



*Electronic Record Retention Policies Do Not
Consistently Ensure That Records Are
Retained and Produced When Requested*

July 13, 2017

Reference Number: 2017-10-034

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number / 202-622-6500

E-mail Address / TIGTACommunications@tigta.treas.gov

Website / <http://www.treasury.gov/tigta>



To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration

P.O. Box 589

Ben Franklin Station

Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.



HIGHLIGHTS

ELECTRONIC RECORD RETENTION POLICIES DO NOT CONSISTENTLY ENSURE THAT RECORDS ARE RETAINED AND PRODUCED WHEN REQUESTED

Highlights

Final Report issued on July 13, 2017

Highlights of Reference Number: 2017-10-034 to the Internal Revenue Service Commissioner.

IMPACT ON TAXPAYERS

The IRS is required by Federal law to retain and produce Federal records when requested through appropriate legal means. Recently, the IRS reported that, when responding to requests from external parties, it had determined that some documents had been lost or destroyed. The Freedom of Information Act enables the public to request access to Federal records and information. The IRS's ability to adequately respond to Federal records requests is essential in maintaining the public's trust and ensuring transparency in Government.

WHY TIGTA DID THE AUDIT

This audit was requested by the Chairman of the House Committee on Ways and Means and Chairman of the Senate Committee on Finance to determine the IRS's policies for record retention, whether the policies comply with Federal requirements, and whether the IRS's practices for responding to requests for records ensure that responsive records are retained and provided according to Federal requirements.

WHAT TIGTA FOUND

IRS policies do not comply with certain Federal requirements that agencies must ensure that all records are retrievable and usable for as long as needed. For example, IRS e-mail retention policies are not adequate because e-mails are not automatically archived for all IRS employees. Instead, the IRS's current policy instructs employees to take manual actions to archive e-mails by saving them permanently on computer hard drives or network shared drives.

This policy has resulted in lost records when computer hard drives are destroyed or damaged. In addition, a recently instituted executive e-mail retention policy, which should have resulted in the archiving of e-mails from specific executives, was not implemented effectively because some executives did not turn on the automatic archiving feature.

For certain cases that TIGTA reviewed, IRS policies were not implemented consistently to ensure that all relevant documents were searched and produced when responding to external requests for records. TIGTA's review of 30 completed Freedom of Information Act requests found that in more than half of the responses, the IRS did not follow its own policies that require it to document what records were searched. TIGTA also found that IRS policies for preserving records from separated employees were not adequate.

WHAT TIGTA RECOMMENDED

TIGTA made five recommendations related to improving the IRS's policies for record retention and responding to external requests for records. For example, TIGTA recommended that the IRS implement an enterprise e-mail solution that enables the IRS to comply with Federal records management requirements. TIGTA also recommended that the newly issued policy on the collection and preservation of Federal records associated with separated employees is disseminated throughout the agency to ensure consistent compliance with Federal records retention requirements.

In their response to our report, IRS management agreed with all five recommendations. The IRS stated that deployment of a new enterprise e-mail solution is currently underway that should enable the IRS to comply with Federal records management requirements. The IRS also stated that it has issued interim guidance on the separating employee clearing process for collecting and preserving Federal records, which has been disseminated throughout the IRS.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 13, 2017

MEMORANDUM FOR INTERNAL REVENUE SERVICE COMMISSIONER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested (Audit # 201610016)

This report presents the results of our review to 1) determine the Internal Revenue Service's (IRS) policies for record retention and whether they comply with Federal requirements and 2) determine whether the IRS's practices for responding to Freedom of Information Act requests, litigation holds, and congressional requests ensure that responsive records are retained and provided according to Federal requirements. This review was requested by the Chairman of the House Committee on Ways and Means and the Chairman of the Senate Committee on Finance and is included in our Fiscal Year 2017 Annual Audit Plan. The review addresses the major management challenge of Protecting Taxpayer Rights.

Management's complete response to the draft report is included as Appendix V. We have concerns about the accuracy of certain statements in the IRS's response to our report. We have noted these concerns in Appendix VI.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me; Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations); or Danny R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Table of Contents

Background	Page 1
Results of Review	Page 7
Record Retention Policies Are Not Compliant With Certain Federal Requirements	Page 7
Recommendations 1 through 3:	Page 16
Some Responses to Requests for Records Did Not Ensure That All Records Were Searched and Produced	Page 17
Recommendations 4 and 5:	Page 21
Appendices	
Appendix I – Detailed Objectives, Scope, and Methodology	Page 22
Appendix II – Major Contributors to This Report	Page 25
Appendix III – Report Distribution List	Page 26
Appendix IV – List of Freedom of Information Act Exemptions	Page 27
Appendix V – Management’s Response to the Draft Report	Page 28
Appendix VI – Office of Audit Comments on Management’s Response	Page 34



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Abbreviations

C.F.R.	Code of Federal Regulations
CTO	Chief Technology Officer
ESCO	Executive Secretariat Correspondence Office
FOIA	Freedom of Information Act
FY	Fiscal Year
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
NARA	National Archives and Records Administration
PGLD	Privacy, Governmental Liaison, and Disclosure
TIGTA	Treasury Inspector General for Tax Administration
UNS	User and Network Services
U.S.C.	United States Code



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Background

Recently, members of Congress voiced concerns that the Internal Revenue Service (IRS) did not produce or had destroyed documents that should have been preserved for responses to Freedom of Information Act (FOIA)¹ requests. On March 21, 2016, the Treasury Inspector General for Tax Administration (TIGTA) received a request from the Chairman of the House Committee on Ways and Means. The letter requested that TIGTA examine and evaluate the IRS's general procedures and compliance or inability to comply with the procedures pertaining to the documents requested by Congress and other Government authorities in response to FOIA requests, litigation holds, and other external party requests.² The Chairman of the Senate Committee on Finance sent a similar request for TIGTA to review the IRS process for document productions in response to Congressional investigations, FOIA requests, or civil litigation.³

The IRS is subject to Federal requirements to identify and preserve Federal records. Federal laws and regulations require that Federal agencies preserve documents that are deemed records as described in the U.S. Code (U.S.C.) and regulated in the Code of Federal Regulations (C.F.R.).⁴ Agencies are also required to ensure that records documenting agency business are created or captured; records are organized and maintained to facilitate their use and ensure integrity throughout their authorized retention periods; and records are available when needed, where needed, and in a usable format to conduct agency business.

On August 24, 2012, in response to the November 2011 Presidential Memorandum on Managing Government Records, the Office of Management and Budget and the National Archives and Records Administration (NARA) issued Memorandum M-12-18, *Managing Government Records Directive*. The directive required that, by December 31, 2016, Federal agencies must manage both permanent and temporary electronic mail records (hereafter referred to as e-mail) in an accessible electronic format. E-mail records must be retained in an appropriate electronic system with the capability to identify, retrieve, and retain the records for as long as they are needed. The November 2011 and August 2012 memoranda marked a renewed attention on the recordkeeping requirements for e-mail messages already in place for Federal agencies.

The C.F.R. requires Federal agencies to implement internal controls over Federal records in electronic information systems to ensure reliability, authenticity, integrity, usability, content,

¹ 5 United States Code Section (§) 552.

² Letter from The Honorable Kevin Brady, Chairman, Committee on Ways and Means, to the Honorable J. Russell George, Inspector General, TIGTA, dated March 21, 2016.

³ Letter from The Honorable Orin Hatch, Chairman, Senate Committee on Finance, to the Honorable J. Russell George, Inspector General, TIGTA, dated September 21, 2016.

⁴ 36 C.F.R. § 1220.30, *Federal Records; General* (Oct. 2009).



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

context, and structure.⁵ Further, the C.F.R. describes the following functionalities that are necessary for electronic recordkeeping:

- Maintain records security: Prevent the unauthorized access, modification, or deletion of declared records, and ensure that appropriate audit trails are in place to track use of the records.
- Declare records: Assign unique identifiers to records.
- Capture records: Import records from other sources, manually enter records into the system, or link records to other systems.
- Organize records: Associate with an approved records schedule and disposition instruction.
- Manage access and retrieval: Establish the appropriate rights for users to access the records and facilitate the search and retrieval of records.
- Preserve records: Ensure that all records are retrievable and usable for as long as needed to conduct agency business. Agencies must develop procedures to enable the migration of records and their associated metadata⁶ to new storage media or formats in order to avoid loss due to media decay or obsolete technology.
- Execute disposition: Identify and effect the transfer of permanent records to the NARA based on approved schedules. Identify and delete temporary records that are eligible for disposal. Apply record holds or freezes on disposition.

In an effort to comply with C.F.R requirements for electronic recordkeeping, the IRS's Records Information Management Program formed the Enterprise eRecords Management Team in November 2014, with approximately two dozen IRS stakeholders. The team was assigned e-mail records management responsibilities that included identifying the needs of electronic records and policy gaps related to e-mail. The IRS's current e-mail system, Exchange Server 2010,⁷ requires users to take manual actions to archive e-mail and results in e-mail records that could be stored in multiple locations. Figure 1 below lists the different locations that the IRS currently stores e-mail records.

