# Exhibit 4

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

AMERICAN OVERSIGHT,

Plaintiff,

v.

PETE HEGSETH, in his official capacity as Secretary of Defense, *et al.*,

Defendants.

Civil Action No. 1:25-cv-883

**DECLARATION OF CHRISTOPHER PILKERTON**

I, Christopher Pilkerton, declare under penalty of perjury:

1. I am the Acting General Counsel at the Department of the Treasury (Treasury), and I have served in this role since February 27, 2025. From January 27, 2025 until becoming Acting General Counsel on February 27, 2025, I served as Counselor to the Treasury Secretary. I am a non-career appointee, reporting directly to the Secretary. In my current role, I am the primary aide to the Secretary concerning legal matters and am responsible for exercising supervision over the Treasury Legal Division.
2. I am familiar with the claims asserted against Secretary Scott Bessent, in his official capacity as Secretary of the Treasury, in the above-captioned action regarding the "Houthi PC Small Group Chat," as referenced in the Amended Complaint ¶ 2, ECF No. 17. Based on personal knowledge and information provided to me in the course of my official duties, I provide this declaration in support of the Defendants' Opposition to the Plaintiff's Motion for a Preliminary Injunction.

3. Attachment A to this declaration is Treasury Directive Publication 80-05 (TDP 80-05), which is currently in force and "establishes basic policy and operating requirements for records management programs within the Department of the Treasury." *See* Attachment A, at 4.

4. Section 3.4 of TDP 80-05, pertains to encrypted applications and states:

> In general, Treasury staff may not use encrypted applications like "WhatsApp" or "Signal" to conduct Treasury-related business. In the even that Treasury staff are in a situation or location where they must use encrypted application to protect Treasury records from risk of unauthorized disclosure, such as during official travel overseas, staff may request temporary use of encrypted applications from the Office of the Chief Information Officer. To prevent the misuse of encrypted applications, they may only be used for an approved, limited period of time in which there is a high risk of unauthorized disclosure. Staff who use encrypted applications for Treasury business are required to forward any Treasury-related messages to non-encrypted Treasury messaging systems within twenty days. This ensures Treasury records are captured, accessible, and maintained under approved records schedules. pertaining to records management at the Department.

*See* Attachment A, at 24.

5. As I previously stated in my declaration in this case dated March 27, 2025 (March Declaration), on March 26, 2025, I sent separate but identical memoranda to Secretary Bessent and Treasury Chief of Staff Daniel Katz, instructing them to take any steps necessary to preserve all existing communications they have sent or received related to the conduct of Treasury business using any electronic messaging application, including but not limited to Signal. I further instructed them that their obligation to preserve records also extends to messages created in the future, and that the preservation requirement applies regardless of whether the messages were created or received using a Treasury-issued device or a personal one.

6. As I further stated in my March Declaration, on March 27, 2025, images were taken from the phones of both Secretary Bessent and Mr. Katz of all existing messages from the "Houthi PC Small Group Chat" and emailed to both Secretary Bessent and Mr. Katz. The existing messages from the "Houthi PC Small Group Chat" consist of all messages from the chat

beginning with a message from Michael Waltz at 1:48pm on March 15, 2025. These messages are now preserved in the Treasury email accounts of both Secretary Bessent and Mr. Katz.

7. On March 28, 2025, additional images were taken from the phone of Secretary Bessent of all remaining existing messages in his Signal account, in addition to the messages from the Houthi PC Small Group Chat referenced in paragraph 6, above. These messages are now preserved in Secretary Bessent's Treasury email account.

8. Treasury received an email from the White House Counsel's Office on April 8 containing a consolidated version of the Signal group chat referenced in the March 24 and 26, 2025 articles in The Atlantic, which was created for federal records purposes. The document was created based on publicly available information and information saved from participants' phones. The document includes content that has not been published by The Atlantic. This document is now saved in Federal Records Act-compliant systems of the agency.

Executed on: 5/7/25

Signed: _____

Christopher Pilkerton
Acting General Counsel
U.S. Department of the Treasury

# Attachment A

# TREASURY DIRECTIVE PUBLICATION 80-05

# RECORDS MANAGEMENT

## FINAL

January 31, 2018

## Table of Contents

**Treasury Directive Publication (TD P 80-05)**

**Records Management**

The issuance of this Treasury Directive Publication (TD P) has been authorized by Treasury Directive (TD) 80-05, "Department of the Treasury Records Management" (Date: TBD).

This TD P establishes basic policy and operating requirements for records management programs within the Department of the Treasury (Department), in furtherance of Treasury Directive 80-05 and applicable federal records law and regulations.

# *1 Introduction*

The Federal Records Act (44 U.S.C. 3101 et. seq.) and related regulations (36 CFR 1222) require each federal agency to make and preserve records necessary to document the agency's policies, decisions, procedures, and essential transactions, as well as protect the legal and financial rights of the U.S. Government. Each federal agency must also maintain an active, continuing program to manage its records efficiently and provide effective controls over the creation, maintenance, and use of records in conducting current business.

