolutely necessary." Other employees have sought to use Dropbox, a cloud-based file hosting service, but IRM has blocked access to the site on OpenNet since 2011 because of the risk of unauthorized access to Department data. The senior IRM official told OIG that the Department seldom encounters "an 'absolutely necessary' condition that would lead to approval for non-emergency processing/transmission of Department work outside [the Department's] network."

OIG identified many examples of staff using personal email accounts to conduct official business; however, OIG could only identify three cases where officials used non-Departmental systems on an exclusive basis for day-to-day operations. These include former Secretaries Powell and Clinton, as well as Jonathan Scott Gration, a former Ambassador to Kenya. Although the former Ambassador was not a member of the Office of the Secretary, the Department's response to his actions demonstrates how such usage is normally handled when Department cybersecurity officials become aware of it. The facts and circumstances surrounding each of these cases are discussed below:

Secretary Powell: Secretary Powell has acknowledged using a personal email account from a commercial Internet provider, which he accessed on a "private line" in his Department office. He further stated that he had two computers at his desk: "a secure State Department machine … used for secure material, and…a laptop [used] for email."[143] Neither the Secretary nor his representative could recall whether Secretary Powell owned the laptop or whether the Department provided it to him. However, the Secretary characterized the use of the laptop as his "unclassified system," which was not connected to OpenNet. In his interview with OIG, Secretary Powell explained that, when he arrived at the Department, the email system in place only permitted communication among Department staff. He therefore requested that information technology staff install the private line so that he could use his personal account to communicate with people outside the Department.[144] He described his email usage as "daily," though OIG was unable to determine how many emails he actually sent and received during his tenure.

[143] *Meet the Press* (NBC television broadcast September 6, 2015) (interview with Colin Powell), available at http://www.nbcnews.com/meet-the-press/meet-press-transcript-september-6-2015-n422606.

[144] Secretary Powell also acknowledged using his personal account to communicate with Department employees. *Meet the Press* (NBC television broadcast September 6, 2015) (interview with Colin Powell).

Various DS and IRM staff told OIG that, before Secretary Powell arrived at the Department, employees did not have Internet connectivity on their desktop computers. The Department's Chief Information Officer (CIO) and Under Secretary for Management during Secretary Powell's tenure reported to OIG that they were aware of Secretary Powell's use of a personal email account and also noted the Secretary's goal was to provide every Department employee with similar Internet and email capabilities at their desktops. The current CIO and Assistant Secretary for Diplomatic Security, who were Department employees during Secretary Powell's tenure, also were both aware of the Secretary's use of a personal email account and recall numerous discussions with senior staff throughout the Department about how to implement the Secretary's intent to provide all employees with Internet connectivity.

However, it is not clear whether staff explicitly addressed restrictions on the use of non-Departmental systems with Secretary Powell. For example, at the beginning of Secretary Powell's tenure, the Department had an outright prohibition on both the installation of privately owned computers in Department facilities and the transmission of SBU information on the Internet.[145] By 2002, the Department had established the requirement to connect to the Internet only on OpenNet.[146] The CIO and Under Secretary for Management during Secretary's Powell's tenure reported to OIG that they believe that these issues were addressed, either by installing a firewall to protect the Secretary's Internet connection or providing the Secretary with a Department laptop. They also reported having multiple discussions with Secretary Powell about the Department's implementation of FISMA requirements. In contrast, current DS and IRM officials who worked at the Department during Secretary Powell's tenure are unsure about the exact configuration of Secretary Powell's systems and whether staff addressed applicable restrictions with the Secretary. However, they reported to OIG that the Department's technology and information security policies were very fluid during Secretary Powell's tenure and that the Department was not aware at the time of the magnitude of the security risks associated with information technology.

Secretary Clinton: By Secretary Clinton's tenure, the Department's guidance was considerably more detailed and more sophisticated. Beginning in late 2005 and continuing through 2011, the Department revised the FAM and issued various memoranda specifically discussing the obligation to use Department systems in most circumstances and identifying the risks of not doing so. Secretary Clinton's cybersecurity practices accordingly must be evaluated in light of these more comprehensive directives.

Secretary Clinton used mobile devices to conduct official business using the personal email account on her private server extensively, as illustrated by the 55,000 pages of material making up the approximately 30,000 emails she provided to the Department in December 2014. Throughout Secretary Clinton's tenure, the FAM stated that normal day-to-day operations

[145] 12 FAM 625.2-1 (April 12, 1996); 5 FAM 751.2 (February 27, 2002).

[146] 5 FAM 871 (December 30, 2002).

should be conducted on an authorized AIS,[147] yet OIG found no evidence that the Secretary requested or obtained guidance or approval to conduct official business via a personal email account on her private server. According to the current CIO and Assistant Secretary for Diplomatic Security, Secretary Clinton had an obligation to discuss using her personal email account to conduct official business with their offices, who in turn would have attempted to provide her with approved and secured means that met her business needs. However, according to these officials, DS and IRM did not—and would not—approve her exclusive reliance on a personal email account to conduct Department business, because of the restrictions in the FAM and the security risks in doing so.

During Secretary Clinton's tenure, the FAM also instructed employees that they were expected to use approved, secure methods to transmit SBU information and that, if they needed to transmit SBU information outside the Department's OpenNet network on a regular basis to non-Departmental addresses, they should request a solution from IRM.[148] However, OIG found no evidence that Secretary Clinton ever contacted IRM to request such a solution, despite the fact that emails exchanged on her personal account regularly contained information marked as SBU.

Similarly, the FAM contained provisions requiring employees who process SBU information on their own devices to ensure that appropriate administrative, technical, and physical safeguards are maintained to protect the confidentiality and integrity of records and to ensure encryption of SBU information with products certified by NIST.[149] With regard to encryption, Secretary Clinton's website states that "robust protections were put in place and additional upgrades and techniques employed over time as they became available, including consulting and employing third party experts."[150] Although this report does not address the safety or security of her system, DS and IRM reported to OIG that Secretary Clinton never demonstrated to them that her private server or mobile device met minimum information security requirements specified by FISMA and the FAM.

In addition to interviewing current and former officials in DS and IRM, OIG interviewed other senior Department officials with relevant knowledge who served under Secretary Clinton, including the Under Secretary for Management, who supervises both DS and IRM; current and former Executive Secretaries; and attorneys within the Office of the Legal Adviser. These officials all stated that they were not asked to approve or otherwise review the use of Secretary Clinton's server and that they had no knowledge of approval or review by other Department staff. These officials also stated that they were unaware of the scope or extent of Secretary Clinton's use of a personal email account, though many of them sent emails to the Secretary on this account. Secretary Clinton's Chief of Staff also testified before the House Select Committee on Benghazi that she was unaware of anyone being consulted about the Secretary's exclusive use of a

[147] 12 FAM 544.3 (November 4, 2005).

[148] 12 FAM 544.2 (November 4, 2005).

[149] 12 FAM 682 (August 4, 2008).

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

personal email address.[151] OIG did find evidence that various staff and senior officials throughout the Department had discussions related to the Secretary's use of non-Departmental systems, suggesting there was some awareness of Secretary Clinton's practices. For example:

- In late-January 2009, in response to Secretary Clinton's desire to take her BlackBerry device into secure areas, her Chief of Staff discussed with senior officials in S/ES and with the Under Secretary for Management alternative solutions, such as setting up a separate stand-alone computer connected to the Internet for Secretary Clinton "to enable her to check her emails from her desk." The Under Secretary's response was "the stand-alone separate network PC is [a] great idea" and that it is "the best solution." According to the Department, no such computer was ever set up.

- In November 2010, Secretary Clinton and her Deputy Chief of Staff for Operations discussed the fact that Secretary Clinton's emails to Department employees were not being received. The Deputy Chief of Staff emailed the Secretary that "we should talk about putting you on state email or releasing your email address to the department so you are not going to spam." In response, the Secretary wrote, "Let's get separate address or device but I don't want any risk of the personal being accessible."[152]

- In August 2011, the Executive Secretary, the Under Secretary for Management, and Secretary Clinton's Chief of Staff and Deputy Chief of Staff, in response to the Secretary's request, discussed via email providing her with a Department BlackBerry to replace her personal BlackBerry, which was malfunctioning, possibly because "her personal email server is down." The then-Executive Secretary informed staff of his intent to provide two devices for the Secretary to use: "one with an operating State Department email account (which would mask her identity, but which would also be subject to FOIA requests), and another which would just have phone and internet capability." In another email exchange, the Director of S/ES-IRM noted that an email account and address had already

[151]The pertinent testimony from the former Chief of Staff, who declined OIG's request for an interview, reads as follows:

Q Was anyone consulted about Secretary Clinton exclusively using a personal email address for her work?
A I don't recall that. If it did happen, I wasn't part of that process. But I don't believe there was a consultation around it, or at least there's not one that I'm aware of, maybe I should better answer that way based on my knowledge.
Q So no private counsel?
A Not that I'm aware of.
Q Okay. The general counsel for the State Department?
A Not that I'm aware of.
Q Okay. Anybody from the National Archives?
A Not that I'm aware of. But I can only speak to my knowledge, obviously.
Q Sure. And anyone from the White House?
A Not that I'm aware of.

[152] Secretary Clinton declined OIG's request for an interview. The former Deputy Chief of Staff for Operations has not responded to OIG's request for an interview.

been set up for the Secretary[153] and also stated that "you should be aware that any email would go through the Department's infrastructure and subject to FOIA searches."[154] However, the Secretary's Deputy Chief of Staff rejected the proposal to use two devices, stating that it "doesn't make a whole lot of sense." OIG found no evidence that the Secretary obtained a Department address or device after this discussion.