⁵ 36 C.F.R. § 1236.10, *Electronic Records Management* (Oct. 2009).

⁶ Metadata is defined as consisting of preserved contextual information describing the history, tracking, and management of an electronic document.

⁷ As of August 2016, the IRS is currently updating its e-mail system.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

Figure 1: IRS Multiple Storage Locations for E-mails

Mailbox Folder	This includes e-mail that exists in the user's mailbox, such as the Inbox, Sent Mail, and Deleted Items. E-mail remains in the user's mailbox, subject to the mailbox size.
Exchange Server	A snapshot of all user mailboxes is stored on an Exchange server.
Network Shared Drive	Since March 31, 2015, IRS executives are required to set Outlook so that e-mail is automatically archived permanently to a shared drive at least every 14 days.
Hard Drive	Users may elect to save e-mail to their hard drives. Laptops stored since January 2016 can be associated with the name of the separated employee.
Removable Media	Users may also save e-mail and other Federal records to devices such as flash drives, compact discs, or external hard drives.
Backup Tape	The Exchange servers containing copies of all mailboxes are backed up to tape. Since May 2013, Exchange server backup tapes are stored indefinitely.

Source: Discussions with IRS Information Technology (IT) organization management and review of IRS policy documents.

In addition to retaining Federal records, agencies must have the capability to produce these records in response to requests initiated through the FOIA, inquiries made by members of Congress, and information requests for discovery in litigation through litigation holds.⁸ The FOIA statute was enacted in 1966 and gives any person the right to request access to Federal agency records that are reasonably described by the requester and not subject to any of the nine FOIA exemptions.⁹ If the request reasonably describes the records, the agency is required to respond to the FOIA request within 20 business days of receipt of the request. The agency must either answer the request or inform the requester that an extension is required in order to respond fully to the request. The requester may also limit the scope of the request to enable the agency to provide an answer in the 20-business-day time frame. The IRS maintains a website to inform the public on how to file a FOIA request and where to send the request. The IRS has also set up an automated system as prescribed in the statute to track, manage, and store FOIA requests.

The IRS has dedicated staff under its Privacy, Governmental Liaison, and Disclosure (PGLD) offices to respond to requests for information under the FOIA statute as well as other types of information requests. These offices respond to all the requests across the country and work directly with requesters and the business units to provide responsive records or explain to the requester why a FOIA request is being denied or partially denied based on the nine exemptions

⁸ A litigation hold is a mechanism used to preserve relevant and responsive records related to any known or anticipated court proceedings.

⁹ 5 U.S.C. § 552, *Freedom of Information Act*, amended October 28, 2009, § (a)(3)(A)(i) and § (b). The Act mandates that all Government documents be released upon request for which nine exemptions do not apply. Appendix IV of this report lists the nine FOIA exemptions.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

in the FOIA statute. Moreover, IRS disclosure managers have been designated as FOIA public liaisons in accordance with Executive Order 13392, *Improving Agency Disclosure of Information*, dated December 14, 2005. The IRS has provided a comprehensive policy on how to handle FOIA requests in its Internal Revenue Manual (IRM).¹⁰ PGLD office caseworkers who process FOIA requests should be familiar with the records and the automated systems that the IRS maintains in order to assist in the location of information and ensure adequate searches.

When search efforts require going beyond searching the automated systems, the assigned PGLD office caseworker identifies which IRS business units may have responsive documents. The caseworker relies on the business unit liaisons to contact records custodians to search and produce the requested records. The caseworkers make a written request for a records search, including guidance for conducting the search, to the appropriate offices. The caseworker must document which IRS offices and employees were contacted and why, the files searched, search terms used, time spent in the search, copy and review process, and the volume and location of records found. Employees are required to search paper and electronic records and document the actions they took to perform the search. Employees are asked to make reasonable efforts to conduct searches for records in electronic formats and to provide records in the format requested. During our review period of Fiscal Year (FY)¹¹ 2012 through the third quarter of FY 2016, IRS records indicate that it processed over 50,000 FOIA requests. Of those 50,000 requests, the IRS provided all the requested documents for 33 percent. The average time to respond to the requests was 20 business days. Figure 2 shows the number of FOIA requests the IRS reported it had received and closed, those that remain open, and the average time spent to respond to the closed requests each fiscal year:

Figure 2: FOIA Cases Received and Closed, Open Cases, and the Average Number of Days to Close

FY	Total	Closed	Open	Average Days to Close
FY 2016 (thru 6/30/2016)	6,436	5,526	910	19
FY 2015	10,180	10,114	66	23
FY 2014	10,458	10,447	11	21
FY 2013	10,989	10,988	1	22
FY 2012	12,131	12,131	-	17
All Audit Years	50,194	49,206	988	20

Source: Review of IRS Automated FOIA tracking system.

¹⁰ IRM 11.3.13 – *Freedom of Information Act* (revised Aug. 14, 2013).

¹¹ A fiscal year is any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

The Office of Chief Counsel also issues litigation holds when litigation is initiated or reasonably anticipated. A litigation hold temporarily suspends the normal record retention policies to ensure that relevant evidence is preserved for use in litigation. This process requires searching, identifying, isolating, and preserving such evidence (whether in paper or electronic form) when litigation is initiated or is reasonably anticipated. The IRS has a dedicated staff within the Office of Chief Counsel who track and maintain litigation hold information. The Office of Chief Counsel is responsible for issuing a litigation hold by informing records custodians of their responsibility to preserve all paper and electronic files pertaining to the case. The litigation hold originates with the responsible attorney in charge of the litigation. Within 30 calendar days of receiving the case, the responsible attorney must notify, in writing, the IRS employees who are identified as records custodians of the responsibility to preserve relevant evidence, including their paper and electronic files. Custodians are identified through communication between the Office of Chief Counsel and relevant business units and are required to promptly forward the notice to their immediate manager. The responsible attorney ensures that custodians respond and provide the requested information within seven business days. If a custodian does not respond, the responsible attorney should follow up with the custodian and, if necessary, the custodian's manager. The attorney is responsible for the issuance, maintenance, collection, processing, and release and termination of the litigation hold.

During the course of litigation, the Office of Chief Counsel may need to request that the IRS IT organization collect electronic data from employees who possess information relevant to the litigation. The Associate Chief Counsel for Procedure and Administration in the Office of Chief Counsel is responsible for all Electronically Stored Information requests. The Office of Chief Counsel submits a request to the IT organization's E-Discovery Office, which supervises the Electronic Discovery Request. This search effort can include the employee's hard drive (when available), shared drives, and the Exchange server (which contains a portion of the employee's e-mails), external devices, IRS systems, and "Bring Your Own Device" hardware.¹² The E-Discovery Office only collects data from server backup tapes when specifically requested to do so by the Office of Chief Counsel. According to the Office of Chief Counsel, it issued over 12,000 litigation holds during our review period.¹³

In addition to FOIA requests and requests for information related to litigation, the IRS may receive information requests from members of Congress. The IRS has policies¹⁴ to respond to congressional inquiries related to oversight functions, which provide detailed instructions on receiving and responding to congressional inquiries. When the IRS receives a request from a

¹² The IT organization implemented the "Bring Your Own Device" program to permit IRS personnel to use non-Government-furnished, personally owned mobile devices for business purposes.

¹³ The figure of 12,000 litigation holds was provided by the IRS, but it could not be verified. The Office of Chief Counsel is currently back-filling the list and does not have a comprehensive list of all litigation-related requests and holds. The 12,000 figure is current as of January 3, 2017. Because this is an internally compiled list, we were unable to compare the list with another source.

¹⁴ IRM 11.3.4, *Disclosure of Official Information, Congressional Inquiries* (Sept. 12, 2013).



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

member of Congress, the Executive Secretariat Correspondence Office (ESCO), an office under the IRS Office of the Chief of Staff, deals specifically with responding to inquiries on behalf of the IRS Commissioner. The ESCO staff works with IRS business unit coordinators and subject matter experts to gather information relevant to these specific inquiries. For high-priority requests, the IRS Commissioner, the Counsel to the Commissioner, and the Chief of Staff may have final approval over the response to Congress. The ESCO's role is to assign requests to the correct personnel, review what is written, and send the final response to the requester once it has been approved and signed. The ESCO does not retrieve or retain any documents in its office. Additionally, congressional investigation document requests are handled by the Office of Chief Counsel. The Office of Chief Counsel takes the lead on document production in these cases. During the audit period, the ESCO received and tracked over 21,000 congressional, taxpayer, and other information requests.

This review was performed in the offices of the PGLD, Chief Counsel, multiple divisions of the IT organization, and the ESCO in multiple locations across the United States during the period March through December 2016. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Detailed information on our audit objectives, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Results of Review

Record Retention Policies Are Not Compliant With Certain Federal Requirements

IRS policies are not in compliance with Federal electronic records requirements and regulations.¹⁵ The IRS's current e-mail system and record retention policies do not ensure that e-mail records are saved and can be searched and retrieved for as long as needed. Additionally, repeated changes in electronic media storage policies, combined with a reliance on employees to maintain records on computer hard drives, has resulted in cases in which Federal records were lost or unintentionally destroyed. Examples from our case reviews show that it is especially difficult for the IRS to retain information from employees who have separated from the IRS.

