U.S. Department of Labor

Office of Inspector General—Office of Audit

REPORT TO THE OFFICE OF THE ASSISTANT SECRETARY FOR ADMINISTRATION AND MANAGEMENT

DEPARTMENT OF LABOR NEEDS IMPROVEMENTS IN MANAGING ITS RECORDS MANAGEMENT PROGRAM FOR CAPTURING ELECTRONIC MESSAGES TO PRESERVE FEDERAL RECORDS

DATE ISSUED: SEPTEMBER 20, 2019
REPORT NUMBER: 17-19-001-07-001

U.S. Department of Labor
Office of Inspector General
Audit

BRIEFLY...

DEPARTMENT OF LABOR NEEDS IMPROVEMENTS IN MANAGING ITS RECORDS MANAGEMENT PROGRAM FOR CAPTURING ELECTRONIC MESSAGES TO PRESERVE FEDERAL RECORDS

September 20, 2019

WHY THE AUDIT WAS CONDUCTED

Federal electronic records pose a challenge to recordkeeping in the Federal Government. To maintain the public's trust and to ensure transparency in the preservation of Federal records, regarding electronic messaging, the Department of Labor (DOL) needs to stay vigilant and close the gap between outdated policies and evolving technologies. Furthermore, all DOL employees must be aware of their responsibility to capture Federal electronic records created or received in personal accounts to ensure the proper preservation of Federal records.

WHAT WAS DONE

Given our concerns, the Office of Inspector General (OIG) contracted with RMA Associates to conduct this audit to answer the following question:

> Does DOL have sufficient controls in place to preserve electronic messages as Federal records of official activities?

To answer this question, RMA reviewed policies and procedures concerning electronic messages and documents, interviewed relevant personnel with knowledge of policies, and interviewed employees for awareness and compliance with policies. The review covered the period September 2017 to June 2019.

READ THE FULL REPORT:

http://www.oig.dol.gov/public/reports/oa/2019/17-19-001-07-001

WHAT WAS FOUND

DOL lacked procedures for identifying, managing, and preserving electronic messages as Federal records. Although not all electronic messages are Federal records, electronic messaging used for official business are Federal records that must be captured and preserved.

DOL did not provide guidance for employees to identify, manage, and maintain electronic messages, such as Twitter Direct Message, Slack, Snapchat, WhatsApp, Pigeon, Yammer, Jive, or other internal collaboration networks, as Federal records. DOL relied on employees to self-report when they conducted official business requiring preservation.

Electronic messages on government-owned devices were deleted and not preserved when the device owner's job responsibilities changed or when the device owner left DOL.

DOL employees surveyed were not aware of Departmental guidance regarding (1) the use of personal electronic messaging accounts to conduct official business, and (2) the authorized use of mobile applications and monitoring of mobile application downloads that encrypt and automatically delete messages.

Actions to address 3 of the 5 recommendations from NARA's assessment of DOL's record management program are in process, but not complete. DOL did not establish formal procedures to provide effective oversight of the Capstone Approach.

DOL established a plan to transfer Federal records in electronic format to the National Archives and Records Administration (NARA) by December 31, 2019.

WHAT WAS RECOMMENDED

RMA Associates made 10 recommendations to the Assistant Secretary for Administration and Management to improve the DOL's electronic records management program.

In response to the draft report, the Assistant Secretary for Administration and Management concurred with 9 of the 10 recommendations to improve DOL's electronic records management program.

TABLE OF CONTENTS

U.S. Department of Labor

Office of Inspector General
Washington, D.C. 20210

INSPECTOR GENERAL'S REPORT

Bryan Slater
Assistant Secretary
for Administration and Management
U.S. Department of Labor
200 Constitution Ave, NW
Washington, DC 20210

The United States Department of Labor (DOL) Office of Inspector General (OIG) contracted with the independent certified public accounting firm of RMA Associates to conduct a performance audit of DOL's records management program.

The objective of RMA's performance audit was to determine if DOL had sufficient controls in place to preserve Federal records on official activities. Per the attached report, RMA concluded DOL needs to improve its controls to better preserve Federal records, or potential Federal records, of electronic messages.

Although not all electronic messages created or received by employees constitute a Federal record, it is possible for DOL employees to use electronic messaging for official business without preserving any of those messages as a Federal record. DOL relied on employees' self-reporting to preserve Federal records of electronic messaging used to conduct official business, but did not monitor, nor have the tools necessary to monitor, electronic messages.

Elliot P. Lewis
Assistant Inspector General for Audit

RMA Associates
Auditors. Consultants. Advisors.

PERFORMANCE AUDIT REPORT

Bryan Slater
Assistant Secretary
for Administration and Management
U.S. Department of Labor
200 Constitution Ave, NW
Washington, DC 20210

This report presents the results of our audit of the Department of Labor's (DOL) management preservation of electronic messages and transferring of permanent electronic records to the National Archives and Records Administration (NARA).

Electronic records pose a challenge to recordkeeping in the Federal Government. To maintain the public's trust and ensure transparency in Government, DOL must identify, manage, and preserve Federal electronic records that are proliferating in formats, expanding in quantity, and vulnerable to quick deletion. As technological advances facilitate the evolution of electronic messaging, it is important for Federal Agencies to keep pace with the evolving technology and redefine what constitutes as a Federal Record. As new, sophisticated mobile applications that enable encryption and automatic deletion of messages become more prevalent, Federal Agencies are tasked with the difficult responsibility of ensuring all forms of communication, including electronic messaging, are maintained and preserved as Federal Records.