In support of these requirements, the Office of Privacy, Transparency, and Records (PTR) has created policies and procedures to manage federal records within the Department. These policies and procedures are also intended to ensure that Treasury bureaus maintain active and effective records management programs.

## *1.1 Authority*

This publication, TD P 80-05, is issued under the authority of TD 80-05. This publication supersedes TD P 80-05, Records and Information Management Manual, dated June 27, 2002, which described the Departmental records management program, policies, and guidance.

## *1.2 Scope*

This publication establishes standards and basic requirements for managing records management programs within the Department.

## *1.3 Applicability*

This TD P sets forth records management standards for Departmental Offices (DO), Treasury bureaus, and the Offices of Inspectors General (collectively, bureaus). The primary audience for this TD P is the bureau records management programs and their leadership, with the support and

participation of all other personnel, including employees, contractor employees, detailees, and interns.

The provisions of this TD P may not be construed to interfere with, or impede the authorities or independence of the Treasury Inspector General, the Treasury Inspector General for Tax Administration, or the Special Inspector General for the Troubled Asset Relief Program.

# *2 Policy*

## *2.1 General*

Bureaus must ensure that their records management policies address key records management requirements, which are organized into the following three categories:

- Primary records management requirements
- Email management requirements
- Electronic records management requirements

## *2.2 Primary Records Management Requirements*

Bureaus must establish policies to ensure the appropriate management of records throughout their entire records life cycle, including basic safeguards against unauthorized access and/or destruction.

*Note:* Any bureau whose records fall within a Departmental Offices records group (such as RG 056) must coordinate with and otherwise support PTR efforts to meet the requirements below.

### *2.2.1 Types of Records*

The Federal Records Act (44 U.S.C. 3301 et. seq.) defines records to include “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”.

Bureaus may issue policies or other guidance to interpret, further define, or otherwise clarify the definition of “records” according to their business needs, consistent with the legal definition above. For example, a bureau may choose to identify specific types of information that the bureau will treat as records, or specific circumstances under which the bureau treats certain documents (such as working drafts) as records.

Bureaus may also issue policies or other guidance to interpret or otherwise clarify the terms "non-records" and "personal documents" for bureau business purposes. Both of these types of materials are excluded from the legal definition of "records."

### *2.2.2 Information Inventory*

Bureaus must ensure that a comprehensive information inventory – i.e., a systematic review of the records types and non-records, the location of such information, and other factors needed to assess the bureau's records management practices – is conducted on a periodic basis. The information inventory should allow the bureau records management program to identify:

- Any unscheduled records (i.e., records that have not been assigned a NARA-approved records schedule or General Records Schedule)
- Other gaps in records management practices – for example, opportunities to improve the documentation of official actions, office filing processes, disposal of non-record materials, and/or identification of essential records

Bureaus may, in their discretion, establish policy prescribing the time and method for conducting information inventories, according to their business needs. For example, such policy may require an information inventory to be conducted at a specified organizational level (e.g. program office, business unit, or division) and/or at a specified interval (e.g. quarterly, annually, or biannually).

Bureaus may also require the affected organizational unit (e.g., program office) to designate a liaison(s) to conduct, lead, or otherwise assist in the information inventory.

### *2.2.3 Records Scheduling Activities*

Bureaus must take steps to update any existing records schedule(s) and establish any new records schedule(s) as appropriate, based on the records analysis above and bureau business need. Bureaus must comply with applicable NARA requirements on the development of records schedules – for example, ensuring they address media neutral formatting guidelines.

Bureaus must identify:

- Existing (bureau-specific) records schedules that require updating
- New (bureau-specific) records schedules that must be established
- General Records Schedule items that may apply to the records types in question

Bureaus may, in their discretion, prescribe the time and manner for conducting the activities in this section **2.2.3**. For example, bureau policy may permit the development of an interim file plan (discussed in section **2.2.4** below), based on existing records schedules, prior to preparing new or updated records schedules for NARA approval.

*Note:* Any bureau whose records fall within any Departmental Offices records group (such as RG 056) must coordinate their records scheduling activities – including use of the NARA Electronic Records Archives system – with PTR.

Bureau policy may also require the affected organizational unit (e.g., program office) to designate a liaison(s) to support these activities.

### *2.2.4 File Plans*

For purposes of this section, a file plan is a document providing instructions on how a specific organization unit (such as a program office) will organize and maintain its business information. Bureau policy must ensure that a file plan(s) is developed and updated on a periodic basis. The file plan should include:

- The types of records within the affected organizational unit (e.g., program office)
- For each records type, the applicable –
  - File code/number or unique identifier
  - The organizational unit that maintains ownership and control, including the name and title of any individual point of contact
  - Records schedule (whether bureau-specific or a General Records Schedule)
  - Retention period
  - Records management handling and disposition instructions (including, but not limited to "cut-off period")
- Description of each records type
- The physical storage location(s), in the case of paper records including off-site storage
- For electronic records, the applicable –
  - Electronic storage location(s) (such as directory name or address)
  - File naming conventions
- Records that are considered "essential records" (discussed in section **2.2.5** below)

Bureaus are strongly encouraged to include additional types of information in the file plan(s) according to business need. For example, a file plan may include Privacy Act related information, such as whether each record type contains personally identifiable information (PII) or Privacy Act information (if the PII meets the Privacy Act requirements for a record maintained in a system of records) and is the subject of a Systems of Records Notice.

