



09/05/2014
2:29 PM

201412443 Rev. 1

United States Department of State

*Under Secretary of State
for Management*

Washington, D.C. 20520

UNCLASSIFIED

AUG 28 2014

MEMORANDUM TO: The Office of the Secretary
The Office of Deputy Secretary Burns
The Office of Deputy Secretary for Management and
Resources Higginbottom
The Director of Foreign Assistance
All Under Secretaries
C- The Office of the Counselor
All Assistant Secretaries
L - The Office of the Legal Advisor
S/CPR - Peter Selfridge
S/P - David McKean
All Special Representatives and Special Envoys
cc: Executive Directors

From:

M - Patrick F. Kennedy

SUBJECT: Senior Officials' Records Management Responsibilities

Senior officials are responsible for creating records necessary to document their activities and for the proper management and preservation of their records (see Tab 1 for the list of Senior Officials to which this memorandum is directed). These responsibilities are applicable to all records made or received in the conduct of agency business regardless of physical format or media. While all Department employees are to preserve records meeting the definition of a record under the Federal Records Act, see 3 FAM 414.8, senior officials' records are generally the most important documents created within the Department and are some of the most valued documents archived at the National Archives and Records Administration (NARA). Proper records management ensures statutory and regulatory compliance, preserves the rights of the government and citizens, supports better decision making, safeguards vital records, preserves organizational memory, minimizes litigation risk (ensuring systematic, documented, and routine disposal of records), and reduces operating costs through control over the lifecycle of the records.

UNCLASSIFIED

UNCLASSIFIED

- 2 -

Specifically, senior officials must create records necessary to document their activities and actions taken on behalf of the Department. A records custodian must be identified who can manage a particular senior official's records in support of proper records lifecycle management, including appropriate access. Departing or transferring Senior Officials must identify their records prior to departure or transfer. Departing Senior Officials are reminded they may take with them only personal papers and non-record materials, subject to review by records officers to ensure compliance with federal records laws and regulations. All records generated by Senior Officials belong to the Department of State.

Defining and Managing Records

Records may exist in many formats, including Instant Messages (IM) and records on mobile devices like BlackBerries, mobile phones, and iPads. Typical records created by Senior Officials include not only e-mails, memos, and similar documents, but also calendars, schedules, and logs of daily activities.

Additionally, Senior Official records should include the following:

- Records pertaining to various committees, including Federal Advisory Boards, councils, and inter-agency and external committees in which the Senior Official participated.
- Materials relating to internal and external meetings, including briefing documents, minutes, and meeting notes.
- Records documenting the development of Department policies and programs, including correspondence, briefing and issue papers, and reports about policy, strategy, research and legislative priorities, program evaluation and planning, and similar topics.
- Reports to Congress and/or the President.

To establish a sound records management program, Senior Officials should, at minimum, take the following steps:

- Designate a records manager responsible for their records.
- Follow established records disposition schedules, which set out the applicable records retention and disposition requirements.
- Establish a plan for maintaining and managing their records.
- Collect, organize, and categorize their records in order to facilitate their preservation, retrieval, use, and disposition.

Specific Email Requirements and Procedures

UNCLASSIFIED

UNCLASSIFIED

- 3 -

E-mail is the most widely-used tool within the Department for the conduct of official business. The Department generates millions of e-mail communications each year, many of which document significant foreign policy and Department business decisions. The standard for determining whether an e-mail message meets the definition of a "record" under the Federal Records Act is the same standard that applies to all other types of Department records (5 FAM 443.2 – see Tab 2).

As a supplement to existing policy, and consistent with the policy in place since 2009, it is important to capture electronically the e-mail accounts of the senior officials listed in Tab 1 as they depart their positions. Instructions for senior officials are provided (see Tab 3).

- 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 e-mail 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 e-mails received on a private account to the senior official's State account and copy outgoing messages to their State account.

Visit the Department's Records Management [website](#) for more information.

Attachments:

Tab 1 – List of Designated Senior Official Positions

Tab 2 – 5 FAM 443.2 (Which E-mail Messages Are Records)

Tab 3 – Instructions for Preserving E-mail of Departing Senior Officials

UNCLASSIFIED

DRAFT: Designated Senior Official Positions – March 5, 2014

*The positions identified below reflect NARA guidance to satisfy the Presidential Directive on retaining Email for Senior Officials. The Electronic Records Management Working Group will subsequently address the companion NARA guidance for retaining all other Email.