In March 2017, NARA issued a memorandum to all Federal Agency Senior Agency Officials for Records Management stating:

> Agencies are responsible for properly managing electronic messages that are Federal records, whether they are SMS texts, encrypted communications, direct messages on social media platforms, e-mail, or created on any other type of electronic messaging system or account.

NARA performed an assessment of the DOL's Records Management Program, which was issued on September 15, 2017. Their assessment focused on e-mail records management. Our intention was not to duplicate NARA's effort; hence, the scope of our audit was focused on electronic messages.

In 2017, the OIG received a request from a Senator and Congresswoman to perform a review of DOL's electronic records management program. Based on the Federal guidelines issued by NARA and the request from public officials, we conducted an audit to answer the following question:

> Does DOL have sufficient controls in place to preserve Federal records on official activities?

As part of our audit, we reviewed policies, procedures, and documents concerning electronic messages; interviewed relevant personnel with the knowledge of DOL policies; requested written representation from DOL officials regarding their understanding and use of electronic Federal records; and interviewed selected personnel from several DOL agencies to verify awareness and compliance with DOL policies.

Based on the results of our audit work, we determined DOL needs to improve controls in place to better preserve Federal records (or potential Federal records) of electronic messages, other than e-mails. Although not all electronic messages created or received by employees constitute a Federal record, it is possible for DOL employees to use electronic messaging for official business without preserving any of those messages as a Federal record. DOL relied on employees' self-reporting to preserve Federal records of electronic messaging used to conduct official business. DOL did not monitor or have the tools necessary to monitor electronic messages.

Additionally, we found DOL did not provide sufficient guidance to its personnel regarding the preservation of electronic messages.

This audit did not constitute an audit of financial statements or an attestation level report as defined under *Government Audit Standards* or AICPA professional Standards.

This report is intended solely for the use of the U.S. Department of Labor Secretary and Inspector General, Comptroller General, OMB, and relevant congressional committees; and is not intended to be and should not be relied upon by anyone other than these specified parties.

RMA Associates
September 18, 2019

RESULTS

While DOL has a records management program, it can strengthen its controls over electronic messages to fully comply with Federal requirements.[1] We noted a lack of documented procedures for identifying, managing, and preserving electronic messages as Federal records. DOL's current practices are not suitably robust to capture all potential text message records needed to support DOL's business decisions.

DOL has limited technical ability to monitor, capture, or retain electronic messages created on government-issued devices. DOL has no ability to monitor, capture, or retain electronic records created on personally-owned devices.

We attributed the lack of oversight of electronic messages to the decentralized nature of the use of electronic messages, DOL's incomplete policies, dependence on self-reporting, and a lack of tools to capture electronic messages.

DOL's ineffective management of electronic messages resulted in an increased risk that:

- Sufficient documentation of governmental decisions was not maintained;
- Records needed in the daily performance of its mission were not efficiently located and retrieved; and
- Records of historical significance were not identified, preserved, and made available to the public.

We reviewed DOL's progress toward preparing for the transfer of all permanent electronic records to NARA in the electronic format by December 31, 2019. We also reviewed DOL's progress in completing the corrective actions from NARA's assessment of DOL's records management program. We found no issue to report that would affect the successful completion of these two tasks.

[1] During the course of the audit, DOL began implementation of corrective action and strengthening of controls. However, as the audit is conducted over a period of time, our results are not modified as a result of the changes made by DOL subsequent to the audit period.

POLICIES AND PROCEDURES DID NOT SUFFICIENTLY DESCRIBE THE REQUIREMENTS FOR RETAINING ELECTRONIC MESSAGING AS FEDERAL RECORDS

We interviewed personnel from the Office of Records, the Office of the Chief Information Officer (OCIO), and the Office of Public Affairs (OPA), and inspected relevant training material[2] and policies[3] to determine if the controls were in place for retaining electronic messaging as Federal records. We noted these materials contained guidance concerning the preservation of e-mails and non-electronic documents as Federal records. We also noted the April 2018 Records Management Training Program defined a Federal record as:

> According to the National Archives and Records Administration (NARA), a record includes all e-mails, electronic databases, books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government 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 Government or because of the informational value of data in them.

We found DOL's Records Management Training Program did not define or provide guidance describing electronic messages, such as text messages, Twitter Direct Message, Slack, Snapchat, WhatsApp, Pigeon, Yammer, Jive, or other internal collaboration networks.

We noted NARA's definition of electronic messages was broader than DOL's definition. Based on 44 U.S. Code 2911 – *Disclosure requirement for official business conducted using non-official electronic messaging accounts*, electronic messages are defined as "electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals."

[2] 2018 EOD Records Management Program Training

[3] DLMS 1-400, DLMS 2-700, and DLMS 5-600, policies for records management, telecommunications, and social media, respectively.