Electronic media storage policies have changed repeatedly and do not ensure that records are retained

IRS standard policies for disposal of computer devices, including desktops, laptops, computer hard drives, and backup tapes, have been revised and reversed several times since May 2013. These repeated changes have had a negative impact on the IRS's ability to meet the record retention requirements and deadlines. The C.F.R. requires Federal agencies to implement internal controls over Federal records in electronic information systems, ensuring that all records are retrievable and usable for as long as needed to conduct business.¹⁶ Prior to May 22, 2013, standard asset disposal policies were in effect for all IRS devices, including desktops, laptops, computer hard drives, and backup tapes. Those standard asset disposal policies instructed IT organization personnel to wipe¹⁷ and reimage¹⁸ computer hard drives when they were no longer needed by IRS users. Subsequent to May 22, 2013, for a period of approximately 2.5 years, standard asset disposal policies for desktops and laptops changed several times. First, the process required wiping and reimaging the computer's hard drive. Next, the policy changed to retaining computers indefinitely. After that, the policy returned to standard asset disposal operations, except for select employees. Finally, asset disposal policies returned to refraining

¹⁵ This audit focused on IRS electronic record retention policies and did not evaluate the various controls the IRS has in place to retain hard-copy Federal records.

¹⁶ 36 C.F.R. § 1236.10, *Electronic Records Management* (Oct. 2009).

¹⁷ Wiping, or clearing, digital storage media is to use software or hardware products to overwrite storage space on the media with nonsensitive data.

¹⁸ Reimaging is the process of reinstalling the operating system and applications on a computer.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

from wiping the data from any hard drive associated with an IRS user.¹⁹ Figure 3 outlines the timeline of the changes made to the electronic media storage policies.

Figure 3: Timeline of IRS Information Technology Record Retention Policies

Prior to May 22, 2013	Standard policies were to wipe and reuse information technology equipment or remove the hard drive and send it to IT organization Enterprise Operations for destruction. Backup tapes were stored for six months and then reused.
May 22, 2013 to July 18, 2013	The Chief Technology Officer (CTO) ²⁰ directed that all media was to be preserved indefinitely.
July 18, 2013 to January 14, 2016	As part of the migration to Windows 7, the CTO authorized IT organization User and Network Services (UNS) to wipe and reimage user computers except those from the Tax Exempt and Government Entities Division and Communications and Liaison.
January 14, 2016 to Present	The UNS Associate Chief Information Officer reissued guidance to refrain from wiping the data from any hard drive associated with an end user.

Source: Discussions with IRS IT organization management and review of IRS policy documents.

These repeated changes impacted the effectiveness of the IRS’s record retention. Specifically, although policy updates were put in place, the hard drives from laptop and desktop computers stored by IT organization Enterprise Operations were not always associated with the name of the employee or the laptop from which the hard drive was taken. Without this correlation, successfully completing a search for specific e-mail or other electronic information residing on a disposed hard drive would be highly unlikely and could result in destroyed records.

For example, for one of the litigation cases reviewed, we found that when an employee separated from the IRS in August 2014, the employee left his laptop with his secretary. That employee was under a litigation hold to ensure that relevant evidence was preserved for use in litigation. However, without a policy in place to ensure that laptops of separating employees under

¹⁹ This updated policy applies to all end-user computing systems, Government furnished smartphones, tablets, and BlackBerry devices, including those belonging to separating employees.

²⁰ During the IRS Future State transition in late 2015 and early 2016, the CTO also had the title of Chief Information Officer. In June 2016, the CTO/Chief Information Officer left the IRS. As of July 2016, the IRS announced a new Chief Information Officer and no longer used the title of CTO.



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

litigation holds were maintained, that laptop was sent to the IT organization for standard sanitization and disposal.²¹

Storage policies for electronic media and computing devices are inefficient and ineffective

The IRS's current storage of hard drives and laptops is not a sustainable electronic recordkeeping solution to meet the record retention expectations required by the C.F.R., specifically, preserving records to ensure that all records are retrievable and usable for as long as needed to conduct agency business. On January 14, 2016, the UNS Associate Chief Information Officer reissued guidance on the asset disposal policy due to a high profile matter in litigation in which the IRS erroneously reported that it had wiped the hard drive from the laptop of a separated employee. The UNS Associate Chief Information Officer reversed the standard asset disposal policy and returned to refraining from wiping the data from any hard drive associated with an end user. To comply with the updated asset retention policies, the IRS has been storing hard drives and computing devices until the hold is lifted and normal processing of the equipment can resume. Hard drives and computing devices of separated employees can be stored in 53 locations within the IRS. Laptops and desktops from the Tax Exempt and Government Entities Division and Communications and Liaison are stored together in a separate location. According to the IRS, it has approximately 32,000 laptops and desktops²² in storage within the IRS. Figure 4 shows laptops, desktops, and hard drives stored on the floor and on shelves at three IRS locations. Currently, the IRS cannot readily produce an inventory report to identify the number and location of hard drives or computing devices currently in storage from separated employees. This condition makes it difficult for the IRS to locate the electronic records of separated employees if needed to respond to FOIA requests or other official inquiries.

The IRS is also accumulating backup tapes and incurring costs to purchase replacement backup tapes because current policy does not allow the reuse of the tapes. Similarly, new laptops are purchased when used laptops are not available in inventory for repairs and laptop loaner purposes. In addition, the IRS will expend considerable effort to process all of the equipment when the temporary asset hold policy is lifted.²³

²¹ Ultimately, the laptop was not destroyed because the employee's hard drive could not be powered on during the standard asset sanitation and disposal process. The hard drive instead was sent to the tape library and unintentionally retained.

²² The 32,000 laptops and desktops include computer equipment associated with employees, computer equipment that has been replaced as part of the IRS's refresh/replace initiative, and other equipment.

²³ During this audit, IT organization management developed a plan of action to inventory the stored computing devices and to prepare for the removal of the devices when the hold policy is lifted.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

Figure 4: Storage of Laptops, Desktops, and Hard Drives



Source: TIGTA's inspection of laptops, desktops, and hard drives stored by the IT organization at three IRS locations.



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Interim actions taken by the IRS while developing an upgraded e-mail solution do not prevent loss of e-mail records

The IRS's current e-mail system, Exchange Server 2010, does not meet Federal requirements for storing and managing e-mail messages. Memorandum M-12-18, issued by the Office of Management and Budget and the NARA, required that by December 31, 2016, Federal agencies must manage both permanent and temporary e-mail records in an accessible electronic format. E-mail records must be retained in an appropriate electronic system with the capability to identify, retrieve, and retain the records for as long as they are needed. As of September 30, 2016, the IRS reported to the NARA that it does not plan to fully deploy its enterprise e-mail solution until September 30, 2017, missing the mandate that Federal agencies must manage all e-mail records in an electronic format by December 31, 2016. As previously reported by TIGTA, the delay is due to the IRS's decision in April 2016 to change the type of e-mail system it would implement, after it had already begun efforts to upgrade its enterprise e-mail system in July 2015.²⁴

Additionally, limitations of IRS's current Exchange Server 2010 requires users to take manual actions to archive, to their computer hard drives, all e-mail and instant messages that are Federal records because the Exchange server mailbox does not provide the necessary storage capacity. According to the IRS, its Future State e-mail system being developed will potentially allow records to be available and searchable while automatically applying a retention policy. However, until a solution is effectively implemented, these e-mails remain difficult, if not impossible, to retain and search when needed. Due to the lack of storage and an automatic archiving solution, end users must store messaging data on the hard drives of their computing systems.

The IRS currently stores e-mail in multiple locations: mailbox folder, Exchange server, network shared drive, hard drive, removable media, and backup tape. There are limitations in the effectiveness of each of these locations for e-mail storage:

- Hard drives and removable media are not backed up.
- Backup tapes are intended for Disaster Recovery purposes and are not practical for searching for e-mail.
- Mailbox folders, Exchange servers, and network shared drives are subject to capacity limitations.

Due to the limitations of the current IRS e-mail system, which necessitate e-mail to be stored on user hard drives, the IRS risks destroying Federal records when user hard drives are erased, lost, or destroyed.

²⁴ TIGTA, Ref. No. 2016-20-080, *Review of the Enterprise E-Mail System Acquisition* (Sept. 2016).



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Implementation of the IRS's interim e-mail archiving policy for executives could be improved

The IRS issued an interim policy requiring IRS executives to archive their e-mail to a shared network drive; however, TIGTA found that this policy was not implemented effectively because some executives did not properly configure their e-mail accounts to archive e-mail as required, and the IRS did not have an authoritative list of all executives required to comply with the interim policy.