Bureaus may establish policy governing the time and manner for establishing and updating the file plan(s), as business needs may require. For example, such policy may require a file plan to be prepared at a specified organizational level (e.g., program office, business unit, or division) and updated at a specified interval (e.g., quarterly, annually, or biannually).

Bureau policy may permit the development of an interim file plan, based on existing records schedules, prior to preparing new or updated records schedules for NARA approval (discussed in section **2.2.3** above).

Bureau policy may require the affected organizational unit (e.g., program office) to designate a liaison(s) to lead or otherwise assist in the creation of the file plan(s) and making updates thereto.

### *2.2.5 Essential or Vital Records*

Federal regulations (36 C.F.R. part 1223 or its successor) define "essential" or "vital" records (collectively, essential records) as those needed to:

- Meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records), or
- Protect legal and financial rights of the U.S. Government and those affected by U.S. Government activities (legal and financial rights records)

Bureau policy must ensure the identification and protection of essential records, and in particular:

- Designate staff responsibilities to identify and protect essential records
- Inform staff about essential records
- Ensure that documentation of essential records is current and complete
- Ensure that essential records are accessible and immediately usable
- Comply with applicable national continuity requirements, such as FEMA Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements* (attached as **Appendix A**)

Bureaus are encouraged to establish an essential records plan to ensure that essential records are periodically assessed, documented, and protected. Bureaus may choose to develop an essential records plan on a stand-alone basis, or as part of other operational planning efforts, such as the bureau Continuity of Operations Plan or Emergency Action Plan.

Bureau policy may require affected organizational units (e.g., program offices) to designate a liaison(s) to lead or otherwise support the identification, documentation, and protection of essential records.

### *2.2.6 Permanent Records*

Permanent records are those that NARA has determined to have sufficient historical or other value to warrant continued preservation by the U.S. Government. Bureau policy must ensure that permanent records are:

- Identified, assigned to an appropriate records schedule, and preserved until their eventual transfer to NARA custody
- Maintained in a manner that allows efficient access and use, to the extent needed for current business operations

- Stored in a manner consistent with applicable NARA requirements
- Not intermixed with temporary or other types of permanent records

*Note:* Any bureaus whose permanent records fall within any Departmental Offices records group (such as RG 056) must coordinate with, and provide support to PTR in scheduling, maintaining, and transferring such records.

See section **2.4.1** below for requirements specific to permanent electronic records.

#### *2.2.6.1 Listing of Permanent Records*

Bureaus must ensure that the bureau records management program identify and keep track of bureau permanent records as needed to meet NARA requirements.

Bureau records management programs are strongly encouraged to maintain and periodically update a list of permanent records (with the full cooperation and support of the program offices that created and/or maintain such records). Bureaus may exercise discretion to determine:

- The types of information contained by the list (e.g., records schedules (including item numbers), locations (physical and electronic), custodians, and NARA transfer instructions)
- The organizational level at which to track permanent records (e.g., program office, business unit, division, or bureau-wide)
- The time and manner for updating the list (e.g., quarterly, annually, or biannually)

Bureaus may establish an interim list of permanent records, based on existing records schedules, prior to preparing new or updated records schedules for NARA approval (discussed in section **2.2.3** above).

Bureaus may require the affected organizational unit (e.g., program office) to designate a liaison(s) to lead or otherwise assist in the creation of the permanent records list and making updates thereto.

#### *2.2.6.2 Transfer of Permanent Records to NARA*

Bureaus must ensure that permanent records are transferred (accessioned) to the permanent legal custody of NARA, according to applicable records schedules. Among other requirements, bureaus must establish policy as needed to timely and consistently transfer permanent records to NARA custody. For example, such policy may require program offices to:

- Verify that no litigation or other “hold” applies to permanent records that are being considered for transfer
- Take active steps to prepare permanent records in their custody for transfer

- Verify that permanent records stored in a NARA records center are appropriate for transfer to NARA custody

Bureaus may establish policy requiring a periodic review of permanent records to ensure the timely transfer of such records to NARA custody. Bureaus may also establish policy governing the time and manner for such a review, as business needs may require. For example, such policy may require the review to be conducted at a specified organizational level (e.g., program office, business unit, or division) and according to a specified interval (e.g., quarterly, annually, or biannually). Bureau policy may require affected organizational units to designate a liaison(s) to support these efforts.

A bureau may choose to store permanent records at a NARA records center at an earlier time – i.e., before transfer to NARA custody is scheduled to occur. The bureau must ensure that such records are no longer necessary for current business operations. All permanent records stored in this fashion remain in the bureau's legal custody until such custody is transferred to NARA, in accordance with applicable records schedules and other NARA requirements.

