Records Management and Electronic Messaging Report

Introduction

This report is issued in accordance with Section 7077 of the Consolidated Appropriations Act, 2016 (P.L. 114-113), that the Secretary of State and the USAID Administrator shall each submit a report to the Committees on Appropriations and to the National Archives and Records Administration detailing, as appropriate and where applicable, the policy of each agency regarding the use or the establishment of email accounts or email servers created outside the .gov domain or not fitted for automated records management as part of a Federal government records management program; the extent to which each agency is in compliance with applicable Federal records management statutes, regulations, and policies; and, steps required, including steps already taken, and the associated costs of compliance.

This report provides the steps USAID has taken to update its policy in light of the most recent revisions to the Federal Records Act to ensure the agency remains in compliance with Federal records management statutes, regulations, and policies. These updates build on existing USAID policies that have continued to prohibit the use of personal emails to transmit official government correspondence as well as detailed requirements for email system security and communication protection both here in Washington as well as at overseas missions.

Section by Section Responses

Section 7077 (2)(A) through (C) of Section 7077(c) requires:

> ***2(A) the policy of each agency regarding the use or the establishment of email accounts or email servers created outside the .gov domain or not fitted for automated records management as part of a Federal government records management program;***

USAID's policy regarding the use or establishment of email accounts or email servers created outside the .gov domain or not fitted for the automated records management statutes, regulations, and policies is articulated in the Automated Directive System (ADS) 502, USAID's Records Management Program, as well as ADS 545, Information System Security, and ADS 549, Telecommunications Management.

ADS 545 provides guidance on *Email Security* and states that “[a]uto-forwarding or redirecting of USAID e-mail to address outside of .gov or .mil domains is prohibited.”

Further, ADS 549 reinforces the need for employees to refer to and adhere to the Agency’s “E-mail Acceptable Use Policy” and the “Standard for Managing Electronic Mail Records.”

In addition, ADS 549 outlines guidance on remote access and requires agency employees regardless of labor category to access media and conduct electronic messaging through Agency-sanctioned sites using the appropriate hardware and software tools issued by the Agency’s Bureau for Management’s Office of Chief Information Officer (M/CIO).

Finally, ADS 502 provides policy guidance to Agency employees regardless of labor category that addresses the use of non-official agency electronic systems to conduct official business. This Section now includes: (1) the requirement that when a non-official agency electronic system is used the message be transmitted back to an official agency record keeping system within 20 days; (2) the designation of certain positions as “senior officials” in the context of records management whose electronic messages will be retained permanently, and; (3) a strengthening of records management exit policy for departing employees.

The Agency has recently updated these policies to clarify the definition of what constitutes electronic messaging to align that definition with the changes made by the Presidential and Federal Records Act Amendments and guidance from NARA.

Attachments A and B provide excerpts from ADS 502 detailing policy guidance to Agency staff regarding electronic messaging.

2(B) the extent to which each agency is in compliance with applicable Federal records management statutes, regulations and policies;

USAID is in compliance with applicable Federal records management statutes and regulations. USAID is committed to sound records management practices and uses a myriad of approaches to ensure compliance with applicable Federal records management statutes, regulations and policies such as the Federal Records Act and related NARA guidance. The agency is currently implementing best practices around records management including:

- Consistently reviewing and updating records management policies;
- Issuing related policy reminders;
- Designing, developing and delivering training worldwide;
- Providing records management technical assistance and support;
- Conducting records management compliance reviews;

- Developing and providing informational literature and handouts (e.g., brochures, pamphlets, infographics, etc.); and
- Completing annual records management reporting requirements

More specifically, pursuant to the deliverables outlined in the November 2011 Presidential Memorandum on Managing Government Records, and corresponding guidance from NARA and OMB, USAID has:

- Named and annually reaffirmed Senior Agency Official (SAO);
- Completed and sent report to the Office of Management and Budget (OMB) and NARA on the status of progress toward the goal of managing all email records in an electronic format;
- Completed and submitted Annual Senior Agency Official for Managing Government Records Reports;
- Completed and submitted Annual Records Management Self-Assessments;
- Identified unscheduled records to ensure records schedules have been submitted to NARA for all existing paper and other non-electronic records;
- Completed required courses and obtained NARA certificate of Federal Records Management Training as required for the Agency Records Officer and USAID records staff;
- Started to develop and implement plans to transition to electronically manage all permanent electronic records for transfer and accessioning to NARA, and taken steps to ensure that records that have been retained by USAID for more than 30 years are being identified for transfer and reported to NARA; and
- Established various methods to inform employees of their records management responsibilities, including creating and updating policies, as well as developing and enhancing training and literature.