While the interim e-mail archiving policy was implemented to improve the IRS's ability to prevent the loss of e-mail records for executives, procedures were not developed to ensure that the e-mails of all designated executives were archived. In December 2014, the IRS issued an interim policy, *Interim Records Retention Policy on E-mail for IRS Executives*. This policy requires that e-mail be archived for all executives whose positions and responsibilities make them most likely to produce e-mail messages that meet the definition of a Federal record. E-mail of the IRS Commissioner and senior officials will be retained permanently. The IRS refers to this group's e-mail accounts as the Capstone accounts. E-mail of other IRS executives and senior managers will be retained for 15 years. Once the Exchange Server 2016 e-mail system is implemented, the solution for records disposition is planned to automate the retention process. It will also include a seven-year retention period for all end users not in the permanent or 15-year retention groups. In October 2015, the NARA approved the IRS's planned *Records Disposition Authority* for the three retention-period groups. However, improvements are needed to ensure that all executive accounts are identified and to verify that e-mails are actually archived for all executives in the permanent and 15-year retention groups.

Although interim policy requires that e-mail be archived for IRS executives, we found four executives from our sample of 20 who were not archiving e-mails as instructed. All four were members of the IRS Senior Executive Team.

Early in Calendar Year 2015, the IT organization compiled a list of 278 executives included in the permanent and 15-year retention groups from several executive pay plans based on information provided by the IRS Human Capital Office. Those executives were provided with instructions, training, and support to assist them in enabling the auto-archiving function of their Outlook e-mail accounts. However, there was no independent verification conducted to confirm that the e-mail accounts were actually configured to auto-archive e-mails as instructed. Additionally, there is no report that can be produced from Outlook or an Exchange server that can provide information to verify e-mail accounts with the auto-archiving function enabled. Therefore, all executives in this initial migration were required to self-certify that they had taken the steps, as instructed, to configure their e-mail accounts to auto-archive e-mail to a shared network drive.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

We tested a judgmental sample²⁵ of 20 executive e-mail accounts and found that four of the 20 (20 percent) executives did not have Outlook properly configured to archive e-mail to a shared drive as required by the interim policy. All four executives were members of the Senior Executive Team, the most senior executives of the IRS. The test showed that two of the four executives were not archiving e-mail at all, one executive was archiving to the hard drive instead of the shared drive that is backed up daily, and one executive was manually archiving e-mail to the shared drive rather than setting up Outlook to allow automatic archiving of the e-mail.

As a result of discussions with TIGTA during this audit, the IRS became aware that, after the initial migration of executives to the interim e-mail retention policy, there were no controls in place to ensure that newly on-boarded executives were also identified and their e-mail accounts were configured to archive their e-mail to a shared network drive. Consequently, the IRS took corrective action and, in September 2016, finalized Standard Operating Procedures designed to ensure that e-mail is archived for all newly on-boarded executives. In addition, the UNS conducted an analysis to identify any executives who started in their executive positions after the initial migration and who did not have their e-mail accounts configured to archive e-mails. A draft report of the results of their analysis as of November 2, 2016, showed that the UNS identified 23 executives whose e-mail accounts were not configured to archive their e-mail when they assumed their executive position.

Lastly, the IRS does not maintain one authoritative list of Capstone and other executive e-mail accounts. While the Standard Operating Procedure includes instructions for capturing the e-mail of executives on-boarding after September 2016, it does not provide for a reconciliation of the separate lists of executives compiled by the IT and PGLD organizations prior to the implementation of the Standard Operating Procedure. The IT organization prepared the initial list of 278 executives early in Calendar Year 2015 based on individuals in several executive pay plans. Since then, the PGLD office has prepared its own list of executives using information from sources different from the IT organization sources. The PGLD office list was compiled based on the IRS's Senior Executive Team and Executive Development lists. TIGTA's analysis showed that 75 names on the initial IT organization list were not included on a later list compiled by the PGLD office due to differing methods of compiling the lists. Without one authoritative list, the IRS cannot ensure that all executives are included in this effort and cannot verify that e-mails are archived for all required accounts.

IRS policy has been updated to help ensure that instant messages that are Federal records are retained

Prior to July 2016, the IRS did not have a well-defined, consistent policy on instant messaging retention for Federal records. Depending on the content of the message, instant messages may fall within the definition of a Federal record and, according to the NARA, agencies that allow instant messaging traffic on their networks must recognize that such content may be a Federal

²⁵ A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

record and must manage the records accordingly. However, at the time, the IRS had chosen to disable the auto-archive function of its instant messaging program, and thus did not save instant messages. Because the IRS did not save instant messages, it would be unable to produce any instant messages as records in response to an external information request.

On July 29, 2016, the PGLD office issued policy guidance for the use and preservation of all electronic messaging systems (including instant and text messaging platforms). The policy prohibits the use of instant messages and text messages for official business and states that if an instant message is created that is a Federal record, the user must save it before the message is closed out. If an instant message warrants retention, but not in conjunction with a case, policy, or project file, employees should move the message into their inbox or other e-mail folder. The message will then take on the retention prescribed under the IRS's e-mail management policy.²⁶ With the policy update, the IRS has provided a requirement and guidance for employees to save electronic messages.

IRS policies for preserving records of separating employees have improved

The design of the IRS's policies for preserving Federal records in the possession of separating employees did not ensure that all records were retained. The C.F.R. and the IRM require that Federal records be preserved for specific retention periods and that the records be searchable, but the IRS could not ensure compliance with these requirements for records associated with separated employees. Specifically, the IRS policy prior to May 2016 relied on separating employees to print Federal records, including those records contained on employee computer hard drives, before leaving the IRS, rather than storing them electronically. However, the IRS issued interim policies in May 2016, which were subsequently formalized in September 2016, to address some of identified gaps in retention of records from separating employees.²⁷ Because these policies were issued during our audit, we were unable to test whether the IRS effectively implemented the changes. Prior to these policy updates, the IRS did not have an effective mechanism for preserving information that may have been contained on separated employees' electronic devices.

The newly issued policies helped provide an improved ability to locate returned computing equipment while in storage. The policies required IT organization staff to update the asset management system records with location information and a litigation hold indicator, if applicable. Previously, the IRS recycled its hard drives as part of the employee separation process. This involved removing used hard drives and removing any remaining files by

²⁶ Instant messages that are subject to a litigation hold, regardless of whether the messages meet the definition of Federal records, must be saved prior to closing out of the message to ensure their preservation in the event they need to be produced.

²⁷ On September 23, 2016, this interim guidance and checklist were incorporated into IRM 1.15.5, *Records and Information Management, Relocating/Removing Records*.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

degaussing.²⁸ Prior to this, there were no standardized policies to ensure that all records and equipment were properly collected for later retrieval. Without implementation of these new policies, the IRS could not ensure that it was able to preserve and retrieve all documents associated with separated employees. Specifically, the newly issued policy requires separating employees to fill out a supplemental checklist, *Records Management Checklist for Separated Employees*, which includes a question asking if the separating employee has moved all Federal records stored on IT organization-issued equipment being turned in (laptop, flash drive, thumb drive, external hard drive, or other removable media) to an accessible, secure location. If yes, the employee must state where the data are stored.

IRS policies in place prior to the September 2016 update created problems for the IRS when attempting to retain and retrieve records associated with separated employees. Specifically, one of the two litigation cases we reviewed during our audit displayed the potential for the destruction of electronic Federal records if separated employees do not ensure that those records are saved and hard drives are preserved. In the one litigation case, the IRS reported in 2014 that 11 employees' hard drives were likely unavailable because the employees had already separated from the IRS. The standard asset disposal policy at the time the employees separated would have been to sanitize and reimage hard drives, making the equipment available for reuse, or to destroy hard drives if they were outdated equipment. However, because at the time the IRS did not have a policy in place to indefinitely preserve e-mails or hard drive contents of separating employees, the IRS assumed potential Federal records on the separated employees' computers had not been preserved.

The IRS recently implemented mandatory records management training for employees and contractors

Prior to FY 2015, the IRS did not provide records management training for IRS employees or contractors. Since July 1997, the C.F.R. requires that all agencies provide guidance and training to all agency personnel on their records management responsibilities, including how to identify Federal records in all formats. In June 2015, the NARA completed an inspection of the IRS's Records and Information Management program that examined whether the IRS's Records and Information Management program was in compliance with Federal requirements. The resulting report recommended that Records and Information Management staff develop and implement mandatory records management training for all staff, including senior executives and contractors, to ensure agencywide understanding of their roles and responsibilities under the law.

Our review found that, starting in FY 2015, records management training material was added to an existing training that all IRS employees and contractors are required to take within 10 days of their hire date and then taken annually each summer thereafter. In July 2016, a separate Records Management training was developed and became part of the employee and contractor mandatory

²⁸ Degaussing is a process in which magnetic media is exposed to a powerful, alternating magnetic field. Degaussing removes any previously written data, leaving the media in a magnetically randomized (blank) state.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

training. The training addresses employee and contractor responsibilities and states that contractors have the same responsibility as agency employees to manage and protect Federal records. The implementation of training requirements has helped the IRS become compliant with Federal regulations and will inform employees and contractors of their responsibilities with respect to record retention requirements.