- OIG identified two individuals who provided technical support to Secretary Clinton. The first, who was at one time an advisor to former President Clinton but was never a Department employee, registered the clintonemail.com domain name on January 13, 2009.[155] The second, a Schedule C political appointee who worked in IRM as a Senior Advisor from May 2009 through February 2013,[156] provided technical support for BlackBerry communications during the Secretary's 2008 campaign for President.[157] OIG reviewed emails showing communications between Department staff and both individuals concerning operational issues affecting the Secretary's email and server from 2010 through at least October 2012. For example, in December 2010, the Senior Advisor worked with S/ES-IRM and IRM staff to resolve issues affecting the ability of emails transmitted through the clintonemail.com domain used by Secretary Clinton to reach Department email addresses using the state.gov domain.[158]

[153] According to the Department, this account was only used by Secretary Clinton's staff to maintain an Outlook calendar.

[154] The former Director of S/ES-IRM declined OIG's request for an interview.

[155] The clintonemail.com domain name was registered with Network Solutions Certificate Authority on January 13, 2009 and identifies the advisor to former President Clinton as the registrant.

[156] Schedule C appointments are those of a "confidential or policy-determining character" 5 C.F.R. § 6.2.

[157] Secretary Clinton's counsel advised OIG that the Senior Advisor "performed technology services for the Clinton family for which he was compensated" by check or wire transfer in varying amounts and various times between 2009 and 2013. In addition, the Senior Advisor's direct supervisors in IRM from 2009 to 2013 told OIG they were unaware of his technical support of the Secretary's email system. While working at the Department, the Senior Advisor reported directly to the Deputy Chief Information Officer (DCIO) for Operations, who in turn reported to the Chief Information Officer (CIO). The DCIO and CIO, who prepared and approved the Senior Advisor's annual evaluations, believed that the Senior Advisor's job functions were limited to supporting mobile computing issues across the entire Department. They told OIG that while they were aware that the Senior Advisor had provided IT support to the Clinton Presidential campaign, they did not know he was providing ongoing support to the Secretary's email system during working hours. They also told OIG that they questioned whether he could support a private client during work hours, given his capacity as a full-time government employee.

[158] At that time, S/ES IRM staff met with the Senior Advisor, who accessed the Secretary's email system and looked at its logs. The issue was ultimately resolved and, on December 21, 2010, S/ES-IRM staff sent senior S/ES staffers an email describing the issue and summarizing the activities undertaken to resolve it. On another occasion, the Senior Advisor met with staff within CTAD and received a briefing on cyber security risks facing the Department. A third interaction took place on October 30, 2012, during the period when Hurricane Sandy disrupted power in the New York City area. An email exchange between Deputy Chief of Staff for Operations and another member of the Secretary's staff revealed that the server located in Secretary Clinton's New York residence was down. Thereafter, the Senior Advisor met with S/ES-IRM staff to ascertain whether the Department could provide support for the server. S/ES-IRM staff reported to OIG that they told the Senior Advisor they could not provide support because it was a private server.

- Two staff in S/ES-IRM reported to OIG that, in late 2010, they each discussed their concerns about Secretary Clinton's use of a personal email account in separate meetings with the then-Director of S/ES-IRM. In one meeting, one staff member raised concerns that information sent and received on Secretary Clinton's account could contain Federal records that needed to be preserved in order to satisfy Federal recordkeeping requirements. According to the staff member, the Director stated that the Secretary's personal system had been reviewed and approved by Department legal staff and that the matter was not to be discussed any further. As previously noted, OIG found no evidence that staff in the Office of the Legal Adviser reviewed or approved Secretary Clinton's personal system. According to the other S/ES-IRM staff member who raised concerns about the server, the Director stated that the mission of S/ES-IRM is to support the Secretary and instructed the staff never to speak of the Secretary's personal email system again.

- On January 9, 2011, the non-Departmental advisor to President Clinton who provided technical support to the Clinton email system notified the Secretary's Deputy Chief of Staff for Operations that he had to shut down the server because he believed "someone was trying to hack us and while they did not get in i didnt [sic] want to let them have the chance to." Later that day, the advisor again wrote to the Deputy Chief of Staff for Operations, "We were attacked again so I shut [the server] down for a few min." On January 10, the Deputy Chief of Staff for Operations emailed the Chief of Staff and the Deputy Chief of Staff for Planning and instructed them not to email the Secretary "anything sensitive" and stated that she could "explain more in person."[159]

Ambassador Gration: Ambassador Gration served as the U.S. Ambassador to Kenya from mid-2011 through mid-2012. OIG first publicly reported on the activities of Ambassador Gration as part of its 2012 inspection of Embassy Nairobi.[160] Prior to the inspection, in June 2011, DS learned that the newly posted Ambassador had drafted and distributed a revised mission policy concerning communications security that authorized him and other mission personnel to use commercial email for daily communication of official government business. That prompted senior DS management and cybersecurity staff to email the Ambassador to advise him that DS was dispatching an experienced Regional Computer Security Officer to provide expertise and

[159] In another incident occurring on May 13, 2011, two of Secretary Clinton's immediate staff discussed via email the Secretary's concern that someone was "hacking into her email" after she received an email with a suspicious link. Several hours later, Secretary Clinton received an email from the personal account of then-Under Secretary of State for Political Affairs that also had a link to a suspect website. The next morning, Secretary Clinton replied to the email with the following message to the Under Secretary: "Is this really from you? I was worried about opening it!" Department policy requires employees to report cybersecurity incidents to IRM security officials when any improper cyber-security practice comes to their attention. 12 FAM 592.4 (January 10, 2007). Notification is required when a user suspects compromise of, among other things, a personally owned device containing personally identifiable information. 12 FAM 682.2-6 (August 4, 2008). However, OIG found no evidence that the Secretary or her staff reported these incidents to computer security personnel or anyone else within the Department.

[160] ISP-I-12-38A (August 2012).

advice in establishing procedures for handling SBU information that adhered to Department standards for the processing of sensitive material. DS further noted that this visit would be "especially timely in the wake of recent headlines concerning a significant hacking effort directed against the private, web-based email accounts of dozens of senior USG officials, which has generated substantial concern from the Secretary, Deputy Secretary Steinberg, and other Department principals." Notwithstanding the Department's concerns, the Ambassador continued to use commercial email for official business.

DS then notified the Ambassador via cable on July 20, 2011, that the FAM did not permit him to use non-government email for day-to-day operations.[161] The cable stated in relevant part:

> The language in 12 FAM 544.3, which states that "it is the Department's general policy that normal day-to-day operations be conducted on an authorized [automated information system]" is purposely included to place employees on notice that if they are given a tool that provides an adequate level of security encryption, such as an OpenNet terminal … or any other Department-supplied security mechanism that works in the given circumstance, they must use it. 12 FAM 544.3 goes on to say that in the absence of a Department-supplied security solution employees can send most SBU information unencrypted via the internet only when necessary, with the knowledge that the nature of the transmission lends itself to unauthorized access, however remote that chance might be. … Given the threats that have emerged since 2005, especially in regard to phishing and spoofing of certain web-based email accounts, we cannot allow the proliferation of this practice beyond maintaining contact during emergencies. We are all working toward the same end—to protect the availability, integrity and confidentiality of Department information and systems, while recognizing that emergency situations may arise, particularly for our employees serving overseas. … The Department is not aware of any exigent circumstances in Nairobi that would authorize a deviation from the requirement to use Department systems for official business.

However, the Ambassador continued to use unauthorized systems to conduct official business. The Department subsequently initiated disciplinary proceedings against him for his failure to follow these directions and for several other infractions, but he resigned before any disciplinary measures were imposed.

OIG could find no other instances where the Department initiated disciplinary procedures against a senior official for using non-Departmental systems for day-to-day operations.

[161] 11 STATE 73417 (July 20, 2011).

CONCLUSION

Longstanding, systemic weaknesses related to electronic records and communications have existed within the Office of the Secretary that go well beyond the tenure of any one Secretary of State. OIG recognizes that technology and Department policy have evolved considerably since Secretary Albright's tenure began in 1997. Nevertheless, the Department generally and the Office of the Secretary in particular have been slow to recognize and to manage effectively the legal requirements and cybersecurity risks associated with electronic data communications, particularly as those risks pertain to its most senior leadership. OIG expects that its recommendations will move the Department steps closer to meaningfully addressing these risks.

RECOMMENDATIONS

To ensure compliance with Federal and Department requirements regarding records preservation and use of non-Departmental systems, OIG has issued the following recommendations to the Bureau of Administration, the Office of the Secretary, the Bureau of Information Resources Management, the Bureau of Human Resources, and the Department's Transparency Coordinator. Their complete responses can be found in Appendix B. The Department also provided technical comments that OIG incorporated as appropriate into this report.

Recommendation 1: The Bureau of Administration should

- continue to issue guidance, including periodic, regular notices, to Department employees to remind them that the use of personal email accounts to conduct official business is discouraged in most circumstances,
- clarify and give specific examples of the types of limited circumstances in which such use would be permissible, and
- instruct employees how to preserve Federal records when using personal email accounts.

Management Response: In its May 23, 2016, response, the Bureau of Administration concurred with this recommendation. It will continue to issue guidance on records management practices and policies, and will ensure that this guidance explicitly reminds employees that the use of personal emails accounts to conduct official business is discouraged.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation of this additional guidance.

Recommendation 2: The Bureau of Administration should amend the *Foreign Affairs Manual* to reflect the updates to Department recordkeeping systems that provide alternatives to print and file emails that constitute Federal records.

Management Response: In its May 23, 2016, response, the Bureau of Administration concurred with this recommendation. It noted that it is currently working with the Transparency Coordinator to update sections of the FAM related to the Department's recordkeeping/retention schedules, with a goal to eliminate the practice of print and file as the Department's policy for the retention of emails by December 31, 2016.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation of the amendment.