- Secretary of State
- Deputy Secretary
- Under Secretary
- Assistant Secretary (AS)
- Regional Deputy Assistant Secretary
- Principal Deputy Assistant Secretary (PDAS)
- Chief of Staff
- Deputy Chief of Staff
- Executive Secretary
- Deputy Executive Secretary
- Executive Assistant to the Principal Officers
- Policy Advisor
- Strategic Advisor
- Chief Speechwriter
- Director of Communications
- Director of Foreign Assistance
- Director of M/PRI
- White House Liaison
- Chief Financial Officer
- Chief Economist
- Chief Information Officer
- Chief of Protocol
- Assistant Chief of Protocol
- Deputy Chief of Protocol
- Counselor
- Comptroller
- Legal Adviser
- Deputy Legal Adviser
- Assistant Legal Adviser
- Counselor on International Law
- Special Assistant to the Legal Adviser
- Principal Deputy Legal Adviser
- Inspector General
- Deputy Inspector General
- Counsel to the Inspector General
- Geographer
- Accountability Review Board Members
- Senior Advisers to the Principals
- Ambassador
- Ambassador-At-Large
- Chief of Mission
- Charges d' Affaires
- Charges d' Affaires ad interim
- Consuls General
- Consuls
- Principal Officer of U.S. Interest Sections
- Deputy Chief of Mission
- Deputy to the Ambassador-At-Large
- Deputy Principal Officers
- Assistant Chiefs of Mission
- Special Envoy
- Deputy Special Envoy
- Special Representative
- United States Permanent Representative
- United States Representative
- United States Deputy Representative
- Alternate Representative
- All individuals formally designated (i.e. by memorandum) as "Acting" in the above listed positions
- Applicable Special Assistants and Staff Assistants to the above listed positions, when they receive and respond to emails on the Senior Official's behalf

**Beyond this list, Bureaus may determine at an office level which individual positions would be considered "Designated Senior Official Positions" for the purposes of email preservation.

5 FAM 440 ELECTRONIC RECORDS, FACSIMILE RECORDS, AND ELECTRONIC MAIL RECORDS

*(CT:IM-126; 02-28-2012)
(Office of Origin: A/GIS/IPS)*

5 FAM 441 ELECTRONIC RECORDS MANAGEMENT

(TL:IM-19; 10-30-1995)

These requirements apply to all electronic records systems: microcomputers; minicomputers; and mainframe computers in networks or stand-alone configurations, regardless of storage media.

a. Electronic Data files.

- (1) Those employees who are responsible for designing electronic records systems that produce, use, or store data files, shall incorporate disposition instructions for the data into the design plan.
- (2) System Administrators must maintain adequate and current technical documentation for electronic records systems that produce, use, or store data files. At a minimum, include:
 - (a) a narrative description of the system (overview);
 - (b) a records layout that describes each field, its name, size, starting or relative position;
 - (c) a description of the form of the data (e.g., alphabetic, zoned decimal, packed decimal or numeric) or a data dictionary. Include the equivalent information and a description of the relationship between data elements in the data bases when associated with a data base management system; and
 - (d) any other technical information needed to read or process the records.
- (3) Electronic data bases that support administrative or housekeeping functions and contain information derived from hard copy records authorized for disposal may be deleted if the hard copy records are maintained in official files.
- (4) Data in electronic form that is not preserved in official hard copy files or supports the primary program or mission of an office, even if preserved in official hard copy files, may not be deleted or destroyed except through authorities granted as prescribed in sections h. and i. below.

b. Documents.

- (1) Electronic records systems that maintain the official file copies of documents shall provide a capability for the disposition of the documents. This includes the requirements for transferring permanent records to the National Archives, when necessary.
- (2) Electronic records systems that maintain the official file copy of documents shall identify each document sufficiently to enable authorized personnel to retrieve, protect, and carry out the disposition of documents in the system. Appropriate identifying information may include: office of origin, TAGS/Terms, subject line, addressee (if any), signatory, author, date, security classification, and authorized disposition.
- (3) Electronic records systems that maintain the official file copy of documents shall provide sufficient security to ensure document integrity.
- (4) Documents such as letters, messages, memorandums, reports, handbooks, directives, and manuals recorded on electronic media may be deleted if the hard copy record is maintained in official files.
- (5) Documents such as letters, messages, memorandums, reports, handbooks, directives, and manuals recorded and preserved on electronic media as the official file copy shall be deleted in accordance with authorized disposition authorities for the equivalent hard copy. If the authority does not exist, the documents in electronic form may not be deleted or destroyed except through authorities granted as prescribed in sections h. and j. below.

c. Spreadsheets.