#### *2.2.6.3 Additional Requirements*

Bureau policy may impose additional requirements to ensure preservation of, and access to permanent records kept in the bureau's possession, according to business need. For example, bureau policy may establish requirements regarding:

- Centralized storage (e.g., in a common electronic and/or physical repository, managed by the bureau records management program) of permanent records that are needed for current business operations
- Interim storage (e.g., at a records center or bureau holding area) of permanent records that are no longer needed in current business operations, but are not yet ready for scheduled transfer to NARA
- Physical conditions of bureau holding areas (such as temperature and humidity) and controls
- Special media formats (e.g., audiovisual, cartographic, or microform records)

### *2.2.7 Temporary Records*

Temporary records are those that NARA has determined to be non-permanent and thus may be disposed of after their retention period has expired. Bureau policy must ensure that temporary records are:

- Identified, assigned to an appropriate records schedule, and preserved until their eventual disposition
- Maintained in a manner that allows efficient access and use, as needed for current business operations
- Not intermixed with permanent records

*Note:* Any bureau whose temporary records fall within any Departmental Offices records group (such as RG 056) must coordinate with, and provide support to PTR in scheduling, maintaining, and disposing such records.

See section **2.4.2** below for requirements specific to temporary electronic records, as well as requirements for temporary records sent to NARA after December 31, 2022 (or other date prescribed by NARA).

#### *2.2.7.1 Disposal of Temporary Records*

NARA-approved retention periods for temporary records are normally mandatory. Accordingly, bureaus must ensure, to the fullest extent possible, that temporary records are timely disposed of when their prescribed retention periods have expired. However, prior to disposition, bureaus must ensure that:

- The records custodian (e.g., program office) receives advance notice of any impending disposal and approves thereof
- No litigation or other "holds" apply to the records in question
- Records are disposed of according to NARA regulations, procedures, and other guidance
- Records that contain any restricted information (e.g., personally identifiable information) are disposed of according to applicable information protection requirements (e.g., Privacy Act)

Bureaus may establish policy requiring a periodic review of temporary records to ensure the timely disposal of such records. Bureaus may also establish policy governing the time and manner for such a review, as business needs may require. For example, such policy may require the review to be conducted at a specified organizational level (e.g., program office, business unit, or division) and according to a specified interval (e.g., quarterly, annually, or biannually). Bureau policy may require affected organizational units to designate a liaison(s) to support these efforts.

Bureaus may, through formal policy or on an ad hoc basis, make exceptions to the mandatory disposal of temporary records according to business need. For example, a bureau may decide that individual documents (otherwise considered to be temporary records) deserve special consideration due to Congressional or national media attention, or significant changes in bureau policy or procedures. Bureaus are strongly urged to weigh the operational impact of such exceptions and should consult with NARA and PTR before proposing a different disposition period for the documents in question.

#### *2.2.7.2 Additional Requirements*

Bureau policy may impose additional requirements to ensure preservation of, and access to temporary records kept in the bureau's possession, according to business need. For example, bureau policy may establish requirements regarding:

- Centralized storage (e.g., in a common electronic and/or physical repository, managed by the bureau records management program) of temporary records that are needed for current business operations
- Interim storage (e.g., at a records center or bureau holding area) of temporary records that are no longer needed in current business operations, but are not yet ready for disposal
- Physical conditions of bureau holding areas (such as temperature and humidity) and controls
- Special media formats (e.g., audiovisual, cartographic, or microform records)

### *2.2.8 Classified Records and CUI*

Bureau policy must ensure that all records considered to be classified or otherwise restricted are secured and maintained at their appropriate security level, in accordance with Executive Order 13526 and related requirements.

Bureau policy must also ensure that all records considered to be controlled unclassified information (CUI) are secured and maintained consistent with NARA and related requirements.

### *2.2.9 Removal of Information (Departing Personnel)*

Bureau policy must ensure that departing personnel take steps necessary to manage and preserve records as part of their departure process. In particular, bureaus must:

- Prohibit the unauthorized removal, deletion, or other destruction of records
- Prohibit (or restrict) the removal of information when –
    - Disclosure of such information is protected (or otherwise limited) by statute, regulations, or other authorities
    - Other business needs require such prohibition (or restrictions) – for example, to protect the ability to assert a legal privilege

In addition to these requirements, bureaus are strongly urged to:

- Take steps to ensure that departing personnel's records and other business information are available to their successors
- Support efforts by departing personnel to review and dispose of non-records and personal documents maintained in agency physical space and/or IT systems

Bureaus have discretion to allow departing personnel to remove specified types of information, other than those described above (for example, extra copies of publicly available records).