2(C) the steps required, including steps already taken, and the associated costs to -
i. comply with paragraph (1)(B) of this subsection
Subsection 7077(c)(1)(B) reads:
(B) The Secretary of State and USAID Administrator shall—

(i) update the policies, directives, and oversight necessary to comply with Federal statutes, regulations, and presidential executive orders and memoranda concerning the preservation of all records made or received in the conduct of official business, including record emails, instant messaging, and other online tools;

USAID has updated its policies and oversight to comply with applicable Federal records management statutes, regulations, and presidential executive orders memoranda. These include:

- Policy and procedures for the appropriate use of electronic messaging;
- Designation of Senior Officials positions for records management;
- Records Management Exit Policy and Checklist for Senior Officials; and
- Records Management Exit Checklist for Employees.

> ***(ii) use funds appropriated by this Act under the headings "Diplomatic and Consular Programs" and "Capital Investment Fund" in title I, and "Operating Expenses" in title II, as appropriate, to improve Federal records management pursuant to the Federal Records Act (44 U.S.C. Chapters 21, 29, 31 and 33) and other applicable Federal records management statutes, regulations, or policies for the Department of State and USAID;***

USAID uses appropriated Operating Expense and Capital Investment funds to ensure compliance with all Federal records statues and regulations. None of this funding is used to support the use or establishment of email accounts or email servers created outside the .gov domain or not fitted for automated records management as part of a Federal government records management program in contravention of the Presidential and Federal Records Act Amendments of 2014 (Public Law 113–187). We are constantly assessing various additional automated tools and other interventions that will improve our management of Federal records. However, we remain constrained due to the appropriated funding levels contained in the FY 2016 Omnibus and over the past few years. For instance, the appropriated FY 2016 Capital Investment Fund level for USAID is $168.3 million, which will have to be used to cover USAID's share of the Capital Security Cost Sharing bill, which leaves nothing for enhancements and investments in new information technologies. USAID continues to re-prioritize existing operational resources to support evolving and increasingly demanding records management activities, yet, with the funding made available and our good faith efforts, it is becoming more difficult to maintain or improve our management of these records.

With regard to records management, the Agency spends an estimated $1.8 million annually for the staff, recurring maintenance of automated tools and systems, and training related to records management. This amount includes the costs associated with the salary and benefits of records personnel, support costs for those personnel, including travel and training, and the delivery of in-person training.

A FY 2015 one-time cost associated with the development of on-line training curriculum for all labor categories was approximately $65,000.

In addition, storing large volumes of information and records both electronically and physically is costly and resource intensive, albeit necessary. The annual estimated electronic hosting costs are $6.7 million and physical storage costs beyond the work space, and external to the Agency, is an estimated $115,000 per annum.

With regard to associated costs expended on FOIA activities, in FY 2015 the total cost was comprised of personnel, litigation and training was approximately $2,656,000. In addition, the FOIA processing database has an estimated annual cost of $30,000 for maintenance, and the purchase of the de-duplication tool was a one-time cost of $70,000 with an annual maintenance cost of $26,000. Each year there has been an increase in FOIA processing costs due to the volume and complexities associated with backlogged and continuing new requests.

These estimates do not take into account the costs associated with Agency personnel staff time around the world to identify and review responsive documents prior to the FOIA office's final review and release determination(s).

(iii) direct departing employees that all Federal records generated by such employees, including senior officials, belong to the Federal Government; and

USAID updated Section 502 of its ADS policy to address records management requirements for departing employees, including senior officials, through an Exit Policy for Employees. The text can be found in Attachment B.

(iv) measurably improve the response time for identifying and retrieving Federal records.

