



May 21, 2019

Electronic Messaging Recordkeeping Requirements

The emergence and widespread governmental adoption of digital technologies that create information subject to the retention and preservation requirements of the Federal Records Act (FRA; 44 U.S.C. Chapters 21, 29, 31, and 33), as amended, and the Presidential Records Act (PRA; 44 U.S.C. §§2201-2209), as amended, may be of interest to Congress, officials charged with maintaining government records, and the public.

Processes related to the preservation and archiving of born-digital record materials created by email (referred to in statute as electronic mail), text messages, mobile applications, and other forms of electronic messaging—whether created using official, governmental resources, or through personal devices owned by government employees—may be of interest to multiple audiences. Congressional interest arises from many perspectives, including compliance with federal recordkeeping laws, the consequence of more-complicated (and potentially incomplete) recordkeeping information, and the ability of Congress to conduct oversight of executive branch activities.

Are Electronic Messages Federal Records?

Records materials are defined not by the media used to store the information but rather by the content of the information itself. Federal records, as defined in Title 44, Section 3301, of the *United States Code*, are “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 ... 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.” If the information meets this definitional criteria, the information must be treated as a federal record, regardless of whether it is in email or other electronic message form.

The National Archives and Records Administration (NARA), which oversees the implementation of the FRA and PRA, issued Bulletin 2014-06, which explains that all agency-administered email accounts are likely to contain federal records. The guidance goes on to say, “Email sent on personal email accounts pertaining to agency business and meeting the definition of Federal records must be filed in an agency recordkeeping system.”

Creation and Maintenance of Electronic Messaging Records

In the course of their official duties, federal employees regularly create federal records and, therefore, have records management responsibilities. The FRA requires federal agency heads to “make and preserve records containing

adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency.”

NARA has promulgated regulations, pursuant to the FRA, stating that executive branch agencies must “create and maintain authentic, reliable, and usable records and ensure that they remain so” until they are provided to NARA for permanent retention or lawfully destroyed. NARA regulations further state that agencies must (1) “integrate records management ... into the design, development, and implementation of electronic information systems,” (2) provide records management guidance and training to all agency personnel, and (3) conduct formal evaluations of the records management effectiveness.

Office of Management and Budget (OMB) Memorandum M-12-18 required agencies to maintain all email records in an accessible electronic format by 2016 and similarly maintain all permanent electronic records by the conclusion of 2019. According to the 2017 Federal Agency Records Management Report on Federal Email Management, issued by NARA after conducting the Records Management Self-Assessment survey (RMSA), 97% of agencies self-reported that they would meet the 2019 deadline.

Identifying and Collecting Records

For Congress and the public to have a complete understanding of agency actions, it is important for agencies to identify and collect electronic messaging records as completely as possible. In practice, however, questions regarding the use of official and personal accounts and the diversity of platforms used to create government records may make a complete collection difficult.

What Is a Non-Official Electronic Messaging Account?

Prior to the enactment of the Presidential and Federal Records Act Amendments of 2014 (P.L. 113-187) in November 2014, the FRA included no explicit language limiting the use of personal electronic messaging to conduct official federal business. Additionally, no timeline existed within the FRA requiring the forwarding of any record created on personal email accounts.

Under P.L. 113-187, executive agency employees are generally prohibited from creating or sending records via a “non-official electronic messaging account” unless the employee copies an official electronic messaging account when sending the message or forwards a copy of the record to an official electronic messaging account no later than 20 days after the original creation or transmission of the record (44 U.S.C. §2911). Similar requirements exist for

presidential and vice presidential records (44 U.S.C. §2209).

Despite these requirements, there appears to be no statutory or regulatory definitions of *non-official electronic messaging account* or *official electronic messaging account*. This ambiguity might create inconsistencies and confusion about the use, access, and disposition of records materials under the FRA and PRA and raises questions for Congress, including:

- Should email accounts through which official business is conducted be government-owned?
- When (if ever) and how should official messages use private applications?
- Should government communications on other applications also be forwarded if technically feasible?
- What happens when private platforms retain records of official government action?

NARA Bulletin 2014-02 provides related guidance but does not fully answer these questions. The bulletin notes that federal agencies must “determine the most appropriate ways to incorporate recordkeeping requirements into their business processes and identify the specific means by which their agencies will fulfill their responsibilities under the Federal Records Act.”

Required Email Record Information

NARA guidance (36 C.F.R. §1236.22) requires certain forms of information be preserved along with email records in particular, including:

- the names of the senders and all addressees, including linking codes or nicknames to the full names of the senders;
- the date the message was sent;
- attachments preserved as part of the email record or linked to the record;
- calendar and task list items if these items meet the definition of *federal record*; and
- draft documents that meet the definition of *federal record*.

Accuracy of Records

As with any federal record, Title 44, Section 3105, of the *United States Code* prohibits the destruction or alteration of electronic records. NARA defines *alteration* as “the unauthorized annotation, addition, or deletion to a record” (36 C.F.R. §1230.3). Agency heads are responsible for maintaining the integrity of federal records, and attempts to alter or unlawfully destroy records are to be reported to NARA. Additionally, the removal, mutilation, or destruction of records is punishable by both fines and imprisonment under Title 18, Section 641, and Title 18, Section 2701, of the *United States Code*.

Storing Electronic Messaging Records

For electronic messaging records to be useful to members of the public, federal employees, and Congress, records must be usable, unaltered, and reliably retrieved for years to come. To accomplish this, NARA guidance and OMB Circular A-130 on “Managing Information as a Strategic Resource” stipulate criteria for appropriate records management and information technology systems.

Circular A-130 primarily governs the security and supervision of government information technology systems. NARA’s storage guidance focuses on the records capacity of the system. In addition to each agency complying with Title 44, Section 3506, of the *United States Code*—which, among other things, requires periodic review of information technology systems—NARA requires agencies to specify forward-thinking criteria to assist records use and retrieval in the future, such as:

- specifying technical characteristics necessary for reading and processing the records;
- defining the contents, determining the restrictions on access and use, and identifying all inputs and outputs;
- understanding the purpose(s) and functions(s) of the system;
- describing update cycles or conditions for adding, changing, or deleting information; and
- ensuring the authorized disposition of records.

Considerations for Congress

Questions regarding the effectiveness of electronic messaging management policies remain for Congress, which may wish to consider the following matters:

Whether agencies are able to comply with existing policy. NARA conducts the RMSA to oversee electronic records management, including electronic messaging. However, the data are self-reported by the agency. NARA acknowledges that it might have to conduct oversight in cases of extreme response changes.

Retention and preservation of electronic messaging records. NARA requires electronic records be copied to “tested and verified new electronic media” before the media on which the records are stored are 10 years old (36 C.F.R. §1236.28). However, the guidance does not specify how these new electronic media are to be verified or by whom.

The capacity of agencies and NARA to preserve digital records and the long-term usability of those formats. By 2022, NARA intends to only accept records in an electronic format. Congressional oversight concerns might include consideration of whether the criteria for making complete electronic messaging and email records are adequate and whether agencies and NARA will have the capacity and technical components in place to ensure a robust capacity to preserve and retrieve government information.

Meghan M. Stuessy, mstuessy@crs.loc.gov, 7-1281