Recommendation 3: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to conduct an inventory of all electronic and hard-copy files in its custody and evaluate them to determine which files should be transferred to the Office of Information Programs and Services in accordance with records disposition schedules or Department email preservation requirements.

Management Response: In its May 16, 2016, response, the Executive Secretariat concurred with this recommendation. It noted that the inventory of electronic and hard copy files has been ongoing since January 2016 and that once it is complete, the Executive Secretariat will retire all such records according to applicable records schedules.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that this effort has been completed.

Recommendation 4: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to improve policies and procedures to promote compliance by all employees within its purview, including the Secretary, with records management requirements. These policies should cover the retirement of records in accordance with records disposition schedules, preservation of email and other electronic records of departing officials, and training of employees on their records preservation responsibilities.

Management Response: In its May 16, 2016, response, the Executive Secretariat concurred with this recommendation. It noted that it is committed to coordinating closely with the Office of Information Programs and Services to provide updated guidance and training to all staff.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts a copy of the policies and procedures.

Recommendation 5: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to ensure that all departing officials within its purview, including the Secretary of State, sign a separation form (DS-109) certifying that they have surrendered all Federal records and classified or administratively controlled documents. In addition, staff should ensure that all incoming officials within its purview, including the Secretary, are thoroughly briefed on their records preservation and retention responsibilities, including records contained on personal email accounts.

Management Response: In its May 16, 2016, response, the Executive Secretariat concurred with this recommendation. It noted that it is instituting a process whereby completed DS-109 forms are placed in the employee's permanent electronic performance files to ensure they are easily accessible.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation of this process.

Recommendation 6: The Department's Transparency Coordinator should work with the Office of Information Programs and Services to develop a quality assurance plan to promptly identify and address Department-wide vulnerabilities in the records preservation process, including lack of oversight and the broad inaccessibility of electronic records.

Management Response: In her May 16, 2016, response, the Transparency Coordinator concurred with this recommendation. She noted that this plan will be part of her continuing efforts, in coordination with the Office of Information Programs and Services and the Executive Secretariat, to improve overall governance of the Department's information, including how it is captured, stored, shared, disposed of, and archived.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts a copy of the quality assurance plan.

Recommendation 7: The Bureau of Information Resource Management should

- issue regular notices to remind Department employees of the risks associated with the use of non-Departmental systems;
- provide periodic briefings on such risks to staff at all levels; and
- evaluate the cost and feasibility of conducting regular audits of computer system usage to ascertain the degree to which Department employees are following the laws and policies concerning the use of personal email accounts.

Management Response: In its May 23, 2016, response, the Bureau of Information Resource Management concurred with this recommendation. It noted that it will continue to issue regular notices regarding the risks associated with the use of non-Departmental systems. With regard to the evaluation of the cost and feasibility of regular computer system audits, the Bureau has considered such an effort but has concluded that audits conducted on such a wide scale would not be beneficial or feasible, especially because the Department already conducts continuous monitoring to ensure the integrity of the Department's networks and systems.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation of additional educational efforts.

Recommendation 8: The Director General of the Foreign Service and Director of Human Resources should amend the *Foreign Affairs Manual* to provide for administrative penalties for Department employees who (1) fail to comply with recordkeeping laws and regulations or (2) fail to comply with Department policy that only authorized information systems are to be used to conduct day-to-day operations. The amendment should include explicit steps employees should take if a reasonable suspicion exists that documents are not being preserved appropriately, including a reminder that the Office of Inspector General has jurisdiction to investigate and refer to appropriate authorities suspected violations of records preservation requirements.

Management Response: In its May 23, 2016, response, the Department concurred with this recommendation. It will revise the FAM accordingly. The Department also noted that under 3 FAM 4370, it currently has authority to discipline violations of any administrative regulations that do not provide a penalty.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation of the revision.

APPENDIX A: RELEVANT LAWS AND POLICIES DURING THE TENURES OF THE FIVE MOST RECENT SECRETARIES OF STATE

Madeleine Albright (January 23, 1997 – January 20, 2001)

***Foreign Affairs Manual* (FAM) and *Foreign Affairs Handbook* (FAH) Requirements for Use of Non-Departmental Systems:** Since 1996, the FAM directed Department of State (Department) systems managers to ensure that privately owned computers were not installed or used in any Department office building.[1]

Applicable Cybersecurity Provisions and Related Guidance: In 1988, Congress enacted the Computer Security Act to require all Federal agencies to identify computer systems containing sensitive information, conduct computer security training, and develop computer security plans.[2] Office of Management and Budget (OMB) Circular A-130 (Appendix III) required Federal agencies to establish security programs containing specified elements, including development of a System Security Plan, assignment of responsibility for security to individuals knowledgeable in information security technology, and regular review of information system security controls. The FAM did not contain specific computer or cybersecurity provisions.

Statutory and Regulatory Requirements for Email Records Preservation: The Federal Records Act of 1950 requires the head of every Federal agency to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency."[3] The agency head is also required to establish and maintain an active, continuing program for the economical and efficient management of agency records that provides for:

- Effective controls over the creation and the maintenance and use of records in the conduct of current business;
- Cooperation with the Archivist in applying standards, procedures, and techniques designed to improve the management of records, promote the maintenance and security of records deemed appropriate for preservation, and facilitate the segregation and disposal of records of temporary value; and
- Compliance with Federal law and regulations.[4]

As part of this program, the agency head must establish safeguards against the removal or loss of records, including making it known to agency employees that agency records may not be

[1] 12 FAM 625.2-1 (April 12, 1996).

[2] Pub. L. No. 100-235 (January 8, 1988).

[3] 44 U.S.C. § 3101.

[4] 44 U.S.C. § 3102. 44 U.S.C. § 3102(3) specifically references "compliance with sections 2101-2117, 2501-2507, 2901-2909, and 3101-3107, of this title and the regulations issued under them."

unlawfully alienated or destroyed and that penalties exist for the unlawful removal or destruction of records.[5] The agency head must notify the Archivist of any actual, impending, or threatened unlawful removal, defacing, alteration, corruption, deletion, erasure, or other destruction of records in the agency's custody.[6] The Federal Records Act define records broadly as

> all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government … or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.[7]

The regulations issued by the National Archives and Records Administration (NARA) in title 36 of the Code of Federal Regulations (C.F.R.) that were in effect during Secretary Albright's tenure specified actions that must be taken by an agency in establishing a records program. These included:

- Assigning an office the responsibility for the development and implementation of agency-wide programs to identify, develop, issue, and periodically review recordkeeping requirements for records for all agency activities at all levels and locations in all media including paper, microform, audiovisual, cartographic, and electronic (including those created or received using electronic mail);
- Integrating programs for the identification, development, issuance, and periodic review of recordkeeping requirements with other records and information resources management programs of the agency;
- Issuing a directive establishing program objectives, responsibilities, and authorities for agency recordkeeping requirements;
- Establishing procedures for the participation of records management officials in developing new or revised agency programs, processes, systems, and procedures in order to ensure that adequate recordkeeping requirements are established and implemented;
- Ensuring that adequate training is provided to all agency personnel on policies, responsibilities, and techniques for the implementation of recordkeeping requirements and the distinction between records and non-record materials, regardless of media, including those materials created by individuals using computers to send or receive electronic mail;

[5] 44 U.S.C. § 3105.

[6] 44 U.S.C. § 3106.

[7] 44 U.S.C. § 3301 (amended 2014). The regulations stated that the medium may be "paper, film, disk, or other physical type or form" and that the method of recording may be "manual, mechanical, photographic, electronic, or any other combination of these or other technologies." 36 C.F.R. § 1222.12(b)(2) (1990).

- Developing and implementing records schedules for all records created and received by the agency;
- Reviewing recordkeeping requirements, as part of the periodic information resources management reviews; and
- Reminding all employees annually of the agency's recordkeeping policies and of the sanctions provided for the unlawful removal or destruction of Federal records.[8]

The regulations explicitly noted that "messages created or received on electronic mail systems may meet the definition of record."[9] Furthermore, the regulations required agencies to develop procedures to ensure that departing officials do not remove Federal records from agency custody.[10] The regulations gave further guidance as to what constitutes a Federal record, specifying that records are those documents that:

- Document the persons, places, things, or matters dealt with by the agency;
- Facilitate action by agency officials and their successors in office;
- Make possible a proper scrutiny by the Congress or other duly authorized agencies of the Government;
- Protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions;
- Document the formulation and execution of basic policies and decisions and the taking of necessary actions, including all significant decisions and commitments reached orally; or
- Document important board, committee, or staff meetings.[11]

The regulations issued by NARA included separate provisions on electronic records management, including email.[12] The requirements for electronic records management largely matched those for general records management, but they did require integrating electronic records management with other records and information resources management and ensuring that adequate training is provided for users of electronic mail systems on recordkeeping requirements.[13] The management of email records had to include instructions on preservation of data regarding transmission, calendar and task lists, and acknowledgements.[14] Agencies were restricted from storing the recordkeeping copy of email messages solely on the electronic mail

[8] 36 C.F.R. § 1222.20 (1995).

[9] 36 C.F.R. § 1222.34(e) (1995). Even prior to the issuance of this provision, emails would have been considered a Federal record based on the broad definition of "record" in the Federal Records Act. 44 U.S.C. § 3301.

[10] 36 C.F.R. § 1222.40 (1990). Even for non-records, the regulations permit removal only with the approval of the head of the agency or the individual authorized to act for the agency on matters pertaining to agency records. 36 C.F.R. § 1222.42.

[11] 36 C.F.R. § 1222.38 (1990).