Furthermore, we noted NARA issued Bulletin 2015-02: *Guidance on Managing Electronic Messages* on July 29, 2015, defined types and examples of text messages as:

Types Of Electronic Messaging	Examples
Chat/instant messaging	Google Chat, Skype for Business, IBM Sametime, Novell Groupwise Messenger, Facebook Messaging
Text messaging, also known as Multimedia Messaging Service and Short Message Service	iMessage, Short Message Service, and Multimedia Messaging Service on devices, such as Blackberry, Windows, Apple or Android devices
Voicemail messaging – systems that can have voicemail sent to e-mail as an attachment; messages that can be sent or received from land-line or mobile phones	Google Voice, voice-to-text conversion
Other messaging platforms or apps, such as social media or mobile device applications. These include text, media and voice messages	Twitter Direct Message, Slack, Snapchat, WhatsApp, Pigeon, Yammer, Jive, or other internal collaboration networks

Without policies, procedures, and training guiding personnel to identify, manage, and preserve Federal electronic messages that are created on messaging platforms or apps, such as social media or mobile devices, DOL increased the risk that:

- Sufficient documentation of governmental decisions was not maintained;
- Records needed in the daily performance of its mission were not efficiently located and retrieved; and
- Records of historical significance were not identified, preserved, and made available to the public.

TECHNICAL CONTROLS WERE NOT CONFIGURED TO MANAGE TEXT MESSAGES AS POSSIBLE FEDERAL RECORDS

Mobile Device Management (MDM) system[4] cannot be configured to capture text messages.

DOL manages its government-issued cellular devices using an MDM system. We found the MDM cannot be configured to capture and retain mobile text messages routinely. However, we were informed that for investigational purposes, DOL captured mobile text messages on a case-by-case basis through coordination with the network provider. We also noted DOL relied on the manual control of employees' self-reporting of electronic messaging for official business for preserving Federal records. Additionally, DOL did not have technical controls in place to monitor or support the preservation of Federal records.

Furthermore, DOL did not classify mobile text messages as defined by NARA Bulletin 2015-02: *Guidance on Managing Electronic Messages.* Bulletin 2015-02 defined text messages, Multimedia Messaging Service (MMS) and Short Message Service (SMS) as types of electronic messaging with the following examples: iMessage, SMS, and MMS on devices, such as Blackberry, Windows, Apple, or Android devices. Consequently, DOL did not inquire whether MMS and SMS messages should be preserved as Federal records.

Skype For Business (Skype)[5] messages were not configured to capture conversations.

The standard instant messaging application provided on DOL devices is Skype for Business. This application allows for recording Skype sessions or conversations. However, DOL did not use the recording feature available in Skype. DOL relied on the manual control of employees' self-reporting Skype sessions used for official business to preserve as Federal records.

[4] Mobile Device Management (MDM) system is management software for the administration in controlling mobile devices, such as smartphones, tablet computers, laptops, and desktop computers within an organization.

[5] Skype for Business is a Microsoft Office communications and collaboration platform that offers features such as instant messaging, voice calls, video calls, online meetings, and screen sharing in one application.

In addition, DOL did not consider Skype for Business messaging as possible Federal records. However, NARA Bulletin 2015-02: *Guidance on Managing Electronic Messages*, states the following related to electronic messages:

"At this time, current business practices make it more likely other types of electronic messages, such as chat and text messages, contain transitory information or information of value for a much shorter period of time. Regardless, agencies must capture and manage these records in compliance with Federal records management laws, regulations, and policies. As use of the electronic messaging systems changes over time, agencies will need to review and update these policies and procedures."

NARA Bulletin 2015-02 specifically notes that Skype for Business is an example of an electronic message that may be a Federal record (in addition to other chat/ instant messaging platforms such as Google Chat, Novell Groupwise Messenger, and Facebook Messaging).

Deletion of electronic messages other than e-mail on government devices is not controlled.

Government-issued device owners' electronic messages, other than e-mail, were deleted when the device owner's job responsibilities changed or when the device owner left DOL. DOL relied on the manual control of employees' self-reporting of electronic messaging for official business to preserve as Federal records. Additionally, DOL did not implement any technical controls to monitor or support the preservation of Federal records. As a result, potential government records may have been lost.

As noted earlier, NARA defined electronic messages more broadly than DOL. Without a proper configuration of an MDM system, cellular devices failed to capture and monitor deletions of electronic messages, including messages in social media apps. DOL increased the risk that:

- Sufficient documentation of governmental decisions was not maintained;
- Records needed in the daily performance of its mission were not efficiently located and retrieved; and
- Records of historical significance were not identified, preserved, and made available to the public.

CONTROLS FOR ELECTRONIC MESSAGING FOR PERSONAL E-MAIL ACCOUNTS CAN BE IMPROVED

We interviewed individuals from the Office of Records, OCIO, and OPA, and inspected relevant training material[6] and policies[7] to determine the guidance issued. We asked pertinent questions to a selection of Senior Agency Officials concerning their use of personal devices and government-issued devices[8]. The Senior Agency Officials did not identify any instances in which personal e-mail accounts or other electronic communication outside of DOL e-mail system were used to create a Federal record.

We found DOL implemented minimal controls to ensure employees followed the policies preserving the Federal record related to personal e-mail accounts or creating/sending records using non-official e-mail or other electronic messaging accounts. Employees were required to self-report the use of electronic messaging for official business. Employees were notified of this requirement through the Records Management Program Training.

We noted 44 U.S. Code 2911 – *Disclosure requirement for official business conducted using non-official electronic messaging accounts*, electronic messages are defined as "electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals."

Personal accounts should only be used in exceptional circumstances. DOL must be proactive in providing consistent training on a recurring basis to ensure all employees are aware of their responsibility to capture electronic messages created or received in personal accounts to meet the requirements in the amended *Federal Records Act*.