USAID is using a multi-pronged approach to improve response time for identifying and retrieving Federal records. This approach includes: improved guidance; expanded training to our global workforce; and use of automated tools to identify official records responsive to any formal inquiry. Standard operating procedures include comprehensive annual file and inventory reporting by operating units to facilitate timely identification and location of records. Additionally, on-going training and technical assistance provided to USAID staff worldwide helps to ensure efficient and effective handling of records and contributes to streamlined practices. More than 800 employees have received records management training during the last twelve months. When records are stored and managed properly, coupled with tools to support and enhance electronic records searches, measurable reduction in response times for identifying and retrieving Federal records are realized. For example, Freedom of Information Act (FOIA) requests for multiple user emails on a given subject previously required manual search through individual accounts. Now, through the use of e-discovery tools, multiple accounts can be searched at once.

2(C)(ii) ensure that all employees at every level have been instructed in procedures and processes to ensure that the documentation of their official duties is captured, preserved, managed, protected, and accessible in official Government systems of the Department of State and USAID.

USAID has established various methods to instruct employees at every level in the proper procedures and processes to ensure that documentation of their official duties is captured, preserved, managed, protected, and accessible in official Government systems. In addition to maintaining written operational policy housed in ADS 502 which staff can access at any time and from anywhere, records management training is currently required for all new employees via USAID's New Employee Orientation program. In addition, USAID is developing a suite of records management trainings targeting specific employee types. On-line training is recommended to become a part of the Agency's mandatory training program and be available to all staff regardless of employment type. Records management is a key component of the worldwide Management Knowledge and Learning program which provides ongoing training and technical assistance to USAID staff in order to reiterate records management responsibility and ensure efficient and effective handling of records.

2(C)(iii) implement the recommendations of the Office of the Inspector General, United States Department of State (OIG), in the March 2015 Review of the State Messaging and Archive Retrieval Toolset and Record Email (ISP-1-15-15) and any recommendations from the OIG review of the records management practices of the Department of State requested by the Secretary on March 25, 2015, if completed.

This section is not applicable to USAID.

2(C)(iv) reduce the backlog of Freedom of Information Act and Congressional oversight requests, and measurably improve the response time for answering such requests.

USAID is committed to reducing the backlog of FOIA, 5 U.S.C. § 552, and Congressional oversight requests, and to measurably improve the response time to these requests. Various steps have been identified and implemented by USAID management to reduce the backlog and improve response time.

USAID is implementing various strategies and solutions to help eliminate the backlog and improve response times, including:

Improved Staffing:

- USAID expanded its FOIA records management staff to ensure continuity of operations and improve understanding of Agency initiatives, thus, increasing efficiencies in FOIA processing.

- In Fiscal Year (FY) 2015 USAID acquired FOIA surge support to assist the agency in reducing its backlog of requests.

- USAID expanded the role of its FOIA professionals to include assessing the release of data in response to the Open Data Initiative and in response to time-sensitive Congressional inquiries.

Improved Search Capability:

- USAID improved its record search capabilities through the use of ediscovery. The automated capability of electronic records searches - using key words and search terms - improves response times. When these documents are maintained in an electronic manner, it permits more efficient digital search versus manual searches of paper files in file cabinets and record retirement boxes.

- USAID also procured a tool to de-duplicate emails. This tool will facilitate FOIA professionals' ability to more quickly discern responsiveness of emails and further eliminate duplicates contained in threaded emails. This tool should help to realize improvements in response times.

Training:

- USAID added FOIA modules to its existing records management instructor-led training titled "Records Management and FOIA Access Training" as well as to the New Employee Orientation (NEO) training.

2(C)(v) strengthen cyber security measures to mitigate vulnerabilities, including those resulting from the use of personal email accounts or servers outside the .gov domain;

In order to continue to strengthen cyber security measures to mitigate vulnerabilities, including those resulting from the use of personal email accounts or servers outside the .gov domain, USAID has strong policies and requires regular training to ensure staff are aware of the policy and risks associated with non-compliance. USAID requires that employees and contractors annually complete both the security refresher and cybersecurity refresher training. Additionally, employees must sign and acknowledge the Agency's updated Rules of Behavior (RoB) annually.

Failure to complete the mandatory trainings results in the suspension of the employee's and/or contractor's ability to log on to any USAID information system, including USAID email.

2(C)(vi) codify in the Foreign Affairs Manual and Automated Directives System the updates referenced in paragraph (1)(B) of this subsection, where appropriate.

USAID has codified the relevant changes to the records management policies in ADS 502: The USAID Records Management Program; ADS 545: Information Systems Security, and ADS 549: Telecommunications Management.