[12] 36 C.F.R. part 1234 (1995).

[13] 36 C.F.R. § 1234.10 (1995).

[14] 36 C.F.R. § 1234.24(a) (1995).

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

The regulations also noted that the use of external communications systems to which an agency has access, but which are neither owned nor controlled by the agency, does not alter in any way the agency's obligation under the Federal Records Act. Specifically, the regulations provided that

> agencies with access to external electronic mail systems shall ensure that Federal records sent or received on these systems are preserved in the appropriate recordkeeping system and that reasonable steps are taken to capture available transmission and receipt data needed by the agency for recordkeeping purposes.[17]

The regulations also focused on the security of electronic records, requiring an effective records security program that ensures that only authorized personnel have access to electronic records; provides for backup and recovery of records; ensures that appropriate agency personnel are trained to safeguard sensitive or classified electronic records; minimizes the risk of unauthorized alteration or erasure of electronic records; and ensures that electronic records security is included in computer systems security plans.[18]

FAM and FAH Requirements for Email Records Preservation: The FAM largely mirrored the statutory requirements. It created a Records Management Program headed by the Chief of the Records Management Branch within the Bureau of Administration (A).[19] The FAM required that all official files must remain in the custody of the Department and must be maintained in accordance with the *Records Management Handbook,* and it prohibited Department employees from improperly removing, retiring, transferring, or destroying Department records.[20] The FAM noted that it is the responsibility of all Department employees and contractors to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the Department."[21]

The FAM emphasized that "all employees must be aware that some of the variety of the messages being exchanged on E-mail are important to the Department and must be preserved; such messages are considered Federal records under the law."[22] It gave examples of emails that could constitute agency records, such as email providing key substantive comments on a draft

[15] 36 C.F.R. § 1234.24(b)(2) (1995).

[16] 36 C.F.R. § 1234.24(d) (1995).

[17] 36 C.F.R. § 1234.24(a)(4) (1995).

[18] 36 C.F.R. § 1234.28 (1995).

[19] 5 FAM 413.1 (October 30, 1995).

[20] 5 FAM 422.1 (October 30, 1995); 5 FAM 423.1 (October 30, 1995).

[21] 5 FAM 413.10 (October 30, 1995).

[22] 5 FAM 443.1(c) (October 30, 1995).

action memorandum; email providing documentation of significant Department decisions and commitments reached orally; and email conveying information of value on important Department activities, such as data on significant programs specially compiled by posts in response to a Department solicitation.[23] The FAM gave instructions on how to preserve email records, noting that

> until technology allowing archival capabilities for long-term electronic storage and retrieval of E-mail messages is available and installed, those messages warranting preservation as records (for periods longer than current E-mail systems routinely maintain them) must be printed out and filed with related records.[24]

For departing employees, the FAM gave the administrative section of each office, bureau, or post the responsibility for reminding all employees who are about to leave the Department or the Foreign Service of the laws and regulations pertaining to the disposition of personal papers and official records; seeing that form OF-109, Separation Statement, is executed for each departing employee and is forwarded to the Office of Personnel for filing in the employee's Official Personnel Folder; and advising departing officials ranked Assistant Secretary and above, or Ambassador, to consult with the Department's Records Officer about depositing in the National Archives or a Presidential archival depository papers that they may have accumulated during their tenure and that may have historical interest.[25] Form OF-109 required the employee to certify that "I have surrendered to responsible officials all unclassified documents and papers relating to the official business of the Government acquired by me while in the employ of the Department."

Other Preservation Guidance: On February 3, 1997, at the beginning of Secretary Albright's tenure, the Office of the Secretary's Executive Secretary sent a memorandum to all Assistant Secretaries on "Records Responsibilities and Reviews." The memorandum referred to a Department Notice on the subject, as well as the Federal Records Act and 5 FAM 443, which covered email records. The memorandum stated that information maintained in email may constitute a record if it meets the statutory definition of a record and stated, "You need not preserve every e-mail message. If a record in electronic media or electronic mail must be preserved, print the files or messages and place the paper record in the appropriate official file; or continue to maintain electronically if feasible."

On July 28, 2000, a notice reminded all Department employees to preserve emails that qualify as records, stating that "those messages containing information that documents Departmental

[23] 5 FAM 443.2(d) (October 30, 1995).

[24] 5 FAM 443.3 (October 30, 1995). For emails considered records, the FAM required preserving the email message, any attachments, and transmission data such as sender, addressee, cc's, and the date and time sent. If the email system did not print this necessary data, employees were instructed to annotate the printed copies with that data.

[25] 5 FAM 413.9 (October 30, 1995).

policies, programs, and activities must be preserved in paper form." It instructed employees to print out such emails and file them with related paper records.

In August 2000, the Bureau of Administration published a Briefing Booklet for Departing Officials on "Senior Officials and Government Records" that included a signed letter from the Secretary stating that records "must be preserved to enhance our national archives and to provide accurate and complete records." The Secretary also noted that "we [senior officials] have a special obligation as the officials who welcomed in a new century and technological era to preserve e-mail messages as federal records, as appropriate."

A December 2000 cable to all ambassadors and administrative officers reminded departing officials to not remove any papers, whether personal or official, from the Department until such materials have been reviewed to ensure compliance with records laws and regulations.[26] It noted that electronic records must be preserved by printing the files or messages and placing the paper record in the appropriate official file.

Colin Powell (January 20, 2001 – January 26, 2005)

FAM and FAH Requirements for Use of Non-Departmental Systems: Beginning in December 2002, the FAM required all Department facilities to use the Department's primary Internet connection, OpenNet, to establish Internet connectivity.[27] OpenNet provided improved information management and heightened information security throughout the Department. If a bureau or post wanted an exception to this policy, it was required to request a waiver.[28]

The Department established rules in May 2004 regulating the use of non-government information systems, called Dedicated Internet Networks (DINs), to access the Internet.[29] A DIN is a stand-alone information network, such as a local network or server, with dedicated Internet access provided by a commercial Internet service provider (ISP). DINs were not to be used to carry out Department business or to transmit sensitive but unclassified (SBU) information. All bureaus and posts were required to submit a waiver to request an exception in order to use a commercial Internet connection for a stand-alone local network or server. The request for a waiver needed to contain detailed information about the network or server, including an explanation of compliance with Department's standards and specific reasons why OpenNet did not meet the requester's official business requirements. The FAM required all waivers to be approved by the Department's Information Technology Change Control Board (IT CCB).[30] According to the IT CCB, it approved approximately 180 such waivers during the first year this provision was in effect.

[26] 00 STATE 228951.

[27] 5 FAM 871 (December 30, 2002). At the time, OpenNet was referred to as "OpenNet Plus."

[28] 5 FAM 872 (December 30, 2002).

[29] 5 FAM 874.2 (May 4, 2004).

[30] 5 FAM 874.2 (May 4, 2004).

Applicable Cybersecurity Provisions and Related Guidance: The E-Government Act, signed into law in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the Act, the Federal Information Security Management Act (FISMA), gave the National Institute of Standards and Technology (NIST) responsibility to develop Federal Government information security standards and guidelines.[31]

Statutory and Regulatory Requirements for Email Records Preservation: The requirements in the Federal Records Act of 1950 and related regulations in title 36 of the C.F.R. did not change.

FAM and FAH Requirements for Email Records Preservation: The requirements in the FAM generally had not changed from Secretary Albright's tenure. However, in 2002, the Department added a section to the FAM on email usage that included a requirement that email users "determine the significance and value of information created on e-mail systems [and] determine the need to preserve those messages that qualify as records."[32] In 2004, the FAM was amended to designate the Director of the Office of Information Programs and Services (IPS) as the Department's Records Officer.[33] This amendment also noted that "email sent or received as a Department official is not personal."[34] Finally, the amendment assigned the responsibilities related to departing officials, including ensuring the OF-109 was signed, to Management Officers, but eliminated the requirement that the OF-109 be filed in the employee's personnel folder.[35]

Other Preservation Guidance: On August 9, 2004, the Executive Secretary sent a memorandum to all Under Secretaries and Assistant Secretaries entitled "Refresher on Records Responsibilities and Review." The memorandum stated that:

> Departing officials may not remove any documentary materials, whether personal or official and whether in written or electronic form, from the Department until they have been reviewed by records and security officers to ensure compliance with records laws and regulations. … In addition, departing officials must ensure that all record material they possess is incorporated in the Department's official files. … Finally, the administrative section of each office and bureau in the Department will ensure that departing officials receive a mandatory briefing and that all departing officials will execute a Separation Statement (OF-109) certifying that they have not retained in their possession classified or administratively controlled documents.

[31] E-Government Act of 2002 (Pub. L. No. 107-347), Title III, Information Security, titled Federal Information Security Management Act of 2002, 116 STAT. 2946 (December 17, 2002). NIST did not promulgate guidance on minimum security requirements until March 2006.

[32] 5 FAM 751.4 (February 27, 2002).

[33] 5 FAM 414.2 (September 17, 2004).

[34] 5 FAM 415.1 (September 17, 2004).

[35] 5 FAM 414.7 (September 17, 2004).

In December 2004, NARA issued a bulletin to remind heads of Federal agencies that official records must remain in the custody of the agency and that they must notify officials and employees that there are criminal penalties for the unlawful removal or destruction of Federal records.[36] Employees may remove extra copies of records or other work-related non-record materials when they leave the agency with the approval of a designated agency official such as the Records Officer or legal counsel. It also noted that "officials and employees must know how to ensure that records are incorporated into files or electronic recordkeeping systems, especially records that were generated electronically on personal computers." Further, the bulletin stated that, "in many cases, officials and employees intermingle their personal and official files. In those cases, the agency may need to review and approve the removal of personal material to ensure that all agency policies are properly followed."