[6] 2018 EOD Records Management Program Training

[7] DLMS 1-400, DLMS 2-700, and DLMS 5-600, policies for records management, telecommunications, and social media, respectively

[8] A selection of Senior Agency Officials were each asked a series of questions related to personal cellular phone use and government-issued cellular phone use. Questions included usage of text messages on personal and government-issued devices for official government business, use of electronic messaging applications (including social media) for official government business, and the awareness of records management requirements for electronic messages outside of Department e-mails.

The *Federal Records Act* (44 U.S.C. 2911 as amended by Pub. L. 113-187) states:

> (a) IN GENERAL.—An officer or employee of an executive agency may not create or send a record using a non-official electronic messaging account unless such officer or employee—
>
> (1) copies an official electronic messaging account of the officer or 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 officer or employee no later than 20 days after the original creation or transmission of the record.

Electronic messages created or received in a personal account meeting the definition of a Federal record must be forwarded to an official electronic messaging account within 20 days. The statutory definition of electronic messages includes e-mail.

Monitoring compliance with records management requirements for personal e-mails is a very difficult task. To ensure the requirements are met, DOL must make every reasonable effort to provide training and ensure awareness of each employee to decrease this risk. During the audit period, there was an increased risk that:

- Sufficient documentation of governmental decisions was not maintained;
- Records needed in the daily performance of its mission were not efficiently located and retrieved; and
- Records of historical significance were not identified, preserved, and made available to the public.

IMPLEMENTING POLICIES AND MONITORING FOR MOBILE DEVICES[9]

We inspected DOL's policies and procedures [Department of Labor Manual Series (DLMS) 1-400, DLMS 2-700, and DLMS 5-600, policies for records management, telecommunications, and social media, respectively] and noted they did not contain specific guidance concerning government-issued devices for

[9] Mobile devices are portable computing devices such as a smartphone or tablet computer.

the use of mobile applications, or for the active monitoring of downloaded mobile applications that encrypt and delete messages automatically.

We noted 44 U.S. Code 2911 – *Disclosure requirement for official business conducted using non-official electronic messaging accounts*, electronic messages are defined as "electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals." Other messaging platforms or apps, such as social media or mobile device applications, are included as types of electronic messaging with the following examples: Twitter Direct Message, Slack, Snapchat, WhatsApp, Pigeon, Yammer, Jive, or other internal collaboration networks.

We conducted a survey of nineteen DOL employees, in which we asked several questions related to DOL's records management policy and practices to determine whether employees were aware of:

- The policies and procedures to determine which text messages to preserve and steps to ensure employees are knowledgeable of this guidance;
- The use of text messages (on government-issued or personal devices) for official business; and
- The deleted, destroyed, lost, or misplaced text messages needed for records management; and, if applicable, the rationale for destroying text communication records.

The majority of surveyed DOL employees generally understood the need to preserve official business as a Federal record. However, they were not aware of specific guidance issued by DOL for personal e-mail accounts, authorized mobile applications, and guidance for actively monitoring downloads of mobile applications that encrypt and automatically delete messages.

Most of the interviewed employees stated they did not use the electronic message accounts or devices for official business and indicated they did not delete, destroy, lose, or misplace text messages needed for records management.

We noted 44 U.S. Code 2911 – *Disclosure requirement for official business conducted using non-official electronic messaging accounts*, electronic messages are defined as "electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals."

We noted NARA Bulletin 2015-02: Guidance on Managing Electronic Messages stated: "Employees create Federal records when they conduct agency business

using personal electronic messaging accounts or devices." This is the case whether or not agencies allow employees to use personal accounts or devices to conduct agency business. This is true for all Federal employees regardless of status. This is also true for contractors, volunteers, and external experts.

Personal accounts should only be used in exceptional circumstances. DOL should provide clear instructions to all employees on their responsibility to capture electronic messages created or received in personal accounts to meet the requirements in the amended *Federal Records Act*.

The *Federal Records Act* (44 U.S.C. 2911 as amended by Pub. L. 113-187) states:

> (a) IN GENERAL.—An officer or employee of an executive agency may not create or send a record using a non-official electronic messaging account unless such officer or employee—
>
> (1) copies an official electronic messaging account of the officer or 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 officer or employee no later than 20 days after the original creation or transmission of the record.

Electronic messages created or received in personal accounts meeting the definition of a Federal record must be forwarded to an official electronic messaging account within 20 days. The statutory definition of electronic messages includes e-mail.

Due to the lack of guidance, DOL personnel may not be fully aware of the records management requirements for electronic messaging related to mobile applications. Additionally, DOL may not be aware of personnel using applications that encrypt and automatically delete messages. Federal records could be created and immediately removed in such applications. As a result, there was an increased risk that:

- Sufficient documentation of governmental decisions was not maintained;
- Records needed in the daily performance of its mission were not efficiently located and retrieved; and
- Records of historical significance were not identified, preserved, and made available to the public.

RECOMMENDATIONS FROM THE FY17 NARA AUDIT REMAIN OPEN

We inspected the Plan of Corrective Action[10] Status Report of January 31, 2019, which was developed in response to the NARA Audit Report. The report showed DOL closed 2 of the 5 recommendations. The 3 open recommendations missed its completion dates. For 2 of the open recommendations, DOL was waiting for policies approvals and for the remaining open recommendation, DOL must fully implement the plan for all permanent electronic records to be in an electronic format. DOL has not established new due dates for the remaining open recommendations.