Attachment A

502.3.4.6 Electronic Messaging

Effective Date: 03/09/2016

The Federal Records Act Amendments of 2014 (**44 USC 2911**) defines electronic messages as "electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals". As defined in **NARA Bulletin 2015-02**, electronic messaging (EM) includes all forms of email (electronic mail), texts, instant messages/chats, social media messaging systems, and voice message platforms. USAID further defines electronic messaging systems as tools, platforms, applications, or other systems used to conduct official business.

The table below (taken from **NARA Bulletin 2015-02** and expanded to include Agency specific information) provides several examples of EM, but should not be considered a complete listing of all EM categories.

Types of EM	Examples
Email	Gmail or Yahoo Mail
Chat/Instant messaging	Google Hangouts, Facebook Messaging, or MyUSAID Messaging
Text messaging, also known as Multimedia Messaging Service (MMS) and Short Message Service (SMS)	iMessage, devices such as Windows or Apple
Voicemail messaging • Can have voicemail sent to email as an attachment. • Messages can be sent or received from landlines or mobile phones.	Google Voice or voice to text conversion
Other messaging platforms or applications (apps), such as social media or mobile device apps. These include text, media, and voice messages.	Twitter Direct Message, Huddle, or other collaboration networks

Electronic messaging systems allow users to send communications in real-time or for later viewing, from one account to another. Some systems allow the use of attachments. USAID authorizes the use of official EM accounts and systems on the Agency network and/or Agency-owned devices/equipment, that are within the USAID.gov domain (see **ADS 545, Information Systems Security** and **ADS 549, Telecommunications Management**).

USAID EM systems are divided into two (2) categories:

Category	Description	Examples

Official EM Systems	Owned by USAID Approved by USAID to conduct Agency business	• usaid.gov email account • text messages from government furnished devices • MyUSAID • USAID Google Hangouts account
Non-official EM Systems	Owned by the employee, or others, not USAID Not approved by USAID to conduct Agency business	• non-official (personal and private) email accounts and servers • text messages from personal devices • non-MyUSAID social media sites • other commercial vendor accounts, systems, tools, or applications

USAID employees, regardless of labor category, must use Agency EM systems to conduct official business. The use of non-official EM systems is not permitted. Such use not only compromises the Agency's ability to preserve and protect Agency records, but could potentially lead to the mismanagement of Agency records and/or the unauthorized disclosure of non-public information. However, in limited exceptional circumstances, use of non-official EM systems may be necessary. To the extent that such use occurs in limited exceptional circumstances, the individual creating, sending, or receiving the record from a non-official electronic messaging system must copy/forward all records to an official USAID electronic messaging account.

These limited exceptional circumstances may include:

- Emergency situations resulting from disruptions to or loss of power that would impede an individual's access to the USAID network;

- The lack of access to or the inadvertent loss, theft, or malfunction of government furnished equipment (GFE);

- Forces of nature such as a catastrophic natural disaster;

- Severe extreme weather conditions such as floods or tornadoes;

- National security events or threats to personal safety; and

- The need to conduct official business during an emergency situation.

Note: Employees must properly document any use of an exceptional circumstance.
Any such use must be temporal in nature and discontinued once the exceptional circumstance no longer exists. Non-official EM systems must not be used to conduct official business as a matter of convenience, or as an ordinary course of business.

As required by **44 U.S.C §2911(a) of the Federal Records Act Amendments of 2014**, USAID employees must not create or send a record using a non-official electronic messaging account unless the employee:

(1) Copies an official electronic messaging account of the employee in the original creation or transmission of the record; or

(2) Forwards a complete copy of the record to an official electronic messaging account of the employee no later than **20 days** after the original creation or transmission of the record.

Forwarding emails from the employees' USAID account to their non-official email account is prohibited except under limited exceptional circumstances such as those referenced above. Actions such as these create records management challenges and cyber security vulnerabilities (see **ADS 545**).

The intentional violation of **44 U.S.C §2911(a) of the Federal Records Act Amendments of 2014** (including any rules, regulations, or other implementing guidelines), as determined by the appropriate supervisor, will be a basis for disciplinary action in accordance with subchapter 1, 11, or V of chapter 75 of title 5, and may include:

- Suspension for 14 days or less; and/or

- Removal, suspension for more than 14 days, reduction in grade or pay, or furlough.