A January 2005 cable to all embassies, posts, and offices reminded them of their responsibilities to preserve records under the Federal Records Act and noted that responsibility for implementing and administering records policies and procedures is given to the Management Section of each Department office.[37]

Condoleezza Rice (January 26, 2005 – January 20, 2009)

FAM and FAH Requirements for Use of Non-Departmental Systems: In November 2005, the FAM listed the connection of prohibited hardware or electronic devices to a Department Automated Information System (AIS) as a cybersecurity violation.[38] In 2007, the Department restated this provision to prohibit the connection of "unauthorized hardware/electronic devices to Department networks," which included non-Department-owned hardware/electronic devices.[39]

Also in November 2005, the Department adopted the policy that normal day-to-day Internet operations are to be conducted on an authorized AIS designed with the proper level of security control to provide authentication and encryption to ensure confidentiality and integrity for transmitting Departmental SBU data and information.[40] Employees with a valid business need may transmit SBU information over the Internet unencrypted so long as they carefully consider that unencrypted emails can pass through foreign and domestic controlled ISPs, putting the confidentiality and integrity of the information at risk. The FAM further specified that employees transmitting SBU information outside the Department's OpenNet network on a regular basis to the same non-Departmental email address should obtain a secure technical solution for those Internet transmissions from the Bureau of Information Resource Management (IRM).[41] The FAM

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

[37] 05 STATE 013345 (January 24, 2005).

[38] 12 FAM 592.2 (November 1, 2005).

[39] 12 FAM 592.2 (January 10, 2007).

[40] 12 FAM 544.3 (November 4, 2005).

[41] 12 FAM 544.2 (November 4, 2005).

noted that SBU information resident on personally owned computers is generally more susceptible to cyber-attacks and/or compromise than information on government-owned computers connected to the Internet.[42] All employees who possessed SBU information on personally owned computers must ensure adequate and appropriate security for the SBU information.[43]

In 2008, the Department amended the FAM to define "remote processing" as the processing of Department information on non-Department-owned systems at non-Departmental facilities.[44] Offices that allow employees to remotely process SBU information must ensure that appropriate administrative, technical, and physical safeguards are maintained to protect the confidentiality and integrity of records.[45] Employees are prohibited from storing or processing SBU information on non-Department-owned computers unless it is necessary in the performance of their duties.[46] Employees must (1) ensure that SBU information is encrypted; (2) destroy SBU information on their personally owned and managed computers and removable media when the files are no longer required; and (3) when using personally owned computers, implement and regularly update basic home security controls, including a firewall, anti-spyware, antivirus, and file-destruction applications, and if those computers are networked, also ensure the same basic controls, plus NIST-certified encryption, for all computers on the network.[47]

Also in 2008, the Department eased the FAM restriction regarding the use or installation of non-Federal-Government-owned computers in any Department facility; such use was now allowed with the written approval of the Bureau of Diplomatic Security (DS) and IRM with certain exceptions.[48]

Applicable Cybersecurity Provisions and Related Guidance: The Department implemented the Cyber Security Incident Program (CSIP) in November 2005 to improve protection of the Department's unclassified/SBU cyber infrastructure by identifying, evaluating, and assigning responsibility for breaches of cybersecurity.[49] CSIP focused on accountability of personnel for actions leading to damage or risk to Department information systems and infrastructure, even when only unclassified material or information is involved.[50] Cybersecurity incidents are defined as acts against, or failure to protect, the Department's unclassified cyber infrastructure.[51]

[42] 12 FAM 544.3 (November 4, 2005).

[43] 12 FAM 544.3 (November 4, 2005).

[44] 12 FAM 682.1 (August 4, 2008).

[45] 12 FAM 682.2-4 (August 4, 2008).

[46] 12 FAM 682.2-4 (August 4, 2008).

[47] 12 FAM 682.2-5 (August 4, 2008). Although the FAM chapter relating to remote access and processing was amended in 2009, 2011, 2014, and 2015, these basic requirements did not change.

[48] 12 FAM 625.2-1 (July 28, 2008).

[49] 12 FAM 591.1(a) (November 1, 2005).

[50] 12 FAM 591.1 (November 1, 2005).

[51] 12 FAM 592 (January 10, 2007).

Reporting cybersecurity incidents is every employee's responsibility, and each employee must be familiar with the list of cybersecurity infractions and violations.[52] Employees must inform their Information Systems Security Office and their Regional or Bureau Security Officer when any improper cybersecurity practice comes to their attention.[53] Improper security practices include personnel compromising the confidentiality of sensitive information, deliberate introduction of a malicious program code, and use of encryption to conceal an unauthorized act, such as the transfer of SBU information to an unauthorized individual.[54]

NIST was tasked with responsibility to develop Federal standards and guidelines to implement FISMA. NIST responded in February 2004 with Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, which established security categories for both information and information systems that are used in conjunction with vulnerability and threat information for assessing the risk to an organization.[55] This was followed in March 2006 by FIPS Publication 200, which specified minimum security requirements for information and information systems supporting Federal agencies. NIST's announcement of the publication of FIPS Publication 200 noted

> this standard is applicable to: (i) all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and (ii) all federal information systems other than those information systems designated as national security systems as defined in [44 U.S.C. § 3552(b)(6)].

Section 3 of FIPS 200 sets forth 17 specifications for minimum security requirements, including the following:

- The Audit and Accountability specification states: "Organizations must (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions."
- The Risk Assessment specification states: "Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational

[52] 12 FAM 592.4 (January 10, 2007).

[53] 12 FAM 592.4 (January 10, 2007).

[54] 12 FAM 592.1 and 592.2 (January 10, 2007).

[55] NIST, FIPS PUB 199: *Standards for Security Categorization of Federal Information and Information Systems* (February 2004).

information systems and the associated processing, storage, or transmission of organizational information."

- The System and Communications Protection specification states: "Organizations must (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

Federal agencies were required to comply with these standards by March 2007.[56]

In 2007, the Department adopted rules implementing these FISMA requirements, including the requirement that non-Departmental information systems that process or store bureau-sponsored Department information on behalf of the Department maintain a baseline of minimum security controls to protect Department information and information systems.[57] Key personnel identified to perform certification and accreditation of non-Departmental systems must not be involved with its development, implementation, or operation, or be under the sponsoring bureau's direct management authority.[58]

DS reported to the Office of Inspector General that, in 2005, the Bureau of Intelligence and Research (INR) issued guidance permitting BlackBerry devices to be used inside secure areas. However, in January 2006, the Office of the Director of National Intelligence issued a clear prohibition on such use, and the INR guidance was immediately rescinded.

Statutory and Regulatory Requirements for Email Records Preservation: The requirements in the Federal Records Act of 1950 had not changed. The records requirements in title 36 of the C.F.R. were also largely the same, except that, in 2006, NARA amended the regulations to allow agencies to store transitory email records (which have minimal or no documentary or evidential value) on an email system rather than requiring employees to print and file them or store them in a recordkeeping system, as long as the transitory records are maintained through the applicable NARA-approved retention period.[59]

FAM and FAH Requirements for Email Records Preservation: The requirements in the FAM generally had not changed. In 2005, the FAM was amended to include a reminder that "every Department of State employee must create and preserve records that properly and adequately

[56] NIST, FIPS PUB 200: *Minimum Security Requirements for Federal Information and Information Systems* (March 2006).

[57] 5 FAM 1065.1-6 (February 22, 2007); 5 FAH-11 H-411.4 (June 25, 2007).

[58] 5 FAH-11 H-411.5 (June 25, 2007).

[59] 71 Fed. Reg. 8807 (February 21, 2006) (amending 36 C.F.R. § 1234.24). NARA also amended 36 C.F.R. § 1234.32 to provide a NARA-approved disposition authority for transitory emails.

document the organization, functions, policies, decisions, procedures, and essential transactions of the Department."[60]

Other Preservation Guidance: A February 2005 cable drafted by the Bureau of Administration and sent over the Secretary's name to all embassies and posts and an announcement to all employees reminded departing officials not to remove any papers until they have been reviewed to ensure compliance with records laws and regulations.[61]

In December 2005, NARA issued a bulletin that reminded agencies that all electronic records created and received by agencies are subject to the same existing statutory and regulatory records management requirements as records in other formats and on other media.[62]

A February 2007 cable drafted by the Bureau of Administration and sent over the Secretary's name to all embassies and posts and an announcement to all employees were distributed to remind employees that, until the new State Messaging and Archive Retrieval Toolset (SMART) is implemented, email, Short Message Service messages, or instant messages that qualify as records must be printed and filed with related paper records, including any attachments and transmission data.[63]

In April, June, and October 2008, announcements to all employees again reminded departing employees not to remove any papers until they had been reviewed. They also stated that "e-mail messages must generally be printed out and filed with related paper records."[64]

On January 15, 2009, the Under Secretary for Management issued a memorandum to all Under Secretaries, Assistant Secretaries, Executive Directors, and Post Management Officers on "Preserving Electronically the Email of Senior Officials upon their Departure." The memorandum required bureaus to copy the email accounts of senior departing officials onto CDs and deliver those CDs to IPS. The requirement was applicable to political appointees, not career staff, and was put in place to supplement the traditional print and file policy for record email.

Hillary Clinton (January 21, 2009 – February 1, 2013)

[60] 5 FAM 422.3 (October 11, 2005).

[61] 05 STATE 018818; Department of State, *Procedures for the Removal of Personal Papers and Non-Record Material*, Announcement No. 2005_02_017, February 3, 2005.

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

[63] 07 STATE 024044; Department of State, *Records Management Procedures*, Announcement No. 2007_02_147, February 28, 2007.