Recommendations

Recommendation 1: The IRS Chief Information Officer should implement an enterprise e-mail solution that enables the IRS to comply with Federal records management requirements, including the ability to organize and maintain the records to facilitate their use when and where they are needed in a usable format and to ensure preservation throughout their authorized retention periods.

Management's Response: The IRS agreed with this recommendation. The IRS stated that deployment of a new enterprise e-mail solution is currently underway and should enable the IRS to comply with Federal records management requirements, including the ability to organize and maintain the records to facilitate their use when and where they are needed in a usable format and to ensure preservation throughout their authorized retention periods.

Recommendation 2: The Director, PGLD, should document the methodology for developing one authoritative list of executives in the permanent and 15-year retention groups and coordinate with IT organization personnel to verify that all identified executive e-mail accounts are properly configured to archive e-mail.

Management's Response: The IRS agreed with this recommendation. The IRS stated that it has developed a Standard Operating Procedure that documents the methodology and step-by-step tasks needed to verify that all identified executive e-mail accounts are properly configured to archive e-mail, including coordination with both the Human Capital Office and IT organization to ensure a single authoritative list. As part of its compliance with Office of Management and Budget Directive M-12-18, the IRS will initiate a systemic migration of all executive e-mail accounts into an appropriate recordkeeping system to ensure all identified executive e-mail accounts are properly configured.

Recommendation 3: The Director, PGLD, should ensure that the newly issued policy on the collection and preservation of Federal records associated with separated employees is disseminated throughout the agency to ensure consistent compliance with Federal records retention requirements within all business units.

Management's Response: The IRS agreed with this recommendation. The IRS issued separating employee clearance interim guidance on May 5, 2016, which was subsequently published in IRM 1.15.5, Records and Information Management, on



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

September 23, 2016. This policy guidance updated the separating employee clearance process for collecting and preserving Federal records. The guidance was disseminated throughout the IRS using various internal communication channels, and the communication is ongoing.

Some Responses to Requests for Records Did Not Ensure That All Records Were Searched and Produced

Our review of a judgmental sample²⁹ of 35 FOIA requests, two requests from congressional committees, and two court cases that required document responses found that, for certain cases, IRS processes in response to requests for records did not consistently ensure that potentially responsive records were searched and produced. Annually, the IRS responds to thousands of FOIA requests and congressional inquiries and issues numerous litigation holds associated with potential court actions. In response to these external requests, specific offices within the IRS, including the Office of Chief Counsel, the PGLD office, and the ESCO, search for responsive records and provide the records to appropriate parties. Although the majority of FOIA requests are completed timely, we found that some cases were not closed timely. We also found instances in which the search methods used were not properly documented in accordance with IRS policies, did not identify all potential custodians, and erroneously concluded that records associated with separated employees had been destroyed when potentially responsive records were available. Federal laws governing FOIA searches, IRS policies for responding to congressional requests, and court procedures all include specific guidance that requires adequate searches of records in response to external requests. However, in some of the cases reviewed, documentation of IRS search efforts in response to requests for records was not adequate.

The IRS responded to a majority of FOIA requests timely, but a small number of responses took more than one year to complete

While congressional requests and litigation-related disclosures usually have response dates specified by the requester, FOIA requests have explicit response deadlines prescribed by law. Specifically, Federal agencies are required to respond to requests within 20 business days of receipt, and can request an extension of 10 working days. If an agency grants a FOIA request, the FOIA statute requires that they make responsive records “promptly available” to the requester.

Of the almost 50,000 FOIA cases closed during the audit period, IRS records indicate that over 36,000 were closed in 20 business days or less. For the almost 13,000 remaining cases, the average closing time was 51 business days. In reviewing the remaining cases that had much longer processing times, we found that 100 cases took between one and two years to close, and

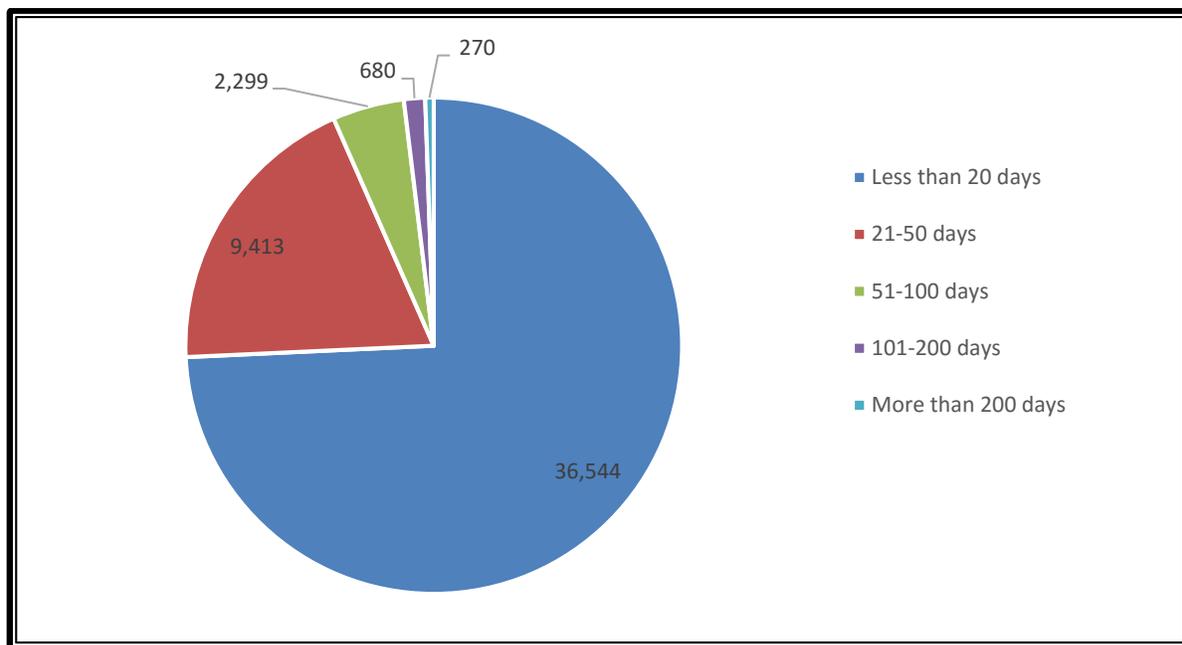
²⁹ A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

three cases took between two and 2.5 years to close. For the FOIA requests that involved longer than normal processing times, the volume of responsive documents can exceed 10,000 pages, and the review process must ensure the redaction of Section (§) 6103 information³⁰ and Privacy Act information as well as information based on FOIA exemptions specifically identified by law.³¹ Additionally, some records are housed in the Federal Records Centers, which have a policy of providing records to the IRS offices within 60 days. Figure 5 shows the breakdown of the IRS's response times for the almost 50,000 FOIA requests closed during our audit period.

Figure 5: IRS Response Time for Closed FOIA Cases



Source: Review of IRS Automated FOIA data of cases closed between October 1, 2011, and June 30 2016.

In addition to the overall analysis of FOIA responses, we also reviewed a judgmental sample of 35 FOIA requests: 18 FOIA cases that the IRS labelled as “sensitive,” two FOIA cases that were referred by PGLD office caseworkers, and 15 cases that the IRS did not label as sensitive.³² Of the 35 FOIA requests we reviewed, 30 cases were closed as of June 30, 2016. Of those 30 cases,

³⁰ 26 U.S.C. § 6103, *Confidentiality and Disclosure of Returns and Return Information*, prohibits disclosure of taxpayer return or return information to a third party, in order to protect the privacy of the taxpayer.

³¹ 5 U.S.C. § 552, *Freedom of Information Act*, lists nine specific exemptions and form the legal basis for the IRS to withhold records or portions of records from the public. Careful consideration of the exemption is required when reviewing responsive records. See Appendix IV for a list of the nine exemptions.

³² The 35 FOIA requests were judgmentally selected based on a variety of ranking criteria, including the type of request (individual taxpayer, administrative request, media/external party sensitive request), the disposition of the FOIA request (full grant, partial grant, full denial), the complexity of the request, and the seniority of the caseworker assigned to the request. A judgmental sample is a nonstatistical sample, and the judgmental sample case results cannot be projected to the population of FOIA requests responded to by the IRS during our audit period.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

23 took longer than 20 business days to close. While many of the 30 requests were closed only a few days after the requested or required date, the average time to close the 30 cases was 212 business days, and the records for some requests took over two calendar years to fully produce. However, it should be noted that we selected FOIA cases with longer response times as part of our sample so that we could determine the cause of these delays. Many of the delays we observed related to the time it took for business units to search for, gather, and provide the responses to the PGLD. The five open cases are awaiting processing by the Office of Chief Counsel, and the average elapsed time was 389 business days.