Bureaus also have discretion to establish appropriate controls on the removal of information by departing personnel, including:

- Bureau review and approval of any proposed removal of information
- Exit interviews for departing personnel to discuss the requirements of this section
- Certification by departing personnel and supervisors of compliance with such requirements (see, for example, Treasury Directive Form TD F 80-05.5, *Removal of Information*, attached as **Appendix B)**

### *2.2.10 Contracting/Procurement*

Bureau policy must, to the fullest extent possible, integrate records management obligations into their existing procurement processes. For example, bureaus must have policies and procedures in place that ensure that a contractor who holds federal records:

- Treats such records as the legal property of the bureau
- Manages them according to applicable records law, regulations, and policy
- Provides for the secure storage and retrieval of records
- Facilitates the transfer of permanent records in the contractor's possession to NARA, in accordance with section **2.2.6** above
- Facilitates the disposal of temporary records in the contractor's possession, according to established records schedules and section **2.2.7** above

Bureaus should ensure that contracts impose clear legal obligations on contractors to appropriately handle and manage federal records. Bureaus should ensure that contracts contain appropriate records management language, including any language required by procurement regulations or policies.

Bureau policy must ensure that records management program staff and liaisons have the appropriate clearance level needed to handle such records.

## *2.3 Email Management*

Bureau policy must ensure that email – including messages that are records, non-records, or personal in nature – is managed in accordance with TD 80-07, *Department of the Treasury Email Management*, and TD P 80-07, *Email Management*. Bureau policy must also ensure that instant messages that are created or received on a Treasury electronic mail system are managed according to TD 80-07 and TD P 80-07.

*Note:* The requirements of this section also apply to instant messages createdt or received on a Treasury email system (such as messages created or received through Microsoft Office Communicator). Instant messages sent or received outside of a Treasury email system are subject to the requirements of section **2.4.3** below.

### *2.4 Electronic Records Management*

Bureaus must establish policies to ensure the appropriate management of electronic records throughout their entire records life cycle as well as ensure basic safeguards against unauthorized destruction, as well as compliance with NARA regulations and guidance.

*Note:* Any bureaus whose records fall within a Departmental Offices records group (such as RG 056) must coordinate with and otherwise support PTR efforts to meet the requirements below.

#### *2.4.1 Permanent Electronic Records*

In addition to the requirements of section **2.2.6** above, bureaus must ensure that, by December 31, 2019, and to the fullest extent possible, permanent electronic records are:

- Managed in an electronic format
- Transferred to NARA possession/custody in an electronic format

Bureaus must comply with all OMB and NARA requirements for permanent electronic records, including those pertaining to format, metadata, and transfer methods.

Bureaus may, in their discretion, determine the manner for managing permanent electronic records, consistent with the requirements above. For example, bureaus may choose to:

- Consolidate all permanent electronic records within a single, enterprise-wide electronic repository
- Assign responsibility for managing permanent electronic records to a specific organizational unit(s) (for example, the bureau records management program or the program offices that generated/use such records)
- Pursue the goals of permanent electronic records management on a stand-alone basis, or as part of other records management initiatives –for example:
    - Managing temporary records in an electronic format (see section **2.4.2** below),
    - Development of file plans (see section **2.2.4** above)

#### *2.4.2 Temporary Electronic Records*

In addition to the requirements of section **2.2.7** above, bureaus must ensure that temporary records sent to NARA after December 31, 2022 (or other date prescribed by NARA) are in approved electronic formats with appropriate metadata. After such date, bureaus must obtain express NARA approval to send temporary records in analog formats.

Bureaus must comply with all OMB and NARA requirements for temporary electronic records, including those pertaining to format and metadata.

Bureaus may, in their discretion, determine the manner for managing temporary electronic records according to business need, consistent with the requirements above. For example, bureaus may choose to:

- Establish a default records schedule(s) and retention period(s) for electronic records, as appropriate
- Require that temporary electronic records be maintained only in a designated electronic repository (or repositories)
- Require that documents maintained outside of designated electronic repositories be managed as non-records
- Assign responsibility for managing temporary electronic records to a specific organizational unit(s) (for example, the bureau records management program or the program offices that generated/use such records)
- Pursue goals relating to temporary electronic records management on a stand-alone basis, or as part of other records management initiatives –for example:
    - Managing permanent records in an electronic format (see section **2.4.1** above),
    - Development of file plans (see section **2.2.4** above)

### *2.4.3 Instant Messaging*

Bureaus must issue policy on management of instant messages, i.e., electronic messages sent or received on Treasury systems via –

| **Type** | **Examples** |
|---|---|
| Text messaging services | • SMS (Short Messaging Service)<br>• MMS (Multimedia Messaging Service) |
| Instant messaging applications | • Skype for Business<br>• iMessage (Apple)<br>• WhatsApp<br>• Facebook Messenger |

*Note:* The requirements of this section do not apply to instant messages that are created or received on a Treasury email system, (such as messages created or received through Microsoft Office Communicator ). Bureaus must ensure that policy on such messages meets the requirements of TD 80-07, *Department of the Treasury Email Management*, and TD P 80-07, *Email Management*.