As with all official records (**18 USC 2071**), including electronic messages, there are criminal penalties for the unlawful removal, defacing, alteration, alienation, or destruction of federal records.

Agencies are required to capture and manage electronic records in compliance with federal record keeping regulations (**36 CFR 1236.22** – **36 CFR 1236.28**). Electronic messages must be captured into an identifiable recordkeeping system to ensure effective records management practices. Additionally, electronic messages are official records and must be handled according to retention and disposition schedules.

Note: The creation, transmission, or distribution of classified information across an unofficial system is prohibited at all times. Any violation of this policy could result in adverse administrative actions and/or criminal penalties against the employee.

a. Additional Standards for Managing Electronic Mail (email) Records

Email records of Agency users must retain information about the receipt of messages if users consider it necessary for documenting Agency activities (i.e, metadata which includes the internal and external email message, any attachment, and essential transmission data such as, who sent the message, the addresses and any other recipients, and when it was sent). Additionally, draft documents, calendars, and task lists that are circulated on email systems can also be considered official Agency records and must be managed accordingly.

Agency employees must not dispose of email records unless the records have met retention requirements and are no longer needed for business use. If emails are ready for removal or destruction (also known as disposition), Agency employees may delete the email message. Alternatively, emails that have not served their retention and are still needed for business use can be moved to an Agency document management system for recordkeeping purposes (e.g., Huddle, Google Drive, Documentum, etc.). Agency employees must manage emails in accordance with the following guidelines:

- **Transitory or personal**: Retention of 90 days or destroy when no longer needed, whichever comes first.

- **Non-Records**: Retention of three years or destroy when no longer needed, whichever comes first.

- **Official record**: Retain as per disposition schedules. Do not destroy early or prior to that period, nor keep longer than the specified retention period as indicated by the disposition schedule.

b. Additional Standards for Managing Electronic Mail (email) Records for Senior Officials

Senior Officials at USAID are individuals occupying executive positions who are responsible for oversight, management, and decision making. By virtue of their position these individuals will frequently have accountability to the Congress of the United States of America and the American Public.

Senior Officials are responsible for creating records to document their activities and for the proper management and preservation of their records. These responsibilities are applicable to all records made or received in the conduct of Agency business, regardless of physical format or media. While all Agency employees, regardless of labor category, must preserve records that meet the definition of a record under the Federal Records Act, Senior Officials' records are generally the most important documents created within the Agency and are some of the most valued documents. It is important to capture the email of Senior Officials. Emails are more likely to contain substantive information and are likely to require retention for several years, and in case of Senior Officials, permanently.

The USAID email accounts of Senior Officials must not be cleared, deleted, or wiped for any reason during the tenure of the Senior Official. Emails of Senior Officials will be retained and transferred to NARA for permanent preservation.

While Senior Officials may delete personal emails, they should be aware that the definition of a personal email is very narrow. The only emails that are personal are those that do not relate to or affect the transaction of Agency business.

In addition, non-record material may be deleted when no longer needed. Non-record material may include:

- Working files that consist of rough notes, drafts, or calculations that are not needed to support the decision trail, in other words papers that lose all value after the work is finalized;

- Extra copies of records kept only as convenience copies;

- Personal papers that are documents unrelated to or having no effect upon the conduct of Agency business;

- Library materials intended only for reference; and/or

- Presentations or papers of a professional nature not representing Agency opinion or policy.

As required by **44 U.S.C §2911 subsection (a) of the Federal Records Act Amendments of 2014**, Senior Officials may not create or send a record using a non-official electronic messaging account to conduct Agency business. However, in exceptional circumstances, the use of non-official EM systems may occur (see **502.3.4.6**).