For the cases with longer response times, PGLD office officials stated that they did not have authority to compel other business units to respond to their requests. For example, the PGLD office has held meetings with the Office of Chief Counsel in order to try to work through the backlog of cases and prioritize workflow. However, the custodian of requested records in one of the Offices of Chief Counsel repeatedly did not respond to multiple overdue FOIA requests from one requestor.

Additionally, according to the IRS, technology currently available in the agency to produce, review, and redact the documents needed to respond to FOIA requests is limited. Specifically, the software used to respond to FOIA requests lacks basic functions, such as the ability to remove duplicate documents. In order to collect and review documents in response to FOIA requests, caseworkers must manually review duplicate documents, scan for key words and phrases that are marked for exemption, and redact text that falls within the nine FOIA exemptions as well as § 6103 and Privacy Act information.

Finally, delays in processing FOIA requests were also affected by the fact that the Office of Chief Counsel has a limited number of staff devoted to processing FOIA requests from the PGLD office. Specifically, three Chief Counsel office paralegals are responsible for initiating the search and collection effort for responsive documents from 14 Chief Counsel office branches, reviewing the documents received from the custodians, and performing redactions³³ for the thousands of pages of documents typically produced for many of these FOIA requests. As a result of the limitations in both staffing and information technology resources in responding to FOIA requests, a small number of FOIA cases we reviewed experienced significant delays.

Policies requiring the IRS to document search efforts were not followed for some cases

For some of the cases we reviewed, the IRS did not document, as required by IRS policy, what records were searched and which custodians searched for the records, and in some cases the IRS did not identify all custodians with responsive records. The FOIA requires that an agency make

³³ Because of the sensitivity of some of the requested documents from the Office of Chief Counsel and Criminal Investigation, those business units perform the redactions prior to sending the documents to the PGLD office.



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

reasonable efforts to search for records that have been reasonably described by the requester. When the IRS receives a FOIA request, PGLD office caseworkers identify which IRS business units they believe have responsive documents. IRS policies direct PGLD office caseworkers to rely on FOIA functional contacts³⁴ within business units to identify custodians of records. The functional contacts direct potential custodians to search for responsive records and then provide those records to the PGLD office. The response must document who searched for the records, the search terms used, the systems searched, and the time expended to search for and retrieve the records. However, for 20 of 30 closed cases reviewed,³⁵ TIGTA found that the IRS did not follow its own policies that require it to document which employees searched for responsive records and what criteria were used in the search. Without this information, the PGLD office was unable to document that an adequate search was performed.

In addition, our case review found four instances in which the IRS did not search for all responsive records. To ensure adequate search efforts, IRS policies state that PGLD office caseworkers should be familiar with the records the IRS maintains and, if necessary, involve various functional areas. We identified four cases for which IRS search efforts did not find all custodians with responsive records. Specifically, for one case, the PGLD office caseworker did not reach all the custodians who had responsive records because the caseworker did not send the request to all the functional contacts of the business unit identified in the incoming request. Instead, the request was sent only to the revenue agent named in the request. The case later went to litigation, and the judge found an inadequate search effort on the part of the IRS. Additional responsive records were found in other business units after one of the senior Office of Chief Counsel attorneys reviewed the request and expanded the search effort. When asked why the FOIA request was not sent to the other departments, the PGLD office caseworker stated that she did not know why she excluded those two areas stated in the FOIA request.

The IRS does not have a consistent policy to search for records from separated employees

As stated previously, IRS policies for preserving Federal records in the possession of separating employees did not ensure that all records were retained. In addition to concerns over the preservation of records, we also found weaknesses in the IRS policy associated with searching for responsive records associated with separated employees. Specifically, our review also found that the IRS did not have a policy regarding when or whether to search for separated employees' records in response to FOIA requests, litigation,³⁶ and congressional requests. In addition, we received different responses from various business units when we inquired about policies

³⁴ Each business unit has a FOIA functional contact who works as a liaison between the PGLD office and the business unit. These coordinators perform this function as an ancillary duty.

³⁵ We reviewed 35 cases, five of which were still open as of June 30, 2016.

³⁶ The Chief Counsel office issued CCDM 34.7.1 on February 24, 2016, related to searching for documents for separated employees as part of the litigation hold process; however, for the litigation cases we reviewed, this policy was not yet in place.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

governing the search for records associated with separated employees in response to a FOIA request. The PGLD office Disclosure Policy and Program Operations Director, the PGLD office caseworkers, and the business unit functional contacts, specifically in the IT organization, described their understanding of the policy, and each description was different.

In our case reviews, we found that IRS efforts in response to requests for records do not consistently search records of separated employees. For example, in one of the litigation cases we examined, the IRS did not search for records associated with one of 11 employees who had separated. In October 2014, the Department of Justice, on behalf of the IRS, filed a document with the court stating that 11 former IRS employees' laptop hard drives were "likely unavailable" for electronic discovery of evidence. However, in our search, we found that, according to the IRS inventory system, one hard drive was listed as in-stock at the time the court document was filed and thus could have been searched to determine if records were still available.

Recommendations

The Director, PGLD, should:

Recommendation 4: Ensure that the policy for documenting search efforts is followed by all employees involved in responding to FOIA requests.

Management's Response: The IRS agreed with this recommendation. The IRS stated that search efforts should be adequately documented by employees processing FOIA requests. To that end, a communique will be issued to all Disclosure personnel emphasizing the need to thoroughly document all search efforts in the electronic FOIA case file and will include the salient sections of IRM 11.3.13 that provide guidance on that process. In addition, training and case reviews will be conducted to review these IRM sections and reinforce search documentation requirements. The IRS will also conduct training for all agency FOIA Functional Coordinators, establishing the expectations for documenting business unit search efforts.

Recommendation 5: Develop a consistent policy that requires Federal records associated with separated employees be searched as part of the IRS's responses to Federal requests for records, and ensure it is followed by all business units.

Management's Response: The IRS agreed with this recommendation. The IRS stated the policy regarding separated employee records is already established and documented within the Records and Information Management IRM, which establishes agency policy surrounding search efforts associated with separated employees. The IRS will establish a complementary process to address FOIA obligations with respect to separated employees and will update the formal FOIA search memo appropriately.



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Appendix I

Detailed Objectives, Scope, and Methodology

Our objectives were to 1) determine what the IRS's policies are for record retention¹ and whether they comply with Federal requirements and 2) determine whether the IRS's practices for responding to FOIA requests, litigation holds, and congressional requests ensure that responsive records are retained and provided according to Federal requirements. To accomplish our objectives, we:

- I. Determined if the IRS's record retention policies, including electronic documents, e-mail, and instant messages, comply with Federal record retention regulations and requirements.
 - A. Obtained all IRS record retention policies, procedures, and practices including retaining records on hard drives, Exchange servers, and Exchange backup tapes.
 - B. Identified and documented all changes in IRS records retention policies from FY 2013 to the present.
 - C. Compared IRS electronic records retention policies, procedures, and practices to Federal requirements and determined if the IRS is in compliance.
- II. Evaluated the effectiveness of the IRS's record retention policies, procedures, and practices to ensure that required records are saved and can be retrieved.
 - A. Determined if retention policies for e-mail, instant messages, hard drives, and backup tapes were consistently communicated.
 - B. Documented the records retention and retrieval responsibilities within the IRS's IT organization.
 - C. Identified all locations where the personal devices and hard drives of separated employees are stored.
 - D. Visited three locations where the hard drives and laptops of separated employees are stored.²

¹ Our audit focused on retention of electronic IRS documents. IRS policies for preserving paper records, such as those related to specific taxpayers which can be stored in paper format at IRS offices and Federal Records Centers, were not included as part of this audit.

² We looked at hard drives and backup tape retention in Martinsburg, West Virginia, and observed the storage of laptops and hard drives in New Carrollton, Maryland, and Memphis, Tennessee.



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

- E. Documented all repositories of e-mail records.
 - F. Selected a judgmental sample³ of Capstone accounts and determined if the individuals associated with the Capstone accounts have complied with the policy to save e-mail.
- III. Examined the IRS's policies and practices for responding to FOIA requests, litigation holds, civil discovery, and congressional requests to determine whether these policies and practices comply with Federal records requirements.
- A. Identified and reviewed Federal guidance and IRS policies and processes that apply to FOIA requests, litigation holds, civil discovery, and congressional requests.
 - B. Reviewed the circumstances under which the IRS informs its employees and contractors that they are custodians and the steps taken to ensure that responsive records are preserved and produced. We determined whether employee and contractor training is designed to ensure that employees and contractors comply with Federal records requirements.
- IV. Tested a judgmental sample of IRS responses to FOIA requests to determine whether the IRS's actions complied with its policies and with FOIA requirements.
- A. Obtained from the IRS Automated FOIA system an extract of FOIA cases received from FY 2012 to present. We assessed the validity of the data we received by electronically testing for missing data, outliers, and obvious errors as well as independently validating the data from the source system during a site visit. We determined the data to be sufficiently reliable for our audit purposes.
 - B. Determined the criteria by which the IRS categorizes its FOIA requests (individual, media, political organizations, *etc.*) and responses (full grant, partial grant, full denial) for purposes of selecting the judgmental sample.
 - C. Selected a sample of FOIA requests to test for compliance with IRS policies and FOIA requirements. The sample was judgmentally selected based on a variety of ranking criteria, including the type of request (individual taxpayer, administrative request, media/external party sensitive request), the disposition of the FOIA (full grant, partial grant, full denial), and the seniority of the caseworker assigned to the request.
 - D. Reviewed the FOIA request responses to ensure compliance with IRS policies and FOIA requirements.
- V. Selected and reviewed in detail instances from FY 2012 to June 30, 2016, in which the IRS was required to provide documents to external parties, including FOIA requesters,

³ A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

other parties to IRS litigation, and congressional requests. We selected a judgmental sample of four cases based on the complexity of the request, the scope of the request, and the public attention surrounding the associated case or issue related to the request.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objectives: the IRS's policies, procedures, and practices for retaining, searching, and producing records. We evaluated these controls by reviewing Federal and IRS policies and requirements; interviewing management; reviewing applicable documentation; reviewing systems used to retain, search, and produce records; and reviewing external requests for information and responses to those requests.