Bureau policy must ensure the capture and management of instant messages that constitute federal records, consistent with the requirements of section **2.2** above and applicable portions of this section **2.4**. Bureaus may exercise discretion to:

- Establish a default records schedule(s) and retention period(s) for instant messages

- Require personnel to copy or forward instant messaging records to designated recordkeeping repositories (such as email)

Notwithstanding these requirements, bureaus may exercise discretion to restrict the use of instant messages according to business need. For example, bureaus may choose to:

- Limit the use of instant messages to transitory or non-records communications
- Limit (or prohibit) –
  - Use of personal instant messaging accounts for official business
  - Use of official instant messaging accounts and/or devices to send/receive personal messages
  - Use/installation of specific instant messaging services or applications – for example, applications that encrypt or auto-delete messages

Bureaus may refer to Departmental Offices policy (attached as **Appendix C**) on instant messaging in developing equivalent policy.

### *2.4.4 Social Media*

Bureaus must issue policy on management of social media, i.e., forms of electronic communication (including websites and applications that facilitate social networking and microblogging) that allow users to generate and distribute online content. Such policy must ensure that social media content that constitutes federal records is captured and managed consistent with section **2.2** above and applicable portions of this section **2.4**.

Bureaus are strongly urged to:

- Determine whether an appropriate General Records Schedule or bureau-specific records schedule would be more suitable to manage social media records
- Provide supplemental guidance to distinguish social media records from non-records (covering,for example, the treatment of of public feedback on a bureau social media post)
- Use an internal (i.e. bureau) system to preserve bureau social media records, rather than rely on an external (e.g. Facebook or Twitter-based) system
- Designate the custodian(s) of social media records (e.g., office of public affairs, CIO, or program office that authored the social media records)
- Designate electronic format(s) for capturing social media records
- Periodically review recordkeeping copies of social media posts to ensure they capture the current (and any interim) online versions
- Remove social media content from the external system once the recordkeeping version has been disposed from the internal bureau system according to its established records schedule

Notwithstanding these requirements, bureaus may exercise discretion to manage the use of social media according to business need. For example, bureaus may choose to:

- Limit the use of social media to transitory communications
- Limit the ability to author social media content to designated program offices
- Limit (or prohibit) –
    - Use of personal social media accounts for official business
    - Use of official accounts and/or devices for personal social media purposes
    - Use/installation of specific social media websites or applications

Bureaus may refer to Departmental Offices policy (attached as **Appendix D**) on social media in developing equivalent policy.

### *2.4.5 IT Governance*

Bureau policy must ensure that records management requirements are fully incorporated into the planning of information technology strategy and systems.

Bureaus are strongly encouraged to:

- Include bureau records officers in IT strategic planning efforts and strategic plan development
- Appoint bureau records officers as voting members of IT governance bodies, including investment review boards and technical review boards
- Incorporate records management requirements into IT compliance efforts, such as those relating to the Privacy Act and OMB Circular A-130, *Managing Information as a Strategic Resource*

### *2.4.6 Cloud Computing*

Cloud computing refers to a model for enabling on-demand network access to a shared pool of computing resources (including servers, storage, applications, and services), as well as other characteristics defined by the National Institute of Standards and Technology (NIST). (See, for example, NIST Publication SP 800-145, *The NIST Definition of Cloud Computing*, or its successor.)

Bureau policy must ensure that records are managed in accordance to applicable law, regulations, and NARA guidance, regardless of cloud service model or provider. Among other requirements and to the fullest extent possible, bureau policy must ensure that:

- Cloud service providers are made aware of the record retention requirements for records stored in the cloud
- Bureaus have the ability to control any proposed deletion of records pursuant to existing records schedules, wherever the records may be located in the cloud

- Records are accessible to search in response to discovery, FOIA, or Privacy Act requests, or for other bureau business needs
- Records are portable and can be removed for recordkeeping purposes (e.g., transfer to NARA) or transition to another computing environment
- Records are preserved and accessible in the event of a contingency, such as a material change in the cloud service provider's business operations (including bankruptcy)

Bureaus may, in their discretion, determine the manner for managing records in cloud environments, according to business need and consistent with the requirements above. For example, bureaus may choose to:

- Establish a default records schedule(s) and retention period(s) for records stored in a cloud environment
- Define which copy of records will be declared as the bureau's record copy
- Require the inclusion of the bureau records officer in the planning, development, deployment, and use of cloud computing environments
- Perform a periodic inventory and records analysis of information (and in particular unscheduled records) stored in a cloud environment
- Periodically test transfers of records to other environments, including internal (bureau) servers, to ensure the records remain portable

Ultimately, an agency maintains responsibility for managing its records whether they reside in a contracted environment or under agency physical custody (see 36 CFR Part 1222.32 (b)). When dealing with a contractor, an agency must include a records management clause in any contract or similar agreement. At a minimum, a records management clause ensures that the federal agency and the contractor are aware of their statutory records management responsibilities.

## *3 Records Management Training*

To meet records management requirements, bureaus must develop training materials, delivery methods, and assessment processes to inform their personnel of records management responsibilities. Bureaus must periodically review and, as needed, revise such training materials, delivery methods, and assessment processes.

### *3.1 Records Management Training Program*

Bureaus must establish, or integrate into existing training programs, a records management training program to educate personnel to preserve and manage federal records consistent with the requirements of section **2** above.