Recommendation	Status	Explanation of Open Items
Recommendation 1: The Senior Agency Official Records Management (SAORM) and the Departmental Records Officer (DRO), in coordination with DOL agencies and offices, must update and formally issue the SRMP as well as institute, by policy or procedure, a periodic review of the SRMP. (44 United States Code 3506 and Office of Management and Budget (OMB) Circular A-130)	Open: Late (Due Date: Q4 FY 2018)	The SRMP (Strategic Records Management Plan) has not been approved.
Recommendation 2: The DRO and Agency Records Officers (ARO) must establish and implement a formal records management evaluation program to ensure all records are managed in accordance with 36 Code of Federal Regulation (CFR) Chapter XII, Subchapter B. (36 CFR 1220.34(j))	Closed	
Recommendation 3.1: The DRO must update Department-level training to ensure its adequacy and that it meets the requirements of 36 CFR 1224.10(e).	Closed	
Recommendation 3.2: Office of the Assistant Secretary for Administration and Management (OASAM) and the DOL DRO must update Department policy and provide the necessary guidance to support the development of customized RM training that reflects the unique records management practices and policies of DOL agencies and offices. (36 CFR 1224.10(e) and NARA Bulletin 2017-01)	Closed	
Recommendation 4: OASAM and Office of the Solicitor should coordinate to update and implement Department-wide policies and procedures for legal holds. (36 CFR 1226.18)	Open: Late (Due Date: Q4 FY 2018)	Policy is written and in the process of review.
Recommendation 5: DOL must develop and implement a plan that will guide its agencies in meeting target 1.1 of M-12-18.	Open: Late (Due Date: Q3 FY 2018)	The plan has not been fully implemented.

[10] Plan of Corrective Action (POCA), January 31, 2019

As such, not closing the remaining open recommendations within the established milestone dates or establishing due dates for the remaining open recommendations, continues to make the DOL records management program vulnerable.

DOL DID NOT ESTABLISH FORMAL PROCEDURES TO PROVIDE EFFECTIVE OVERSIGHT OF THE CAPSTONE APPROACH

On March 25, 2016, the Deputy Secretary issued a memorandum announcing DOL's intention to adopt NARA's Capstone Approach to e-mail records management. The Capstone Approach permits agencies to manage e-mail records in a more simplified and automated way that allows for the categorization and scheduling of e-mail based on the work and/or position of the e-mail account owner, rather than on the content of each e-mail. This allows e-mail disposition to be carried out in a systematic way, where e-mail within accounts designated as permanent are transferred to the legal custody of the National Archives, and e-mail within accounts designated as temporary are eligible for eventual destruction.

The memorandum directed DOL agencies to propose their list of Capstone Officials, or those individuals whose e-mail will be considered permanent. Capstone Officials include senior agency officials, including the Secretary of Labor; Deputy Secretary; Assistant Secretaries; Deputy Assistant Secretaries; Principal management positions (e.g. Chief Information Officer); Directors of significant program offices; Principal regional officials; and roles or positions that routinely provide advice and oversight to the agency (e.g. General Counsel, Chief of Staff, Special Assistants). Based on the Capstone approach, the Department developed a Capstone List of employees whose e-mails would be kept permanently.

We inspected Department policies and procedures to determine whether they included any guidance concerning the Capstone Approach. We did not identify any policies or procedures that provided guidance.

We inspected documentation from the Department’s quarterly meeting with all Agency Records Officers (AROs) and Administrative Officers (AOs) and noted that training was provided in the meetings, in addition to initial onboard training. The meetings provided detailed information of the Capstone Approach and included time for open questions and answers.

We inspected documentation that evidenced a quarterly review process of the listing of all Capstone Officials has been established. The process has not been formalized into a Standard Operating Procedure (SOP) or other formal guidance. However, controls take time to mature and show evidence of effectiveness.

NARA Bulletin 2014-06, issued September 15, 2014 states:

> When adopting the Capstone approach, agencies must identify those e-mail accounts most likely to contain records that should be preserved as permanent. Agencies will determine Capstone accounts based on their business needs. They should identify the accounts of individuals who, by virtue of their work, office, or position, are likely to create or receive permanently valuable Federal records. Capstone officials will generally be the top-level senior officials of an agency, but may also be other key decision makers at lower levels of the agency.
>
> Following this approach, an agency can schedule all of the e-mail in Capstone accounts as permanent records. The agency could then schedule the remaining (non-Capstone) e-mail as temporary and retain all of them for a set period of time based on the agency's needs.

The lack of procedures over the development and oversight of the Department's Capstone list may circumvent Federal requirements to ensure permanent retention of e-mails that are considered valuable Federal records and should be permanently retained.

DOL HAS ESTABLISHED A PLAN TO TRANSFER PERMANENT ELECTRONIC RECORDS TO NARA IN THE ELECTRONIC FORMAT BY DECEMBER 31, 2019

Memorandum M-12-18, *Managing Government Records Directive,* issued August 24, 2012, requires the following of federal agencies:

> By December 31, 2019, all permanent electronic records in Federal agencies will be managed electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format.