[64] Department of State, *Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material*, Announcement No. 2008_04_089, April 17, 2008; Department of State, *Reminder – Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material*, Announcement No. 2008_06_095, June 16, 2008; Department of State, *Reminder – Departing Officials: Procedures for the Removal of Personal Papers and Non-Record Material*, Announcement No. 2008_10_087, October, 16, 2008.

FAM and FAH Requirements for Use of Non-Departmental Systems: A December 2009 FAM provision states that non-Department-owned personal digital assistants (PDAs) may only be turned on and used within Department areas that are strictly unclassified (such as the cafeteria) and may not connect with a Department network except via a Department-approved remote-access program.[65]

Applicable Cybersecurity Provisions and Related Guidance: To meet the requirements of FISMA, the Department implemented a mandatory annual requirement for all Department computer users to take Cybersecurity Awareness training.[66]

Beginning in 2009, the Cyber Threat Analysis Division (CTAD) in DS issued regular notices to Department computer users highlighting cybersecurity threats. CTAD notices addressed BlackBerry security vulnerabilities, citing this device as a weak link in a computer network.[67] CTAD warned that BlackBerry devices must be configured in accordance with Department security guidelines.

CTAD's concerns also included cybersecurity risks faced during international travel. According to an article posted by CTAD, digital threats begin immediately after landing in a foreign country. A primary threat is traced to the traveler's mobile device (BlackBerry or other smart device) which is necessarily connected to the local cellular tower. This connection gives foreign entities the opportunity to intercept voice and email transmissions immediately after the traveler arrives overseas.[68]

The E-Government Act and NIST FIPS PUB 200 were unchanged.

Statutory and Regulatory Requirements for Email Records Preservation: The requirements in the Federal Records Act of 1950 had not changed. In October 2009, NARA published a final rule that revised and reorganized its records management regulations.[69] The existing requirements were largely retained, but renumbered.[70] New responsibilities were added to agencies' records program duties, including assigning records management responsibilities in each program/mission to ensure incorporation of recordkeeping requirements into agency

[65] 12 FAM 683.2-3 (December 2, 2009).

[66] 13 FAM 331 (December 22, 2010).

[67] CTAD, *Security Checklist* (December 15, 2009); CTAD, *Cyber Security Awareness* (March 3, 2011).

[68] *How to manage cybersecurity risks of international travel* (September 15, 2010) by (ISC)2 Government Advisory Board Executive Writers Bureau (posted by CTAD on January 26, 2011).

[69] 74 Fed. Reg. 51004 (Oct 2, 2009).

[70] For example, the requirements of an agency records program were moved from 36 C.F.R. § 1222.20 to 36 C.F.R. §§ 1220.30, 1220.32, and 1220.34. Requirements regarding departing officials were moved from 36 C.F.R. §§ 1222.40, 1222.42 to 36 C.F.R. §§ 1222.18, 1222.24(a)(6).

programs.[71] The new section on managing email records required preservation of email attachments that are an integral part of the record.[72] It also stated:

> Agencies that allow employees to send and receive official electronic mail messages using a system not operated by the agency must ensure that Federal records sent or received on such systems are preserved in the appropriate agency recordkeeping system.[73]

FAM and FAH Requirements for Email Records Preservation: The requirements in the FAM and FAH generally had not changed.

Other Preservation Guidance: In June 2009, the Department sent an announcement regarding preservation of email messages.[74] It reminded employees of the requirement to preserve email records, citing the FAM and C.F.R. provisions, and noted that, until SMART becomes available, employees must print and file emails that are Federal records.

In November 2009, the Department sent a cable to all embassies and posts and an announcement to all employees reminding them that all Department employees have records management responsibilities.[75] It noted that Federal records can be found "in any media including e-mail, instant messages, social media, etc."

On November 28, 2011, President Obama issued a memorandum to the heads of executive departments and agencies requiring them to submit a report to the Archivist and the Director of OMB that

> (i) describes the agency's current plans for improving or maintaining its records management program, particularly with respect to managing electronic records, including email and social media, deploying cloud based services or storage solutions, and meeting other records challenges; (ii) identifies any provisions, or omissions, in relevant statutes, regulations, or official NARA guidance that currently pose an obstacle to the agency's adoption of sound, cost effective records management policies and practices; and (iii) identifies policies or programs that, if included in the Records Management Directive required by section 3 of this memorandum or adopted or implemented by NARA, would assist the agency's efforts to improve records management.[76]

---

[71] 36 C.F.R. § 1220.34 (2010).

[72] 36 C.F.R. § 1236.22(a)(2) (2010).

[73] 36 C.F.R. § 1236.22(b) (2010).

[74] Department of State, *Preserving Electronic Message (E-mail) Records*, Announcement No. 2009_06_090, June 17, 2009.

[75] 09 STATE 120561; Department of State, *Records Management Responsibilities*, Announcement No. 2009_11_125, November 23, 2009.

[76] *Presidential Memorandum – Managing Government Records* (November 28, 2011).

In August 2012, OMB and NARA issued a memorandum to the heads of executive departments, agencies, and independent agencies in part directing agencies to eliminate paper and use electronic recordkeeping. Per this memorandum, agencies will be required to manage all email records in an electronic format by December 31, 2016. [77]

John Kerry (February 1, 2013 – Present)

FAM and FAH Requirements for Use of Non-Departmental Systems: On May 1, 2014, the Department amended the definition of a DIN to require the DIN to be on a Department-owned and operated discrete non-sensitive unclassified local area network that is not connected to any other Department system.[78] In addition, the domestic approving authority for a DIN changed from the Department's IT CCB to the relevant bureau's Executive Director or equivalent.[79]

A September 2014 FAH provision stated that supervisors must exercise "particular care and judgment" in allowing users to remotely process SBU information and must advise users that all non-Department-owned storage media containing Department SBU information must be encrypted with products certified by NIST.[80] Employees were prohibited from remotely processing classified or SBU/NOFORN (not releasable to foreign nationals) information.[81] Employees were also required to (1) exercise "particular care and judgment" in remotely processing SBU information; (2) destroy SBU files saved on personally owned and managed information systems and removable media when the files are no longer required; and (3) implement and regularly update basic home security controls, including a firewall, anti-spyware, antivirus, and file-destruction applications. If an employee used a networked personally owned information system, he or she had to ensure that all information systems on the network implemented these security requirements.

The FAH further prohibits the installation of non-Departmental information systems within Department facilities without the written authorization of DS and IRM.[82] This provision replaced an identical FAM provision issued in 2008.

In 2015, a new FAH provision was added regarding non-Department-owned mobile devices. The FAH provision included a rule requiring a 10-foot separation between a PDA and classified processing equipment, a ban on connecting to a Department network except via a Department-

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

[78] 5 FAM 872 (May 1, 2014).

[79] 5 FAM 872.1 (May 1, 2014).

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

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

[82] 12 FAH-10 H-112.14-2 (September 19, 2014).

approved remote-access program, and a requirement to conduct normal day-to-day Department operations on a Department information system because it has the proper security controls to protect Department information.[83]

Applicable Cybersecurity Provisions and Related Guidance: The Federal Information Security Modernization Act of 2014, enacted in December 2014, updated FISMA by clarifying the roles of OMB and the Department of Homeland Security, improving security by moving away from paperwork requirements, and making improvements in the way that Federal data breaches are managed and reported.[84] Rules and guidance governing cybersecurity threats have not changed.

Statutory and Regulatory Requirements for Email Records Preservation: In 2014, Congress enacted the Presidential and Federal Records Act Amendments of 2014, which amended several sections of the Federal Records Act.[85] It simplified the definition of record to:

> all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them…[86]

The Act noted that the definition of "recorded information" includes "information created, manipulated, communicated, or stored in digital or electronic form." The Act also added a provision that prohibited agency employees from creating or sending a record from a non-official electronic messaging account unless they copy their official electronic messaging account in the original creation or transmission of the record or forward a complete copy of the record to their official electronic messaging account within 20 days.[87]

The requirements in title 36 of the C.F.R. had not changed.

FAM and FAH Requirements for Email Records Preservation: The requirements in the FAM generally had not changed. However, in October 2014, the Department issued an interim directive superseding some of the FAM requirements.[88] The directive noted that employees may delete personal emails, but that "the only e-mails that are personal or non-record are those that

[83] 12 FAH-10 H-165.4 (May 20, 2015).

[84] Pub. L. No. 113-283 (December 18, 2014).

[85] Pub. L. No. 113-187 (November 26, 2014).

[86] 44 U.S.C. § 3301(a).

[87] 44 U.S.C. § 2911(a).

[88] Department of State, *A Message from Under Secretary for Management Patrick F. Kennedy regarding State Department Records Responsibilities and Policy*, Announcement No. 2014_10_115, October 17, 2014.

do not relate to or affect the transaction of Government business." The directive also noted that departing employees may only take personal papers and non-record materials, subject to review by records officials. It reminded employees that "all federal records generated by employees, including senior officials, belong to the Department of State." Finally, the directive stated that:

> employees generally should not use private e-mail accounts (e.g., Gmail, AOL, Yahoo, etc.) for official business. However, in those very limited circumstances when it becomes necessary to do so, the email messages covering official business sent from or received in a personal account must be captured and preserved in one of the Department's official electronic records systems. The best way for employees to ensure this is to forward e-mail messages from a private account to their respective State account. Private email accounts should not be used for classified information.