Bureau training program(s) must comply with applicable OMB and NARA requirements for records management training. (See **Appendix E**, NARA Bulletin 2017-01, *Agency Records Management Training Requirements*, or its successor.)

Bureaus have discretion to deliver records management training and training materials in the manner they deem appropriate for their users' educational needs.

To help ensure effective records management training, bureaus may require program offices to designate qualified staff members to serve as liaisons to, and trainers on behalf of, the bureau records management program.

Bureaus must also implement and update training as needed.

### *3.2 Training, Reporting & Assessment*

Bureaus must periodically:

- Monitor and assess the effectiveness of their training programs and related processes
- Track training of new and current personnel
- Gather and incorporate feedback, as appropriate

Bureaus shall report on the foregoing to PTR as part of their Departmental records management reporting responsibilities.

PTR reserves the right to assess bureau training programs for compliance with Departmental policy.

## *4 Compliance & Oversight*

### *4.1 Records Officers and Liaisons*

To comply with OMB, NARA, and Treasury records management requirements, each bureau will designate a records officer to provide leadership for the bureau records management program. Among other duties, the bureau records officer is responsible for leading:

- Development of bureau records policy, consistent with section **2** above
- Bureau records training, consistent with section **3** above
- Bureau compliance processes, oversight activities, and reporting, consistent with this section **4**

The bureau records officer will act as liaison to PTR on records management matters affecting his or her bureau. Each bureau must notify PTR of their records officer on a semi-annual basis

(by the dates designated by PTR), and any change in records officer within five business days of such change.

Bureaus may exercise discretion to designate records liaisons to coordinate records management activities within the bureau. Bureaus may designate records liaisons at a specified organizational level (e.g., program office, business unit, or division) and/or for a specified term (e.g. annually, biannually, or until a new designation is made). Bureau records officers should consider maintaining a current list of records liaisons, updating it on a semi-annual basis, and requiring notification of any change in records liaison within five business days of such change.

### *4.2 Compliance Requirements*

Bureaus must incorporate records management requirements, including those set forth in section **2** above, into their records management programs, policies, and procedures.

Bureaus must establish compliance processes as needed to effectively implement the records management policies described in section **2** above.

Bureaus are strongly urged to foster cooperation and coordination, to the fullest extent possible, among all stakeholders whose involvement, participation, or support is required to implement effective records management processes.

### *4.3 Oversight Requirements*

As required by NARA, PTR will regularly evaluate and monitor the Department-wide records management program, including bureau-level records management programs.

Bureaus must regularly evaluate and monitor their records management program for effectiveness and compliance with applicable laws, regulations, and policies.

### *4.4 Reporting Requirements*

#### *4.4.1 Compliance Reporting*

Bureaus must support Department-wide external reporting on compliance with records management requirements including, for example, the submission of annual Senior Agency Official reports and Records Management Self-Assessments to NARA.

Bureaus must report the status of their compliance with the requirements of this TD P to PTR on no less than an annual basis.

The Department reserves the right to develop further reporting requirements as needs dictate.

### *4.4.2 Incident Reporting*

Each bureau must promptly report to NARA any unlawful or accidental removal, defacing, alteration, or destruction of records in that bureau's custody, in the manner prescribed by NARA regulations (36 CFR 1230 or its successor). Bureaus must ensure that appropriate reporting policies and procedures are in place to comply with NARA requirements.

Bureaus are strongly urged to include PTR on all reporting to and related communications with NARA under this section **4.4.2**, to the fullest extent possible.

## *5 Litigation Holds*

A litigation hold, or document preservation directive, is a temporary suspension of the disposition under the applicable records schedule for documents that are reasonably anticipated to be relevant to a lawsuit or related matter.

Bureaus must establish policies to ensure that bureau records are preserved in the event of a litigation hold. Bureaus must ensure that litigation hold processes are managed under the direction of the appropriate bureau chief counsel.

## *6 Freedom of Information Act*

Bureaus must establish policies to preserve, access, and search records to respond to requests under the FOIA. Bureaus must ensure that bureau FOIA offices direct any FOIA-related processes.

## *7 References and Authorities*

Federal Records Act, 44 U.S.C. Chapter 31 (revised 2014)

Treasury Directive 80-07, *Department of the Treasury Email Management*

Treasury Directive Publication 80-07, *Email Management*

Office of Management and Budget (OMB) Memorandum M-12-18, *Managing Government Records Directive*

Executive Order (E.O.) 13526, *Classified National Security Information*

OMB Circular A-130, *Managing Information as a Strategic Resource*

NARA Bulletin 2010-05, *Guidance on Managing Records in Cloud Computing Environments*

NARA Bulletin 2012-02, *Guidance on Managing Content on Shared Drives*

NARA Bulletin 2015-02, *Guidance on Managing Electronic Messages*

NARA Bulletin 2015-04, *Metadata Guidance for the Transfer of Permanent Electronic Records*

NARA Transmittal No. 26: General Records Schedule 6.1, *Email Managed Under a Capstone Approach* (issued September 2016)

National Archives Strategic Plan FY 2018-2022 (September 11, 2017 draft)

## *8 Appendices*

**Appendix A: FEMA Federal Continuity Directive 1**

**Appendix B: Treasury Directive Form TD F 80-05.5**

**Appendix C: Departmental Offices - Instant Messaging Guidance**

**Appendix D: Departmental Offices – Social Media Guidance** [Reserved]

**Appendix E: NARA Bulletin 2017-01**

**Appendix F: Departmental Offices – Records Management Guide (and FAQ)** [Reserved]

# *Text and Instant Messaging Records Policy*

*Appendix to Treasury Directive Publication 80-05*

FINAL

May 22, 2019

## *1.0 Introduction*

This document outlines the basic requirements for records management regarding text and instant messaging and serves as an appendix to Treasury Directive Publication 80-05.