- (1) Spreadsheets recorded on electronic media may be deleted when no longer needed to update or produce hard copy if the hard copy record is maintained in official files.
- (2) Spreadsheets recorded and preserved on electronic media shall be deleted in accordance with authorized disposition authorities for the equivalent hard copy.

d. Electronic records are acceptable as evidence in federal courts. Rule 803 (6), Federal Rules of Evidence, has been interpreted to include computer records. Further under Rule 1006, summary electronic records may be provided to limit the quantity of information considered during judicial proceedings. The courts must believe that records admitted before it are "trustworthy" that is, they must clearly and accurately relate the facts as originally presented or in summary form.

e. Administrators of electronic records systems shall ensure that only authorized personnel have access to electronic records.

f. Administrators of electronic records systems shall provide for the backup and recovery of records.

- g. Administrators of electronic records systems shall make certain that storage media meet applicable requirements prescribed in 36 CFR 1234.28. These requirements are also contained in FIRM Bulletin B-1 and are discussed in the RMH, 5 FAH-4 H-219.
- h. Retention of electronic records.
- (1) The information in electronic records systems and related documentation and indexes must be scheduled for disposition no later than one year after the implementation of the system.
 - (2) Procedures must be established for systematically backing up, copying, reformatting, and providing other necessary maintenance for the retention and usability of electronic records throughout their prescribed life cycles.
- i. Destruction of electronic records.
- (1) Electronic records may be destroyed only in accordance with a records disposition authority approved by the Archivist of the United States. This authority is obtained through the Records Management Branch (OIS/RA/RD).
 - (2) This process is exclusive, and records of the United States Government, including electronic records, may not be alienated or destroyed except through this process.
 - (3) Electronic records scheduled for destruction must be disposed of in a manner that ensures protection of any sensitive, proprietary or national security information. Magnetic recording media are not to be reused if the previously recorded information can be compromised in any way. Refer to 12 FAM for requirements regarding the security of magnetic media.
- j. All automated information systems (AIS) or facsimile machines used to process or store electronic records must comply with the security regulations contained in 12 FAM.

5 FAM 442 FACSIMILE RECORDS

(TL:IM-19; 10-30-1995)

The use of facsimile (FAX) equipment in appropriate and cost-effective circumstances is encouraged in the Department. Facsimile transmissions have the same potential to be Federal records as any other documentary materials received in Federal offices. The method of transmitting a document does not relieve sending or receiving offices of the responsibility for adequately and properly documenting official actions and activities and for ensuring the integrity of records. See the RMH, 5 FAH-4, for more guidance on facsimile records. See 5 FAM 561 for policies on FAX transmissions, including use of secure FAX equipment and using FAX equipment to send correspondence to members of Congress.

5 FAM 442.1 Facsimile Label

(TL:IM-19; 10-30-1995)

The Records Management Branch (OIS/RA/RD) has designed a facsimile transmission label (Form DS-1905), to be affixed to facsimile equipment. The label serves as a reminder to users of the responsibility to file record copies of facsimiles and to photocopy record copies of thermal paper facsimiles onto plain paper for filing. The labels are available from OIS/RA/RD.

5 FAM 442.2 FAX Transmittal Forms

(TL:IM-19; 10-30-1995)

- a. Form DS-1890, Unclassified Facsimile Transmittal Cover Sheet, and Form DS-1890-A, Classified Facsimile Transmittal Cover Sheet, are Department forms that are available for use in transmitting documents. Their use is not mandatory. These forms are available on the INFOFORMS disk, which is part of the Department's INFOEXPRESS application. At a minimum, the transmittal form which is used by an office, should contain the following information:
 - date of transmittal
 - sending and receiving office information (symbol, name, voice & fax telephone numbers)
 - subject information, including TAGS/Terms to help properly file the documents
 - any comments regarding the transmission
 - appropriate security classification, when using a secure fax machine.
- b. Transmittal cover sheets containing substantive comments are to be filed with related record material. Those containing informal messages can be destroyed upon receipt or when no longer needed.

5 FAM 443 ELECTRONIC MAIL (E-MAIL) RECORDS

5 FAM 443.1 Principles Governing E-Mail Communications

(TL:IM-19; 10-30-1995)

- a. All Government employees and contractors are required by law to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency (Federal Records Act, or "FRA," 44 U.S.C. 3101 et

seq). In addition, Federal regulations govern the life cycle of these records: they must be properly stored and preserved, available for retrieval, and subject to appropriate approved disposition schedules.