In October 2015, the Department updated the FAM to incorporate these requirements.[89]

The responsibilities of Management Officers related to departing employees have not changed since Secretary Powell's tenure; however, in 2015, the Department changed the name of the separation form from OF-109 to DS-109. The pertinent language in the form did not change.[90]

Other Preservation Guidance: In February 2013, the Department sent an announcement to all employees reminding senior officials that they may only take personal papers and non-record materials following a review by a records official to ensure compliance with Federal records laws and regulations.[91]

In August 2013, NARA published a bulletin authorizing agencies to use a "Capstone" approach to managing email records, in lieu of print and file.[92] The Capstone approach allows for the automatic capture of records that should be preserved as permanent from the accounts of officials at or near the top of an agency or an organizational subcomponent. In September 2013, NARA published a bulletin that stated that, "while agency employees should not generally use personal email accounts to conduct official agency business, there may be times when agencies authorize the use of personal email accounts." In these cases, "agency employees must ensure that all Federal records sent or received on personal email systems are captured and managed in

[89] 5 FAM 443.7 (October 23, 2015).

[90] 5 FAM 414.7 (June 19, 2015).

[91] Department of State, *Departing Senior Officials: Government Records and Personal Papers*, Announcement No. 2013_02_122, February 26, 2013.

[92] NARA, *Guidance on a New Approach to Managing Email Records*, Bulletin No. 2013-02 (August 29, 2013). In 2014, NARA and OMB issued guidance on managing emails to be used in conjunction with NARA's Capstone guidance. *Memorandum for the Heads of Executive Departments and Agencies and Independent Agencies: Guidance on Managing Email*, M-14-16 (September 15, 2014).

accordance with agency recordkeeping practices."[93] In 2015, NARA issued guidance on managing other forms of electronic messaging, including social media and texts.[94]

On August 28, 2014, the Under Secretary for Management sent a memorandum to the Office of the Secretary, all Under Secretaries and Assistant Secretaries, and a number of other offices to remind them of their responsibility for creating, managing, and preserving records "regardless of physical format or media." It noted that "records may exist in many formats, including Instant Messages (IM) and records on mobile devices like BlackBerrys, mobile phones, and iPads." It also included specific requirements relating to emails, including:

- At no time during designated senior officials' tenure will their e-mail accounts be cleared, deleted, or wiped for any reason.
- While senior officials may delete personal e-mails, they should be aware that the definition of a personal e-mail is very narrow. The only e-mails that are personal are those that do not relate to or affect the transaction of Government business.
- As a general matter, to ensure a complete record of their activities, senior officials should not use their private e-mail accounts (e.g., Gmail) for official business. If a senior official uses his or her private email account for the conduct of official business, she or he must ensure that records pertaining to official business that are sent from or received on such e-mail account are captured and maintained. The best way to ensure this is to forward incoming emails received on a private account to the senior official's State account and copy outgoing messages to their State account. [95]

[93] NARA, *Guidance for agency employees on the management of Federal records, including email accounts, and the protection of Federal records from unauthorized removal*, Bulletin No. 2013-03 (September 9, 2013).

[94] NARA, *Guidance on Managing Electronic Messages*, Bulletin No. 2015-02 (July 29, 2015).

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

APPENDIX B: MANAGEMENT RESPONSES

UNCLASSIFIED

TO: Inspector General – Steve Linick

FROM: Transparency Coordinator - Janice L. Jacobs

SUBJECT: OIG Draft Report – "Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements (ESP-16-03): Responses to Recommendations

In March 2015, Secretary Kerry asked the Office of the Inspector General to review the Department's efforts to preserve a full and complete record of American foreign policy, and our procedures for making that record available to the American public. We welcome the opportunity to respond to your report, *Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements*, the fourth installment of your review. As your reports recognize, through our work with your office, as well as the Department's efforts to meet Presidential and Department directives, we have made great progress towards a better preserved and more accessible public record. As demonstrated in the enclosed responses and comments to your specific recommendations, the Department is committed to continuing to improve. However, I also want to acknowledge and highlight how far we have already come.

For decades, the government has been working to adapt longstanding recordkeeping principles and rules to the email-dominated modern era. The Federal Records Act and the Freedom of Information Act are established pillars of transparent government, but email and other communications technologies create difficult challenges for implementation. As your report describes, over the years the Department has been good at drafting principles on the importance of preserving email; however, only recently have we begun to match results with our aspirations. The National Archives and Records Administration (NARA) has acknowledged that the entire federal government—not just the State Department—continues to grapple with these challenges. In fact, NARA has issued some of its most relevant guidance regarding these matters in the last three years.

Today, I can attest to the Department's goal of leading on these issues in the future. Earlier this year, Secretary Kerry issued a Department-wide notice on the critical importance of the Freedom of Information Act, demonstrating a

commitment to transparency at the most senior level. In September 2015, Secretary Kerry announced my appointment as the Department's Transparency Coordinator to oversee the Department's efforts on these matters. At the time, the Department was already engaged in a process to meet the President's *Managing Government Records* directive, including through the robust work of our Electronic Records Management Working Group. We are on track to meet the benchmarks of the President's directive for 2016; for example, your report notes that the Department is in the process of procuring new technology to manage emails electronically.

In addition, in 2014 the Department issued guidance on the use of personal emails—in effect anticipating later changes to the Federal Records Act—and initiated the Department's implementation of the Capstone program in February 2015 to archive automatically senior officials' emails. Over 200 officials are already covered by Capstone, with more on the way. We also have already closed a number of the recommendations in your first three reports.

Finally, the Executive Secretariat, Bureau of Administration, and other relevant bureaus have established a strong working relationship to improve records management. We are already cataloguing our current holdings of electronic archives, improving the way we search email records, and establishing procedures for archiving records going forward.

As a result of these and other efforts, today the Department is much differently situated than during historical periods described in your report. It is clear that the Department could have done better at preserving emails of Secretaries of State and their senior staff going back several administrations. However, by early 2015, the Department had already taken important steps to address these issues. As noted above, our Electronic Records Management Working Group was already established. In addition, the Department had already received Secretary Clinton's emails and undertook to release over 30,000 of them to the public. The National Archives and Records Administration concluded that our efforts with respect to Secretary Clinton and her senior staff mitigated past problems, as has a federal district court in a suit brought under the Federal Records Act. As you note in the report, you concur with this conclusion.

The way we conduct diplomacy has evolved significantly in recent years from a time when official cables were one of the primary ways we communicated. Modern technology has unquestionably enhanced our mission; however, there is still work to do to ensure that we preserve a record of our work. We look forward

to working with your office in the future on these issues, and remain committed to building on what we have already accomplished.

May 23, 2016

UNCLASSIFIED

TO: Inspector General – Steve Linick

FROM: M – Patrick Kennedy

SUBJECT: Draft report – "Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements" (ESP-16-03 dated May 2016)

Thank you for the opportunity to comment on subject draft report. Over the past year, the Department has taken steps to improve its records management practices and we believe we have made progress. However, more progress can be made, and we are committed to reaching the December 2016 goal set by NARA for email retention and continue advancing sound records management.

Responses to recommendations from bureaus within the M family follow below.

Recommendation 1: The Bureau of Administration should

- issue guidance, including periodic, regular notices, to Department employees to remind them that the use of personal email accounts to conduct official business is discouraged in most circumstances,
- clarify and give specific examples of the types of limited circumstances in which such use would be permissible, and
- instruct employees how to preserve Federal records when using personal email accounts.

Department Response: The Bureau of Administration concurs with this recommendation and will continue to issue guidance on records management practices and policies, and will ensure that this guidance explicitly reminds employees that the use of personal emails accounts to conduct official business is discouraged. Similar to previous records management guidance, such guidance will be provided to employees in writing (via Department Notices and ALDACs) and in appropriate briefings (i.e. training courses, meetings, etc.) to remind employees of their responsibility for preserving documentation of official activities, including emails. The Department will consider additional means by which to inform employees of records management requirements and best practices.

Recommendation 2: The Bureau of Administration should amend the *Foreign Affairs Manual* to reflect the updates to Department recordkeeping systems that provide alternatives to print and file.

Department Response: We concur with this recommendation, but please edit to read "alternatives to print and file emails that are records."

The Bureau of Administration is currently working with the Office of the Transparency Coordinator to update 5 FAM and chapter subparts related to Department's recordkeeping/retention schedules. The goal to eliminate the practice of print and file as the Department's policy and practice for the retention of emails by December 31, 2016, which is also the deadline by which the Department is supposed to implement a solution to manage all emails. All other electronic documents should follow this electronic retention practice by the end of 2019.

Recommendation 7: The Bureau of Information Resource Management (IRM) should

- issue regular notices to remind Department employees of the risks associated with the use of non-Departmental systems;
- provide periodic briefings on such risks to staff at all levels; and
- evaluate the cost and feasibility of conducting regular audits of computer system usage to ascertain the degree to which Department employees are following the laws and policies concerning the use of personal email accounts.

Department Response: The Department concurs with the first two bullet points of this recommendation. IRM will continue to issue regular notices regarding the risks associated with the use of non-Departmental systems.

Regarding the third bullet, audits conducted on such a wide scale would not be beneficial or feasible. Limited use of personal email is acceptable under current policy and allowable under law. The Department already conducts continuous monitoring to ensure the integrity of the Department networks and systems and in fact was a government leader in this regard. State's Continuous Diagnostics and Monitoring which is also known as iPost has been adopted and modified by DHS into the new government-wide Continuous Diagnostics and Mitigation program (CDM). Under 5 FAM 724, the Department can audit an employee's network activity or workstation

use, which includes but is not limited to electronic communication, Internet access, local disk files, and server files when there is suspicion that improper use of government equipment has occurred. In addition, Information Systems Security Officers (ISSOs) worldwide are required to review systems and security logs on a regular basis.