## *2.0 Scope*

This policy establishes standards and basic requirements for managing text and instant messaging records within the Departmental Offices (DO). It applies to all DO employees, contractors, detailees, and interns who create, receive, or maintain records on behalf of Treasury.

## *3.0 Policy*

Treasury staff may use Treasury-provided text and instant messaging applications to communicate about internal business matters. Treasury staff should not use these formats to capture official business and decision-making communications; in the event that such information is transmitted over text or instant message applications, employees should take steps to manage and in some cases preserve this information if it documents business decisions or is otherwise important for programmatic purposes. This ensures that Treasury records are captured, accessible, and maintained under approved records schedules.

### *3.1 Records Creation*

Treasury staff must preserve text and instant messaging content from the system they use if such content contains information about Treasury business. Any text or instant messages created or received outside of Treasury systems which document Treasury business must be forwarded to an official Treasury-managed account within twenty calendar days of creation or receipt. These requirements apply to messages created or received in applications outside of the secure applications provided by Treasury on agency issued devices or on personal devices. Offices should determine the repository for storing records created in this manner. In the event a repository has not been designated, staff should forward the records to their Treasury email account.

### *3.2 Electronic Messaging Systems*

Treasury provides staff with applications for text and instant messaging, including Skype and Microsoft Communicator. Staff are expected to use these applications for Treasury-related text and instant messaging whenever possible.

### *3.3 Personal Applications and Devices*

In the rare event that a Treasury employee is unable to use a Treasury-issued text or instant message application, and sends or receives an instant or text message on a personal device or an application not provided by Treasury, the employee is required to forward that message to a Treasury-managed account within twenty days.

*3.4 Encrypted Applications*

In general, Treasury staff may not use encrypted applications like "WhatsApp" or "Signal" to conduct Treasury-related business. In the event that Treasury staff are in a situation or location where they must use encrypted application to protect Treasury records from risk of unauthorized disclosure, such as during official travel overseas, staff may request temporary use of encrypted applications from the Office of the Chief Information Officer. To prevent the misuse of encrypted applications, they may only be used for an approved, limited period of time in which there is a high risk of unauthorized disclosure.

Staff who use encrypted applications for Treasury business are required to forward any Treasury-related messages to non-encrypted Treasury messaging systems within twenty days. This ensures Treasury records are captured, accessible, and maintained under approved records schedules.

*3.5 Classified and Controlled Unclassified Information (CUI)*

This policy does not apply to classified information or CUI. Treasury staff may not use personal devices or applications to communicate classified information or CUI.

*3.6 Litigation Holds*

A litigation hold or document preservation directive creates a temporary suspension of the disposition under the applicable records schedule for documents that are reasonably anticipated to be relevant to a lawsuit or related matter. Litigation hold processes are managed under the direction of the Office of the General Counsel, which may choose to apply litigation holds or document preservation directives to text and instant messages.

*3.7 Retention Schedule*

The majority of text and instant messages created or received in the course of Treasury business are temporary federal records and will be maintained and destroyed according to an approved records schedule. Messages that do not document significant Treasury business or decisions should be destroyed according to General Records Schedule (GRS) 5.2, Transitory and Intermediary Records, item 010, which authorizes the disposition of transitory and intermediary records when no longer needed for business use.

If the content of a text or instant message captures significant agency business or decisions, or otherwise has long-term informational value (generally greater than 90 days) to Treasury, Treasury staff are required to maintain records in a system using Treasury's Records Control Schedules.

*3.8 Records Destruction*

Treasury staff may delete text or instant messaging content from the system they use, provided it has fallen under the definition of transitory information. Otherwise, they may not delete or remove messaging content prior to its records schedule disposal date.

## *5.0 Definitions*

a. Electronic messaging system: An electronic system which creates, receives, and maintains records.
b. Text messaging: Phone-to-phone short messaging services and multimedia messaging services.
c. Instant messaging: Computer-to-computer messaging services.
d. Text and instant messaging applications: Electronic messaging systems, i.e. Skype for Business, iMessage.
e. Encrypted applications: Instant messaging applications with features that include two-way encryption i.e. WhatsApp, Signal.
f. Records: Includes 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.
g. Transitory records: Short-term records are required only for a short time (generally less than 90 days) and are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision making.
h. Official Treasury-managed account: an account created and managed by Treasury for a business related purpose.