- b. As the Department's information modernization program goes forward, new forms of electronic communications have become increasingly available within the Department and between the Department and overseas posts. One example of the improvements that modernization has brought is the automatic electronic preservation of departmental telegrams. Employees are reminded that under current policy departmental telegrams should be used to convey policy decisions or instructions to or from posts, to commit or request the commitment of resources to or from posts, or for official reporting by posts.
- c. Another important modern improvement is the ease of communication now afforded to the Department world-wide through the use of E-mail. Employees are encouraged to use E-mail because it is a cost-efficient communications tool. 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. The following guidance is designed to help employees determine which of their E-mail messages must be preserved as Federal records and which may be deleted without further authorization because they are not Federal record materials.

5 FAM 443.2 Which E-Mail Messages are Records

(TL:IM-19; 10-30-1995)

- a. E-mail messages are records when they meet the definition of records in the Federal Records Act. The definition states that documentary materials are Federal records when they:
 - are made or received by an agency under Federal law or in connection with public business; and
 - are preserved or are appropriate for preservation as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government, or because of the informational value of the data in them.
- b. The intention of this guidance is not to require the preservation of every E-mail message. Its purpose is to direct the preservation of those messages that contain information that is necessary to ensure that departmental policies, programs, and activities are adequately documented. E-mail message creators and recipients must decide whether a particular message is appropriate for preservation. In making these decisions, all personnel should exercise the same judgment they use when determining whether to retain and file paper records.
- c. Under FRA regulations (36 CFR 1222.38), principal categories of materials, including E-mail, that are to be preserved are:

- records that document the formulation and execution of basic policies and decisions and the taking of necessary actions;
 - records that document important meetings;
 - records that facilitate action by agency officials and their successors in office;
 - records that make possible a proper scrutiny by the Congress or other duly authorized agencies of the Government; and
 - records that protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions.
- d. For example, just like paper records, E-mail messages that may constitute Federal records include:
- (1) E-mail providing key substantive comments on a draft action memorandum, if the E-mail message adds to a proper understanding of the formulation or execution of Department action;
 - (2) E-mail providing documentation of significant Department decisions and commitments reached orally (person to person, by telecommunications, or in conference) and not otherwise documented in Department files;
 - (3) E-mail conveying information of value on important Department activities, e.g. data on significant programs specially compiled by posts in response to a Department solicitation, if the E-mail message adds to a proper understanding of Department operations and responsibilities.

5 FAM 443.3 How to Preserve E-Mail Records

(TL:IM-19; 10-30-1995)

For those E-mail messages and attachments that meet the statutory definition of records, it is essential to ensure that the record documentation include the E-mail message, any attachments, and essential transmission data (i.e. who sent the message, the addressees and any other recipients, and when it was sent). In addition, information about the receipt of messages should be retained if users consider it necessary for adequately documenting Department activities. If transmission and necessary receipt data is not printed by the particular E-mail system, the paper copies must be annotated as necessary to include such data. 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. Instructions for printing and handling of Federal records for most of the Department's existing E-mail systems have been prepared and will be available through bureau Executive Offices

5 FAM 443.4 Records Management Reviews

(TL:IM-19; 10-30-1995)

The Department's Records Management Office (OIS/RA/RD) conducts periodic reviews of the records management practices both at headquarters and at overseas posts. These reviews ensure proper records creation, maintenance, and disposition by the Department. These periodic reviews now will include monitoring of the implementation of the Department's E-mail policy.

5 FAM 443.5 Points to Remember About E-Mail

(TL:IM-19; 10-30-1995)

- Department E-mail systems are for official use only by authorized personnel.
- The information in the systems is Departmental, not personal. No expectation of privacy or confidentiality applies.
- Before deleting any E-mail message, apply these guidelines to determine whether it meets the legal definition of a records and if so, print it.
- Be certain the printed message kept as a record contains the essential transmission and receipt data; if not, print the data or annotate the printed copy.
- File the printed messages and essential transmission and receipt data with related files of the office.
- Messages that are not records may be deleted when no longer needed.
- Certain E-mail messages that are not Federal records may still be subject to pending requests and demands under the Freedom of Information Act, the Privacy Act, and litigation and court orders, and should be preserved until no longer needed for such purposes.
- Classified information must be sent via classified E-mail channels only, with the proper classification identified on each document.
- When E-mail is retained as a record, the periods of its retention is governed by records retention schedules. Under those schedules, records are kept for defined periods of time pending destruction or transfer to the National Archives.

5 FAM 443.6 Future Technology

(TL:IM-19; 10-30-1995)

- a. The Department is actively working to develop systems that will enable those E-mail messages that are official records to be preserved electronically.
- b. These regulations are in compliance with those set forth by the National Archives and Records Administration.

- c. The Department and all posts are requested to bring these regulations to the attention of all Department employees and contractors and to begin its implementation immediately.