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Appendix II

Major Contributors to This Report

Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations)
Danny R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
John L. Ledford, Director
Jonathan T. Meyer, Director
Myron L. Gulley, Audit Manager
Deanna G. Lee, Audit Manager
LaToya R. Penn, Audit Manager
Joan M. Bonomi, Lead Auditor
Sharon M. Downey, Lead Auditor
Lara Phillippe, Senior Auditor
Sylvia Sloan-McPherson, Senior Auditor
Daniel Burd, Auditor
Craig LeQuire, Auditor
Meghann Noon-Miller, Auditor



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Chief Information Officer
Director, Office of Audit Coordination



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Appendix IV

List of Freedom of Information Act Exemptions

Exemption 1	Information that is classified to protect national security.
Exemption 2	Information related solely to the internal personnel rules and practices of an agency.
Exemption 3	Information that is prohibited from disclosure by another Federal law.
Exemption 4	Trade secrets or commercial or financial information that is confidential or privileged.
Exemption 5	Privileged communications within or between agencies, including: <ul style="list-style-type: none">- Deliberative Process Privilege.- Attorney-Work Product Privilege.- Attorney-Client Privilege.
Exemption 6	Information that, if disclosed, would invade another individual's personal privacy.
Exemption 7	Information compiled for law enforcement purposes that: <ul style="list-style-type: none">- 7(A). Could reasonably be expected to interfere with enforcement proceedings.- 7(B). Would deprive a person of a right to a fair trial or an impartial adjudication.- 7(C). Could reasonably be expected to constitute an unwarranted invasion of personal privacy.- 7(D). Could reasonably be expected to disclose the identity of a confidential source.- 7(E). Would disclose techniques and procedures for law enforcement investigations or prosecutions.- 7(F). Could reasonably be expected to endanger the life or physical safety of any individual.
Exemption 8	Information that concerns the supervision of financial institutions.
Exemption 9	Geological information on wells.

Source: 5 U.S.C. § 552, Freedom of Information Act.



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Appendix V

Management's Response to the Draft Report

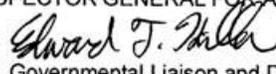


PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

June 8, 2017

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Edward T. Killen 
Director, Privacy, Governmental Liaison and Disclosure

SUBJECT: Draft Audit Report – Electronic Record Retention Policies Do Not
Consistently Ensure That Records Are Retained and Produced
When Requested (Audit #201610016)

Thank you for the opportunity to review the above referenced draft audit report. We agree with the recommendations and appreciate your recognition of the positive steps taken by IRS to update our policies related to electronic records. The IRS is committed to properly retaining electronic and paper records and producing those records when requested. We are pleased to report that the National Archives and Records Administration (NARA) recently assessed our success criteria toward full compliance with the Managing Government Records Directive (M -12 -18) and rated the IRS at a "low risk of not managing email effectively."¹

While we agree with your recommendations, we wish to offer additional perspective regarding the IRS official recordkeeping system and the cases selected for review. For the period under audit, the IRS followed NARA guidance which allows agencies to maintain official records in paper format while transitioning to an approved system for storing records in an electronic format.² This context and timing is important because during the time period covered by this audit, IRS policies for maintaining official records were in full compliance with NARA regulations for a paper system transitioning to an electronic system. As such, we do not agree with your finding that IRS policies do not comply with the NARA guidelines in place during the time of this audit.

¹ See National Archives and Records Administration, 2016 Federal Email Management Reports, available at <https://www.archives.gov/records-mgmt/email-management/email-management-reports-2016> (last visited May 19, 2017).

² National Archives and Records Administration (NARA) guidance and products acknowledge the need to "print and file" in the absence of an acceptable electronic recordkeeping solution. See *NARA 861 – Email Records Management*, (February 5, 2015), 861.2 Policy, that states, "Email records dated on or before January 22, 2013 are governed by NARA's "print and file" policy for managing email records.", (February 5, 2015); See also NARA, *White Paper on The Capstone Approach and Capstone GRS*, that states, "Until recently, NARA supported this [print and file] practice even as it encouraged agencies to adopt electronic recordkeeping systems. 7, (April 2015), and NARA, Department of the Treasury, Internal Revenue Service, *Records Management Inspection Report*, (June 30, 2015).



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

2

The audit report refers to an IRS policy instructing employees to manually save emails to hard drives. While instructions do exist for saving emails to hard drives to mitigate lack of storage space, this process does not constitute an approved system for maintaining Federal records and is not IRS records policy. Rather, IRS policies require employees to print electronic records and place paper copies in official files.³ Contrary to the report, policies requiring employees to convert electronic records to paper format for filing helps, rather than hinders, maintaining official records if computer hard drives are damaged or destroyed.

The report states that IRS electronic media storage policies changed repeatedly since May 2013, and this created a negative impact on our ability to meet record retention requirements and deadlines. While we agree that asset disposal policies changed, the changes were necessary to maintain records management integrity. Electronic media storage guidance and procedures were revised on three occasions between May 22, 2013 and January 14, 2016, specifically to reduce the potential for inadvertent destruction of files residing locally on laptop or desktop hard drives during processing through standard equipment sanitization and disposal procedures. The necessary policy changes addressed specific Congressional and litigation hold requirements while also mitigating a procedural gap in the separating employee clearance (SEC) process. Additionally, the policy changes allowed for the repurposing of usable laptop and desktop equipment thereby reducing overall replacement costs. The policy updates were necessary because of the changed circumstances.

The report contains pictures of laptops, desktops and hard drives stored at three IRS locations, yet fails to provide the context for the items stored and the security measures in place to protect these items. The vast majority of the equipment in the photographs was generated from the replacement of aged equipment (e.g., laptops, desktops, servers). As described above under IRS policies, electronic records located on an employee's computer should be printed and placed in the official file or managed in another appropriate recordkeeping system. In addition, when an employee's aged equipment is scheduled for replacement, it is IRS's practice to move the data from the old hard drive to the new equipment during the replacement process. Consequently, data residing on aged equipment should be copied to the new equipment. For the specific equipment in the photos held under a Congressional or litigation hold, data should have been moved from the hard drives to other platforms before storage. With respect to the small portion of equipment that was obtained from separated employees, this equipment also should not contain official records because of the print and file policy described above, and IRS policy regarding separating employee records set forth in the Records and Information Management (RIM) Internal Revenue Manual (IRM).

³ Internal Revenue Manual, 1.15.6.9, Retention and Disposition of Electronic Records, (03-27-2014).



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

3

Our ability to properly store and locate records is one of the key reasons the IRS is able to respond in a timely manner to Freedom of Information Act (FOIA) requests. As the report notes, the IRS responds to the majority (about 3/4th) of FOIA requests within 20 days. Some of the cases with much longer processing times involved documents that were requested by both Congress and outside organizations (through FOIA or litigation). Those documents had to be provided to Congress first, which contributed to delays for the outside organizations.

We are concerned about the finding that Freedom of Information Act (FOIA) cases did not document what records were searched. While we agree with your recommendation to ensure the policy for documenting search efforts is followed, in general we believe adequate searches took place to facilitate appropriate record production to FOIA requestors. This is corroborated by the small number of requests that result in litigation each year. This background is important to understand. Our offices process and release hundreds of thousands of pages during each fiscal year. In FY2016 alone, the IRS processed 8,791 FOIA requests; however, less than one percent of that amount resulted in litigation.⁴

The cases selected for review in this engagement were chosen specifically because there were public allegations of perceived or actual data loss, or because they were so large and complex they would be expected to stress the system. We appreciate that because TIGTA used a judgmental sample instead of a statistically valid sample, the findings in this report cannot be projected to apply to the population of FOIA responses, Congressional responses or other matters in which the IRS produces records to requestors. Nevertheless, the recommendations made raise good points that can improve our overall processes.

Attached is a detailed response outlining our corrective actions.

If you have any questions, please contact me at 202-317-6449, or a member of your staff may contact Celia Doggette, Director, Identity and Records Protection, at 202-317-6451.