In order to meet this requirement of M-12-18, DOL developed an implementation plan with internal deadlines to ensure successful completion. DOL has been successful in meeting internal goals and deadlines to date, and most recently held a meeting with NARA officials (April 2, 2019) to present the Department's implementation plan. DOL's implementation plan details the steps necessary to meet the requirement of M-12-18, and we did not identify any aspects which would indicate that the deadline of December 31, 2019, will not be met.

DOL OFFICIALS REPRESENT UNDERSTANDING AND USE OF ELECTRONIC FEDERAL RECORDS

We issued a series of three representation statements to 197 DOL officials on the Department's Capstone Official List as of February 26, 2019 deemed likely to create Federal records. We requested that each official provide a response to the following three statements regarding their understanding of and use of electronic Federal records.

1. I am _____ aware or _____ not aware of my responsibility for maintaining electronic Federal records in accordance with The Federal Records Act. This includes electronic messages that should be retained as Federal records for my agency whether created on my private devices or government-issued devices, both non-encrypted and encrypted.

2. I am _____ aware or _____ not aware of any uncorrected instances of personal or Agency noncompliance with The Federal Records Act as it relates to electronic records that should be retained as Federal records for my agency.

3. I am _____ aware or _____ not aware of instances in which applications were used for disappearing messages to transmit agency business information that should be retained as a Federal record for my agency.

We noted no concerns or issues based on the responses provided by each official.

RECOMMENDATIONS

We recommend the Assistant Secretary of Administration and Policy take the following actions:

1. Revise policies and procedures to provide explicit guidance concerning text messages, Twitter Direct Message, Slack, Snapchat, WhatsApp, Pigeon, Yammer, Jive, and other internal collaboration networks.

2. Revise policies and procedures to provide more emphasis on electronic messaging in the Records Management Training Program.

3. Research a technical solution, to the extent possible, to allow personnel to capture and retain text messages on government-issued devices, or, if the resource requirement for this would be too significant, consider the signature of an affidavit by Senior Agency Officials on an annual basis to certify any Federal records from text messages have been retained.

4. Emphasize in training and policies that if Skype for Business is used to create a Federal record, it should be captured by the creator and retained as a Federal record.

5. On an annual basis, request a certification from employees that they have not utilized their personal e-mail to conduct Government business. In the event that employees have utilized their personal e-mail, request a certification that they have forwarded any e-mails to their Government e-mail account.

6. Make every reasonable effort to provide training and ensure awareness of each employee to avoid use of personal e-mail.

7. Add to its rules of behavior or similar document an explanation of the employees' responsibility in preserving Federal records and require employees to sign the document indicating they have preserved all electronic messages that are potentially Federal records in accordance with DOL and NARA requirements.

8. Revise policies and procedures to provide explicit guidance addressing the use of mobile applications.

9. To improve awareness of guidance:

    a. Revise policies, procedures, and training to emphasize the requirements of maintaining Federal records;
    b. Monitor compliance with the requirements; and
    c. Require each employee to annually sign a statement certifying he or she has surrendered all documentation related to the official business of the Government and require a review of documents proposed for removal by the employee.

10. Develop official procedures to provide concrete guidance on the Capstone Approach. The procedures should include guidance on official review of the listing of Capstone Officials on a recurring basis.

SUMMARY OF OASAM'S RESPONSE

The Assistant Secretary of Administration and Management agreed with 9 of the 10 recommendations in the draft report.

Management disagreed with the recommendation to request an annual certification from employees that they have not utilized their personal e-mail to conduct Government business or in the event that employees have utilized their personal e-mail, that they have forwarded any e-mails to their Government e-mail account. The Assistant Secretary of Administration and Management stated certification is not required by law or regulation. However, OASAM stated it has updated the 2019 Records Management Training for all employees to include detailed guidance and explicit language from the Federal Records Act on personal email, which also includes a Records Management Rules of Behavior acknowledgement form. Similarly, the New Employee Orientation provides guidance on personal email.

RMA Response:

While RMA acknowledges although not specifically required by law, in the absence of other controls, the annual certification would provide DOL reasonable assurance that employees have properly preserved Federal records. We will evaluate OASAM's proposed Records Management Rules of Behavior acknowledgement form included in the 2019 Records Management Training for all employees to determine if it meets the intent of the recommendation.

Management's response to the draft report is included in its entirely in Appendix B.

We appreciate the cooperation and courtesies OASAM extended us during this audit.

RMA Associates
September 18, 2019

APPENDIX A: SCOPE, METHODOLOGY, & AUDIT OBJECTIVES

SCOPE

The scope of RMA Associates, LLC (RMA)'s audit focused on the preservation of DOL's electronic messages and transferring of permanent electronic records to the National Archives and Records Administration (NARA). It included DOL's most recent records management program policies, procedures, and practices. To avoid duplication of NARA's effort on its most recent NARA Records Management Inspection Report on e-mail records management, our scope focused on electronic messages. RMA's audit procedures covered the period of September 2017 through June 2019.

METHODOLOGY

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To accomplish our objective, we inquired of individuals from the Office of Records, the Office of the Chief Information Officer (OCIO), the Office of Public Affairs (OPA), and a selection of Senior Agency Officials; inspected relevant training material, policies, and procedures; surveyed a selection of DOL employees; and issued representative statements to DOL Capstone Officials.