The following positions reflect NARA guidance and satisfy the Presidential Directive on retaining email for Senior Officials for the purposes of records management:

- Administrator;
- Deputy Administrator/Chief Operating Officer;
- Associate Administrator;
- Assistant Administrators;
- Assistants to the Administrator;
- Mission Directors;
- Chief Human Capital Officer;
- Chief Financial Officer;
- Chief Information Officer;

- Senior Procurement Executive;
- Chief Real Property Officer;
- Director, U.S. Global Development Lab;
- Director, Office of Small and Disadvantaged Business Utilization;
- Director, Office of Budget and Resource Management;
- Director, Office of Security;
- Director, Office of Civil Rights and Diversity;
- Agency Counselor;
- Chief Economist;
- General Counsel;
- Inspector General;
- Chief Strategy Officer;
- Chief of Staff;
- Executive Secretary;

- All individuals formally designated as "Acting" in the above listed positions; and

- 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, the Administrator, Senior Agency Official for Managing Government Records, or Agency Records Officer may determine which individual positions would be considered “Designated Senior Official Positions” for the purposes of email preservation.

502.3.4.7 Additional Standard for Text Messages on Government Furnished Mobile Devices

Effective Date: 03/09/2016

USAID defines a text message as a mobile communication, which may also include multimedia content such as pictures, video, or audio (see **ADS 545.6** for additional information on types of text messages). These guidelines apply to any records created on any government furnished equipment (GFE) owned or provided by USAID (e.g. tablets, laptops, blackberries, iphones, or androids).

Text messaging, and the like, are typically captured via a third party service provider, and are not stored on the Agency network. Therefore, USAID does not encourage the use of text messaging to conduct official Agency business. However, if an official record is created, sent, or received via text to conduct Agency business, it is the responsibility of the USAID employee to ensure that any federal records of the Agency are appropriately captured within an official USAID recordkeeping system (see **502.3.4.6**). To accomplish this, the employee must forward the communication to an official electronic messaging account of the employee no later than **20 days** after the original creation or transmission of the record.

All messages sent or received on a government-furnished mobile device is the property of the Agency and not the employee.

All employees, regardless of labor category, must forward any text messages relating to Agency business to their official USAID account for permanent retention.

Attachment B

502.3.7 Exit Policy

Effective Date: 03/09/2016

As stated in **ADS 451, Separations and Exit Clearance**, USAID employees must follow these procedures when departing or transferring from USAID.

USAID employees must complete **AID Form 502-2, USAID Records Management Exit Checklist for Employees** or **ADS 502-3 for Senior Officials** before separating from USAID. The Records Liaison Officer (RLO) and supervisor must verify that records have been handled properly according to USAID's records management policies (see **502.3.2** for official records definition). This ensures that all records and non-public material created, received, or maintained during the exiting employee's tenure remains in the Agency's custody upon separation or transfer.

The exit policy procedures apply to all USAID employees, regardless of labor category, when the employee separates from the Agency due to:

- Resignation,
- Retirement, or
- Transfer to another government agency.

Employees transferring within the Agency must ensure that official records within their custody are accessible to office RLO or supervisor, if the RLO is not available.

Any records that USAID employees create or receive during their employment are the property of USAID. It is the responsibility of every USAID employee to protect records in their custody. Per the **Federal Records Act of 1950, as amended**, USAID employees are reminded that official records may not be removed from government custody, and may not be destroyed, unless they have met the requirements of a records disposition schedule.

Note: USAID employees designated as Senior Officials will follow supplemental exit policy requirements outlined in **502.3.7.1**.

(1) The Authorizing Official must:

a. Consider and identify records in their custody. Records may be stored in more than one location and in more than one format. The media types outlined below must be considered[1]. The supervisor must be made aware of any records stored in these locations and must receive a list, as well as storage locations, of the records.

Media types to consider:

- Paper
- Electronic Messages (e.g. email, chats, IM)
- CD-ROMs
- Collaboration tools

More specifically:

- Hard Drive or Personal Drive
- Shared Drive
- Email System
- Text Messaging, Chat/Instant Messaging
- Laptop or other Government Furnished Equipment (GFE)
- Web or Social Media Sites
- Huddle, Google Drive

b. Separate all official records from non-record materials (see **502.3.2.1** for a definition of non-record materials).

c. Either transfer electronic records located on any of the device locations identified above to an accessible recordkeeping system, supervisor, and/or successor, or make the records available to a supervisor and/or successor.

d. Provide a list of any record and its location undergoing any of the following: FOIA request, audit, litigation hold, or Congressional inquiry.

e. Dispose of and/or remove any non-record materials.

f. Remove or provide any passwords to a supervisor and/or successor.

g. Certify and inform supervisor of all records created or received and certify that non-public or official record content of the Agency is not removed without proper approval.