5 FAM 444 THROUGH 449 UNASSIGNED

Instructions for Preserving Email of Departing Senior Officials August 2014

- 1) As part of the employee check-out process, Executive Directors and Post Management Officers must notify their system administrators of the departure of designated Senior Officials and direct the system administrators to replicate the Official's remaining email onto CDs according to the following directions. If possible ask departing Officials to delete truly personal emails (to/from family, friends, and other non-work related emails) from their inbox, sent mail and PST. folders.
- 2) Note, preceding the Senior Officials' departure, at no time during their tenure in a position will their email account be deleted, cleared, or wiped for any reason. If, for instance, they reach their maximum allotted space in their mailbox, the Executive Director, Post Management Officer, and the system administrator will work constructively with the Senior Official to move older emails into stable and secure storage until the check-out process delineated in Instruction 1 is initiated.
- 3) System administrators must disable (but NOT delete) the OpenNet, ClassNet, POEMS and PACE Active Directory (AD) accounts of departing Officials.
- 4) System administrators do NOT delete the OpenNet, ClassNet, POEMS and PACE email accounts of departing Officials.
- 5) System administrators DO hide (but not remove) names of departing Officials from GALs.
- 6) System administrators DO delete the names of departing Officials from DLs.
- 7) Executive Directors, Office Directors or equivalent (Domestic Offices) or Management Counselors/Officers (Posts) must provide A/GIS/IPS/RA (by OpenNet mail to Records-DL@state.gov) with (a) the name of departed officials, (b) the designated Bureau/Post Records Management Coordinator, and (c) the Bureau/Post System Administrator. After the information is copied to the CDs, **the bureau/post must verify that the CDs are readable before sending.**
- 8) System administrators should create CDs for each OpenNet, ClassNet, POEMS and PACE email account of departed Officials. One set must be created for retirement, using the form DS-693, to A/GIS/IPS/RA for records preservation; the other is for Bureau/Post use, if required. See the *How to Retire Records* page of the DOS Records Management intranet site for further guidance on retiring records using the DS-693:
<http://a.m.state.sbu/sites/gis/ips/RA/Pages/RetiredRecords.aspx>.
- 9) System administrators must use the following .PST naming conventions:

- a. For "Mailbox" content, use the user name followed by "_MB".
- b. i.e., Smith_John H_MB. If the mailbox exceeds the capacity of one CD, use: Smith_John H_MB1 for the first .PST created by the system administrator and Smith_John H_MB2 for the second .PST created by the system administrator, etc. (System administrators can decide where/how to split the content among multiple CDs.)
- c. For existing (user created) .PSTs, aka "personal folders", (this is a misnomer used by Microsoft since the content is "official", not "personal"), use the user name followed by "_PF" i.e. Smith, John H_PF. If the existing PSTs exceed the capacity of one CD, or there are multiple .PSTs, use Smith, John H_PF1 for the first .PST, Smith, John H_PF2 for the second .PST, etc. (System administrators can decide where/how to split the content among multiple CDs.)

10) CD markings:

- a. CDs from OpenNet, POEMS and PACE should be marked "SBU" (i.e., content not intended for public disclosure in accordance with 12 FAM 5400). CDs from ClassNet must be marked "Secret" (12 FAM 632.1-6).
- b. CDs must be marked with the user's name and office symbol or Post (example: John H. Doe, IRM/OPS/MSO).
- c. CDs must be marked with the users SMTP address (example jdoe@state.gov or jdoe@state.sgov.gov).
- d. In the event .PST exceeds one CD, the CDs must include X of Y (example, 1 of 3.)

11) Distributed System Administrator roles:

- a. IRM will handle CD production for email accounts of users under IT Desktop Consolidation.
- b. Bureau/Office system administrators will handle CD production for email accounts that are NOT managed under IT Desktop Consolidation.
- c. Post system administrators should handle CD production for their email accounts.
- d. IRM's IT Service Center (IT Service Center@State.gov or (202) 647-2000) will be available to assist Post and Bureau system administrators with technical support for the .PST and CD creation process.

12) System administrators must NOT delete the source mailbox or .PST files until after receipt of an email confirmation from A/GIS/IPS/RA and authorization to delete.

13) Technical questions relating to the CD creation can be sent to the IT Service Center on OpenNet at ITServiceCenter@state.gov or on ClassNet to ITServiceCenter@state.sgov.gov or by calling 202-647-2000. **Other questions can be sent to A/GIS/IPS/RA on OpenNet at records-dl@state.gov or on ClassNet at records-dl@state.sgov.gov.**

NOTE: Transferring records through Direct Network Transfer is *also an available option for the emails of Senior Officials*. For assistance, please contact records@state.gov.