RMA's procedures did not include:

- Inspection of personal e-mail accounts;
- Inspection of personal mobile devices;
- Inspection of data on government furnished equipment (GFE), such as text messages or application downloads;
- Inquiry or inspection concerning whether any DOL official has directed or advised any agency employee to delay or withhold a response to a Congressional request for information;
- Inquiry or inspection concerning whether any DOL official has directed or advised any agency employee or Congressional staff

member the agency will only provide requested documents or information to a Committee chair;
- Inquiry or inspection concerning previous OIG-provided recommendations to DOL regarding its management of the preservation of electronic records and compliance with Congressional document requests;
- Inquiry of the Secretary of Labor concerning the use of personal e-mail accounts to conduct government business; or
- Inquiry or inspection concerning whether all e-mails related to government activities or public policy are being reviewed in response to Freedom of Information Act requests.

In planning and performing our audit, we considered internal controls relevant to our audit objective. We obtained an understanding of those controls and assessed control risk as necessary to achieve our objective. The objective of our audit was not to provide assurance of the internal controls. Therefore, we did not express an opinion on DOL's records management program's internal controls. Our consideration of internal controls would not necessarily disclose all matters that might be significant deficiencies. Because of the inherent limitations on internal controls, or misstatements, noncompliance may occur and not be detected.

CRITERIA

- DLMS 1 Chapter 400 – Records Management
- DLMS 2 Chapter 700 – Telecommunications
- DLMS 5 Chapter 600 – Social Media
- OMB M-12-18 Memorandum for the Heads of Executive Departments and Agencies and Independent Agencies: Managing Government Records Directives
- 44 U.S. Code 2911 – *Disclosure requirement for official business conducted using non-official electronic messaging accounts*
- NARA Bulletin 2015-02: *Guidance on Managing Electronic Messages*
- *Federal Records Act* (44 U.S.C. 2911 as amended by Pub. L. 113-187)

AUDIT OBJECTIVES

The objective of the audit was to determine whether DOL has sufficient controls in place to preserve Federal records on official activities. The overall objective was accomplished through the following sub-objectives:

- **Objective 1:** Determine the controls DOL has in place to know it has all the records it should have, including, but not limited to, SMS texts, unauthorized encrypted communications, and direct messages on social media platforms.
- **Objective 2:** Determine whether DOL issued guidance for personal e-mail accounts and authorized mobile applications and actively monitored downloads of mobile applications that encrypt and automatically delete messages.
- **Objective 3:** Determine the extent to which Senior Agency Officials and staff used text messages on their government-issued mobile devices for official business.
- **Objective 4:** Determine whether DOL provided effective records management training and outreach.
- **Objective 5:** Determine whether DOL was on track to manage all permanent electronic records to the fullest extent possible for eventual transfer and access by NARA in the electronic format by December 31, 2019.
- **Objective 6:** Determine the extent to which DOL acted on the recommendations from the latest NARA audit.
- **Objective 7:** Determine whether DOL provided effective oversight of its approach for Capstone Officials.

APPENDIX B: OASAM RESPONSE TO THE REPORT

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

SEP 13 2019

Mr. Elliot P. Lewis
Assistant Inspector General for Audit
U.S. Department of Labor
200 Constitution Ave. NW
Washington, DC 20210

Dear Mr. Lewis:

Thank you for the opportunity to review and comment on draft report 17-19-001-07-001, *Department of Labor Needs Improvements in Managing its Records Management Program to Capture Electronic Messages for Preserving Federal Records*. We appreciate the Office of Inspector General's efforts and insights. The draft report contains ten recommendations, all of which we believe have either been resolved or are in the process of being resolved. Outlined below is a detailed response to each recommendation.

1. Revise policies and procedures to provide explicit guidance concerning text messages, Twitter Direct Message, Slack, Snapchat, WhatsApp, Pigeon, Yammer, Jive, and other internal collaboration networks.

   Management Response: Management concurs with this recommendation. The Office of the Assistant Secretary for Administration and Management (OASAM) has drafted a policy memorandum on electronic messaging, which is currently in departmental clearance. Once the memorandum is issued, OASAM will update the Department of Labor Manual Series (DLMS) with the new policy on electronic messages.

   Additionally, OASAM updated the 2019 Records Management Training for all employees to include detailed guidance and explicit language from the Federal Records Act on managing electronic messages. Similarly, both the New Employee Orientation and Entrance Briefing for Senior Officials and Political Appointees provide guidance on managing electronic messages.

2. Revise policies and procedures to provide more emphasis on electronic messaging in the Records Management Training Program.

   Management Response: Management concurs with this recommendation. In an effort to ensure that all employees are aware of their records management responsibilities specifically concerning electronic messages, OASAM has updated the 2019 Records Management Training for all employees to include detailed guidance and explicit language from the Federal Records Act on managing electronic messages. Likewise, both the New Employee Orientation and Entrance Briefing for Senior Officials and Political Appointees provide guidance on managing electronic messages.

3. Research a technical solution, to the extent possible, to allow personnel to capture and retain text messages on government-issued devices, or, if the resource requirement for this would be too significant, consider the signature of an affidavit by Senior Agency Officials on an annual basis to certify any Federal records from text messages have been retained.

   Management Response: Management concurs with this recommendation. The Office of the Chief Information Officer (OCIO) is currently blocking a feature, which would allow users to forward text messages to their official government email address via iron ports for security reasons. Removing this security feature would create a large vulnerability. Further, text messages cannot be captured using third-party applications due to budgetary constraints.