Regarding the first bullet point, the Bureau of Information Resource Management continues to issue notices and provide briefings on risks associated with the use of non-Departmental systems. For example:

- Mandatory PS 800 Cyber Security Awareness Training course
- Informational links
  - https://intranet.ds.state.sbu/DS/SI/CS/Awareness1/Content/Email.aspx for email, or
  - one level higher for other types of awareness information
- Department Notices (recent)
  - 2016_03_128 Global Cyber Foreign Policy Training Workshop on April 25-29, 2016
  - 2016_02_035 Revised 12 FAM 620 and New 12 FAH-10 (Unclassified Cyber Security Policies) are published
  - 2015_11_063 October was National Cyber Security Awareness Month
- IT Customer Service Bulletins (e.g., 7/30/15) and also Information Announcements on http://irm.m.state.sbu/sites/ops/CSO/ITSC/default.aspx
- DS Cybersecurity Awareness In Case You Missed It
- Cyber Security Awareness month – October
- Tips of the Day
  - Tips of the Day and StateNet advertisement on *Protecting SBU Outside the Department* and *Protecting Personal Email Accounts*
- Fact Sheet on *Protecting Personal Email Accounts*
- Fact Sheet on *How to Handle Suspicious Email* (including personal email)
- Fact Sheet on *Email Safety*
- Personal Email Security Best Practices guide
- How to Report Suspicious Messages/Activity on Webmail Accounts guide
- *Notes* blast emails on Personal Email Addresses, Personal Email Reminder, How to Handle Suspicious Email, Sending SBU Over the

Internet, Cloud Computing, Cloud Security, Protecting OpenNet When Accessing Personal Email Accounts

- *Awareness Bulletin* on Personal Email Accounts and Out of Office Messages
- Personal Email Guides (Gmail, Hotmail, Yahoo, Outlook)
- Information Systems Security Officer (ISSO) Role-Based Training – mandatory for ISSOs
- A-100 Foreign Service Generalist class – general overview
- IRM Tradecraft
  - YW319 - IRM Tradecraft for the Information Technology Manager
  - YW387 - Information Resources Management Tradecraft
- Diplomatic Security Training Center (DSTC) summary:
  - For FY 2015 DSTC conducted 80 course sessions in different cybersecurity areas (including those for ISSOs)
  - For FY-2016, DSTC has scheduled 81 different cybersecurity courses
- Ambassador/PO and DCM seminars – overview

We will review whether the material in these notices and courses needs to be updated or expanded.

Recommendation 8: The Director General of the Foreign Service and Director of Human Resources should amend the *Foreign Affairs Manual* to provide for administrative penalties for Department employees who (1) fail to comply with recordkeeping laws and regulations or (2) fail to comply with the requirement that only authorized information systems are to be used to conduct day-to-day operations. The amendment should include explicit steps employees should take if a reasonable suspicion exists that documents are not being preserved appropriately, including a reminder that the Office of Inspector General has jurisdiction to investigate and refer to appropriate authorities suspected violations of records preservation requirements.

Department Response: The Department concurs with this recommendation and will implement it by revising, following any appropriate consultation with the unions, the lists of disciplinary offenses contained at 3 FAM 4377 and 4542 to include explicitly violations of laws, regulations and directives regarding records management, including preservation. (At present, such offenses would fall into general catch-all provisions contained in each list.)

With respect to the second sentence of Recommendation 8, as part of its continuing issuance of records guidance, the Bureau of Administration, in coordination with the Bureau of Human Resources, will include guidance on how and where to raise records management concerns. Such guidance will remind employees of the jurisdiction of the Office of Inspector General.

United States Department of State

Washington, D.C. 20520

May 16, 2016

UNCLASSIFIED

TO: Steve Linick, Inspector General

FROM: Joseph E. Macmanus, Executive Secretary

SUBJECT: Response to Draft OIG Review of Email Records Management and Cybersecurity Requirements Involving the Office of the Secretary

The Executive Secretariat thanks the OIG for the opportunity to respond to this review. The Secretariat values the OIG's study of electronic records management – a Department-wide challenge that we will continue to address. The Secretariat has the following specific responses to the recommendations contained in the report.

Recommendation 3: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to conduct an inventory of all electronic and hard-copy files in its custody and evaluate them to determine which files should be transferred to the Office of Information Programs and Services in accordance with records disposition schedules or Department email preservation requirements.

> **Department Response**: The Executive Secretariat agrees with this recommendation and notes that the inventory of electronic and hard copy files has been ongoing since January 2016. The Executive Secretariat agrees this is an important and necessary project.

Recommendation 4: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to adopt policies and procedures to ensure compliance by all employees within its purview, including the Secretary, with records management requirements. These policies should cover the retirement of records in accordance with records disposition schedules, preservation of email and other electronic records of departing officials, and training of employees in their records preservation responsibilities.

UNCLASSIFIED

Department Response: The Executive Secretariat strongly agrees with the OIG recommendation that it should work closely with the Office of Information Programs and Services to fully implement policies and procedures to improve compliance with records management responsibilities, including the retirement of records in accordance with records disposition schedules, preservation of email and other electronic records of departing officials, and training of employees on their records preservation responsibilities. The Executive Secretariat staff is committed to coordinating closely with the Office of Information Programs and Services to provide updated guidance and training to all staff.

Recommendation 5: The Office of the Secretary, Executive Secretariat, should work with the Office of Information Programs and Services to ensure that all departing officials within its purview, including the Secretary of State, sign a separation form (DS-109) certifying that they have surrendered all Federal records and classified or administratively controlled documents. In addition, staff should ensure that all incoming officials within its purview, including the Secretary, clearly understand their records preservation and retention responsibilities, including records contained on personal email accounts.

Department Response: The Executive Secretariat agrees with the OIG recommendation that it should ensure all departing officials within its purview, including the Secretary of State, sign a separation agreement form (DS-109), and that all incoming staff clearly understand their records preservation and retention responsibilities. The Executive Secretariat is instituting a process whereby employees' completed DS-109 forms are placed in their permanent electronic performance files (eOPF) to ensure they easily accessible.

UNCLASSIFIED

TO: Inspector General – Steve Linick

FROM: Transparency Coordinator – Janice L. Jacobs

SUBJECT: Draft report – "Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements" (ESP-16-03 dated May 2016)

Thank you for the opportunity to comment on subject draft report, which includes the following recommendation:

"The Department's Transparency Coordinator should work with the Office of Information Programs and Services to develop a quality assurance plan to promptly identify and address Department-wide vulnerabilities in the records preservation process, including lack of oversight and the broad inaccessibility of electronic records."

I concur and am happy to comply with your recommendation as part of my continuing efforts, in coordination with the Office of Information Programs and Services (A/GIS/IPS) and the Executive Secretariat (S/ES), to improve overall governance of the Department's information – how it is captured, stored, shared, disposed of, and archived as appropriate. Your findings will help inform these efforts. The report's focus on email records is particularly relevant given that all federal agencies have been directed by the White House and the National Archives and Records Administration (NARA) to manage all email records in an electronic format by December 31 of this year. Department progress towards this goal is well underway with measures either already in place or on the horizon. The Capstone program mentioned in your report, whereby the emails of designated senior officials are all captured and retained permanently, is one such step already taken by the Department.

By December 2019, all permanent electronic records in federal agencies must be managed electronically to the fullest extent possible. This will be a huge undertaking requiring a governance structure for all forms of information created or received by the Department. The Department is committed to getting this right to help assure a 21st century enterprise-wide information management system that advances the Department's goals of increased efficiency, transparency and accountability. We will not succeed without sufficient metrics, quality controls, and general oversight of the system we create. This is why the quality assurance plan you've recommended is so important.

As I move forward, I remain mindful of Secretary Kerry's strong commitment to improving the Department's records management and transparency systems in order to preserve the record of U.S. foreign policy and to share that story with the wider public.

ABBREVIATIONS

A	Bureau of Administration
AIS	Automated Information System
C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
CSIP	Cyber Security Incident Program
CTAD	Cyber Threat Analysis Division
D-MR	Deputy Secretary for Management and Resources
DCIO	Deputy Chief Information Officer
Department	Department of State
DIN	Dedicated Internet Network
DS	Bureau of Diplomatic Security
ERMWG	Electronic Records Management Working Group
FAH	*Foreign Affairs Handbook*
FAM	*Foreign Affairs Manual*
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GAO	Government Accountability Office
INR	Bureau of Intelligence and Research
IPS	Office of Information Programs and Services
IRM	Bureau of Information Resource Management
ISP	Internet service provider

IT CCB	Information Technology Change Control Board
L	Office of the Legal Adviser
M	Under Secretary for Management
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NOFORN	not releasable to foreign nationals
OIG	Office of Inspector General
OMB	Office of Management and Budget
PDA	personal digital assistant
.pst	Personal Storage Table (Microsoft Outlook file format)
S	Office of the Secretary
S/ES	Office of the Secretary, Executive Secretariat
S/ES-EX	Office of the Executive Director, S/ES
S/ES-IRM	Office of Information Resources Management, S/ES
SAO	Senior Agency Official
SBU	sensitive but unclassified
SMART	State Messaging and Archive Retrieval Toolset

OIG TEAM MEMBERS

Jennifer L. Costello, Team Leader, Office of Evaluations and Special Projects
David Z. Seide, Team Leader, Office of Evaluations and Special Projects
Jeffrey McDermott, Office of Evaluations and Special Projects
Robert Lovely, Office of Evaluations and Special Projects
Michael Bosserdet, Office of Inspections
Brett Fegley, Office of Inspections
Kristene McMinn, Office of Inspections
Timothy Williams, Office of Inspections
Aaron Leonard, Office of Audits
Phillip Ropella, Office of Audits
Kelly Minghella, Office of Investigations
Eric Myers, Office of Investigations

HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926
OIG.state.gov/HOTLINE
If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:
OIGWPEAOmbuds@state.gov