(2) The supervisor must:

a. Ensure that records needed for work-in-progress are reassigned to another employee.

[1] This list is not all inclusive but provides examples of what to consider.

b. Certify and verify the information completed on the Exit Checklist and certify that the employee is not removing any non-public or official record content of the Agency without proper approval.

c. Retain certified checklist per the records disposition schedule.

(3) The RLO must certify and verify the information completed on the Exit Checklist and that the employee is not removing any non-public or official record content of the Agency without proper approval. In the event the RLO is not available, an Authorizing Official may certify the checklist. The Authorizing Official may be the employee's supervisor, the Agency Records Officer, or designee.

(4) Exiting employees are prohibited from:

a. Removing any non-public or official records without proper approval.

b. Destroying or transferring records, except per records disposition schedule instructions. **Note:** Dispositioning authority is trumped when records are the subject of a FOIA request, audit, litigation, and/or Congressional inquiry. Exiting Senior Officials must identify all such records and provide a list of titles and locations on the checklist for their Authorizing Official.

502.3.7.1 Exit Policy for Senior Officials

Effective Date: 03/09/2016

Exiting Senior Officials will follow the guidance stated in **ADS 451, Separations and Exit Clearance** and section **502.3.7.1** when separating from USAID (see **502.3.4.6** for a list of Senior Officials).

Senior Officials must complete **AID Form 502-3, USAID Records Management Exit Checklist for Senior Officials**, before separating from USAID.

The exit policy procedures apply to all USAID Senior Officials separating from the Agency due to:

- Resignation,
- Retirement, or
- Transfer to another government agency.

The Authorizing Official and RLO must verify that the Senior Official's records have been handled properly according to USAID's records management policies to ensure that all records and non-public material created, received, or maintained during the exiting Senior Official's tenure remains in the Agency's custody upon separation (see **502.3.2** for the definition of official records). The Authorizing Official may be the Senior Official's supervisor, the Agency Records Officer, or designee.

Note: USAID employees NOT designated as Senior Officials will follow the exit policy requirements outlined in **502.3.7**.

(1) USAID Senior Officials must:

a. Consider and identify records in their custody. Records may be stored in more than one location and in more than one format. The media types outlined below must be considered[2]. Additional consideration should be given to drafts that have been created during the Senior Official's tenure. The final version of the draft should be deemed the official copy and preserved. The Authorizing Official must be made aware of any records stored in these locations and must receive a list, as well as storage locations, of the records.

Media types to consider:

- Paper
- Electronic (including email)
- CD
- Collaboration tools

More specially:

- Hard Drive or Personal Drive
- Shared Drive
- Email System
- Text Messaging, Chat/Instant Messaging
- Laptop or Government Furnished Equipment (GFE)
- Web or Social Media Sites
- Huddle, Google Drive

b. Separate all official records from non-record materials (see **502.3.2.1** for the definition of non-record materials).

[2] This list is not all inclusive but provides examples of what to consider.

c. Either transfer electronic records located on any of the device locations identified above to an accessible recordkeeping system, supervisor, and/or successor, or make the records available to a supervisor and/or successor.

d. Provide a list of any record and its location undergoing any of the following: FOIA request, audit, litigation hold, or Congressional inquiry.

e. Dispose of and/or remove any non-record materials.

f. Remove or provide any passwords to a supervisor and/or successor.

g. Certify and inform supervisor of all records created or received during Senior Official's tenure and certify that non-public or official record content of the Agency is not removed without proper approval.

(2) The Authorizing Official must:

a. Ensure that records needed for work-in-progress are reassigned.

b. Certify and verify the information completed on the Exit Checklist and certify that the Senior Official is not removing any non-public or official record content of the Agency without proper approval.

c. Retain certified checklist per the records disposition schedule.

(3) The RLO must certify and verify the information completed on the Exit Checklist and certify that the Senior Official is not removing any non-public or official record content of the Agency without proper approval.

(4) Exiting Senior Officials are prohibited from:

a. Removing any non-public or official records without proper approval.

b. Destroying or transferring records, except per records disposition schedule instructions. **Note:** Dispositioning authority is trumped when records are the subject of a FOIA request, audit, litigation, and/or Congressional inquiry. Exiting Senior Officials must identify all such records and provide a list of titles and locations on the checklist for their Authorizing Official.