   A draft policy memorandum on electronic messaging is currently in departmental clearance. This memorandum will explicitly discourage the use of text messaging to create Federal records. Once the memorandum is issued, OASAM will update the DLMS with the new policy on electronic messages.

   Currently, OASAM requires users with Government Furnished Equipment (GFE) devices to sign a Mobile Device Management (MDM) Rules of Behavior acknowledgement form. Additionally, OASAM has updated the 2019 Records Management Training for all employees to include a Records Management Rules of Behavior acknowledgement form.

4. Emphasize in training and policies that if Skype for Business is used to create a Federal record, it should be captured by the creator and retained as a Federal record.

   Management Response: Management concurs with this recommendation. The Bargaining Unit agreement does not allow for the capture of Skype for Business instant messages, which is why the feature is disabled. Users are prohibited from creating Federal records using instant messages, which is expressly stated in the Federal Records Act Amendments of 2014 (PL 113-187). The Act "prohibits Federal officers and employees from creating or sending a record using non-official email or other electronic messaging accounts unless they simultaneously copy an official Government email or other electronic messaging account, or, within 20 days forward a complete copy of the record to such an official account. Penalties may apply for not following these guidelines." This policy is included in the 2019 Records Management Training for all employees, the New Employee Orientation, and will be included in the aforementioned policy memorandum awaiting release.

5. On an annual basis, request a certification from employees that they have not utilized their personal e-mail to conduct Government business. In the event that employees have utilized their personal e-mail, request a certification that they have forwarded any e-mails to their Government e-mail account.

   Management Response: Management disagrees with this recommendation. Certification is not required by law or regulation, and therefore not an appropriate

2

recommendation. However, OASAM has updated the 2019 Records Management Training for all employees to include detailed guidance and explicit language from the Federal Records Act on personal email, which also includes a Records Management Rules of Behavior acknowledgement form. Similarly, the New Employee Orientation provides guidance on personal email.

Management considers this recommendation unnecessary.

6. Make every reasonable effort to provide training and ensure awareness of each employee to avoid use of personal e-mail.

   Management Response: Management concurs with this recommendation. The Department already provides sufficient training. Conducting agency business via personal email is only permitted in rare and extenuating circumstances. Users are instructed in both the annual Records Management Training and New Employee Orientation to avoid the use of personal email and in the event that it is unavoidable, that they must capture and preserve the email within 20 days as instructed in the Federal Records Act Amendments of 2014.

7. Add to its rules of behavior or similar document an explanation of the employees' responsibility in preserving Federal records and require employees to sign the document indicating they have preserved all electronic messages that are potentially Federal records in accordance with DOL and NARA requirements.

   Management Response: Management concurs with this recommendation. OASAM has updated the 2019 Records Management Training for all employees to include a Records Management Rules of Behavior acknowledgement form.

8. Revise policies and procedures to provide explicit guidance addressing the use of mobile applications.

   Management Response: Management concurs with this recommendation. . OCIO is currently reviewing policy and technical solutions related to the ability to download encryption and other messaging applications. In accordance with the Mobile Device Rules of Behavior, Mobile application download(s) (App Store, Play Store, etc.) outside of what is installed on the smartphone or tablet during device provisioning is not permitted. Only certified applications made available through the DOL approved "App Catalog" may be installed on GFE mobile devices.

9. To improve awareness of guidance:
   a. Revise policies, procedures, and training to emphasize the requirements of maintaining Federal records;
   b. Monitor compliance with the requirements; and
   c. Require each employee to annually sign a statement certifying he or she has surrendered all documentation related to the official business of the Government and require a review of documents proposed for removal by the employee.

3

Management Response: Management concurs with this recommendation. The Department already provides adequate training, policies, and procedures on preservation requirements for Federal records.

The Departmental Records Officer (DRO) in partnership with the Agency Records Officers (ARO) continuously monitor compliance with the Federal Records Act. The DRO is currently conducting an internal evaluation of all agency records programs in order to ensure compliance.

All employees are required to certify (DL1-107) that they are not removing any Federal records and are provided with Records Management Documentary Materials Removal Guidance. Furthermore, all senior officials are provided with an exit briefing and are required to sign forms DL1-6057 or DL1-6058.

10. Develop official procedures to provide concrete guidance on the Capstone Approach. The procedures should include guidance on official review of the listing of Capstone Officials on a recurring basis.

Management Response: Management concurs with this recommendation. The Former Deputy Secretary issued the official Capstone policy in a 2016 policy memorandum. All AROs have been provided with training on Capstone, its implementation, and the requirements to update the Capstone official list each quarter.

The Office of Asset and Resource Management is currently working with the Office of the Solicitor and OCIO to develop additional standard operating procedures on the regular review of Capstone accounts, which will be codified in the DLMS.

Should you have any questions regarding the Department's response, please have your staff contact Tanisha Bynum-Frazier, Director, Office of Asset and Resource Management, at (202) 693-4546.

Sincerely,

Bryan Slater
Assistant Secretary for
Administration and Management

4

REPORT FRAUD, WASTE, OR ABUSE
TO THE DEPARTMENT OF LABOR

Online
http://www.oig.dol.gov/hotline.htm

Telephone
(800) 347-3756 or (202) 693-6999

Fax
(202) 693-7020

Address
Office of Inspector General
U.S. Department of Labor
200 Constitution Avenue, NW
Room S-5506
Washington, DC 20210