Attachment

⁴ Department of the Treasury, *2016 Freedom of Information Act Annual Report*, available at https://www.treasury.gov/FOIA/Documents/FY16_Annual_Report_FINAL.pdf (last visited May 23, 2017), 15.



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Attachment

RECOMMENDATION 1: The IRS Chief Information Officer should implement an enterprise email solution that enables the IRS to comply with Federal records management requirements, including the ability to organize and maintain the records to facilitate their use when and where they are needed in a usable format, and ensure preservation throughout their authorized retention periods.

CORRECTIVE ACTION: The IRS agrees with this recommendation. Deployment of a new enterprise email solution is currently underway. The new enterprise email solution will enable IRS to comply with Federal records management requirements, including the ability to organize and maintain the records to facilitate their use when and where they are needed in a usable format, and ensure preservation throughout their authorized retention periods.

IMPLEMENTATION DATE: October 15, 2017

RESPONSIBLE OFFICIALS: IRS Chief Information Officer (Associate Chief Information Officer, Enterprise Operations)

CORRECTIVE ACTION MONITORING PLAN: The IRS will monitor implementation of the recommendation as part of the servicewide roll-out of the Enterprise Exchange Upgrade.

RECOMMENDATION 2: The Director, Privacy, Governmental Liaison, and Disclosure, should document the methodology for developing one authoritative list of executives in the permanent and 15-year retention groups, and coordinate with IT organization personnel to verify that all identified executive email accounts are properly configured to archive email.

CORRECTIVE ACTIONS: The IRS agrees with this recommendation.

1. We developed a Standard Operating Procedure (SOP) that documents the methodology and step-by-step tasks needed to verify that all identified executive email accounts are properly configured to archive email, including coordination with both the Human Capital Office and Information Technology to ensure a single authoritative list.
2. As part of its compliance with OMB Directive M-12-18, IRS will initiate a systemic migration of all executive email accounts into an appropriate record keeping system to ensure all identified executive email accounts are properly configured.

IMPLEMENTATION DATES:

1. Implemented
2. October 15, 2017



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

RESPONSIBLE OFFICIALS:

1. Director, Privacy, Governmental Liaison and Disclosure (Director, Identity and Records Protection)
2. IRS Chief Information Officer (Associate Chief Information Officer, Enterprise Operations)

CORRECTIVE ACTION MONITORING PLAN: The IRS will monitor implementation of the recommendation as part of the servicewide roll-out of the Enterprise Exchange Upgrade.

RECOMMENDATION 3: The Director, Privacy, Governmental Liaison, and Disclosure, should ensure that the newly issued policy on the collection and preservation of Federal records associated with separated employees is disseminated throughout the agency to ensure consistent compliance with Federal records retention requirements within all business units.

CORRECTIVE ACTIONS: The IRS agrees with this recommendation. We issued separating employee clearance (SEC) interim guidance on May 5, 2016, which was subsequently published in Internal Revenue Manual (IRM) 1.15.5, Records and Information Management, on September 23, 2016. This policy guidance updated the SEC process for collecting and preserving Federal records. This guidance was disseminated throughout the IRS using various internal communication channels and this communication is on-going.

IMPLEMENTATION DATE: Implemented

RESPONSIBLE OFFICIALS: Director, Privacy, Governmental Liaison and Disclosure (Director, Identity and Records Protection)

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION 4: Ensure that the policy for documenting search efforts is followed by all employees involved in responding to FOIA requests.

CORRECTIVE ACTIONS: The IRS agrees with this recommendation. Search efforts should be adequately documented by employees processing FOIA requests. To that end, a communique will be issued to all Disclosure personnel, emphasizing the need to thoroughly document all search efforts in the electronic FOIA case file and will include the salient sections of IRM 11.3.13 that provide guidance on that process. In addition, training and case reviews will be conducted to review these IRM sections and reinforce search documentation requirements. We will conduct training for all agency FOIA



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Functional Coordinators (FFCs), establishing the expectations for documenting Business Unit search efforts.

IMPLEMENTATION DATE: December 15, 2017

RESPONSIBLE OFFICIALS: Director, Privacy, Governmental Liaison and Disclosure (Director, Governmental Liaison, Disclosure and Safeguards)

CORRECTIVE ACTION MONITORING PLAN: The IRS will monitor implementation of the recommendation as part of the overall project plan established to ensure that the policy for documenting search efforts is followed by all employees involved in responding to FOIA requests. The corrective action plan includes the following target dates:

- Issue a communique to reemphasize the requirement to document search efforts: 06/30/2017
- Conduct training for Disclosure employees on search efforts and documentation requirements: 10/31/2017
- Conduct training for all agency FOIA Functional Coordinators FFCs to establishing the expectations for documenting Business Unit search efforts: 12/15/2017

RECOMMENDATION 5: Develop a consistent policy that requires Federal records associated with separated employees be searched as part of the IRS's responses to FOIA requests for records, and ensure it is followed by all business units.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The policy regarding separated employee records is already established and documented within the Records and Information Management (RIM) Internal Revenue Manual (IRM), which establishes agency policy surrounding search efforts associated with separated employees. We will establish a complementary process to address our FOIA obligations with respect to separated employees. We will update the formal FOIA search memo appropriately.

IMPLEMENTATION DATE: December 15, 2017

RESPONSIBLE OFFICIALS: Director, Privacy, Governmental Liaison and Disclosure (Director, Governmental Liaison, Disclosure and Safeguards)

CORRECTIVE ACTION MONITORING PLAN: The IRS will monitor implementation of the recommendation as part of the overall project plan established to ensure Federal records associated with separated employees are properly searched and documented.



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

Appendix VI

Office of Audit Comments on Management's Response

In response to our draft report, the Director, PGLD, agreed with our recommendations but stated that some of our findings were not accurate. We believe those statements warrant additional comment. We have included management's response and our related comments below.

Management's Response: *For the period under audit, the IRS followed NARA guidance which allows agencies to maintain official records in paper format while transitioning to an approved system for storing records in an electronic format. This context and timing is important because during the time period covered by this audit, IRS policies for maintaining official records were in full compliance with NARA regulations for a paper system transitioning to an electronic system. As such, we do not agree with your finding that IRS policies do not comply with the NARA guidelines in place during the time of this audit.*

The audit report refers to an IRS policy instructing employees to manually save emails to hard drives. While instructions do exist for saving emails to hard drives to mitigate lack of storage space, this process does not constitute an approved system for maintaining Federal records and is not IRS records policy. Rather, IRS policies require employees to print electronic records and place paper copies in official files. Contrary to the report, policies requiring employees to convert electronic records to paper format for filing helps, rather than hinders, maintaining official records if computer hard drives are damaged or destroyed.

Office of Audit Comment: The IRS misstated TIGTA's finding. TIGTA found that IRS record retention policies are not compliant with certain Federal requirements, specifically 36 C.F.R § 1236.10¹ stating that agencies must ensure that all electronic records are retrievable and usable for as long as needed. This requirement has been in place since 2009, which includes the entire audit period covered by our report. The IRS's ever-changing electronic media storage policies, and the IRS's reliance on employees to store electronic Federal records contained in e-mail on employee hard drives, negatively affected the IRS's ability to comply with Federal requirements.

In addition, while the IRS's print-and-file policy could have theoretically been compliant with separate NARA guidelines prior to December of 2016, NARA's review of the IRS's record retention practices in June 2015 found areas of noncompliance. Specifically, NARA found that the IRS's e-mail management practices and technologies do not secure

¹ 36 C.F.R. § 1236, *Electronic Records Management* (Oct. 2009).



*Electronic Record Retention Policies Do Not Consistently Ensure
That Records Are Retained and Produced When Requested*

all record e-mail against potential loss. Given this finding, the IRS's statement that it was in full compliance with NARA regulations is not factual.

Subsequent to December 31, 2016, the IRS has not been compliant with additional newly issued NARA guidelines. Specifically, in August of 2012, the Office of Management and Budget and NARA issued Memorandum M-12-18, *Managing Government Records Directive*. The directive required that, by December 31, 2016, Federal agencies must manage both permanent and temporary e-mails in an accessible electronic format. E-mail records must be retained in an appropriate electronic system with the capability to identify, retrieve, and retain the records for as long as they are needed. The IRS is in the process of implementing a new e-mail system with these capabilities, but the system has not been implemented. Due to the delay in implementation of the IRS's new e-mail system, it is not in compliance with the directive.

Finally, in its response, the IRS makes the statement that its print-and-file paper system helps, rather than hinders, Federal record preservation. TIGTA does not agree with that assessment. With tens of thousands of IRS employees creating potentially millions of Federal records via e-mail, reliance on employees to print and file each record is not a viable option and not one to which the IRS has adhered. During ongoing TIGTA audits of IRS operations, the IRS has been unable to locate paper case files containing documents we requested as part of our audits of Collection Due Process case files and Appeals International case processing. Specifically, in the review of Appeals' decisions on international cases, the IRS could not locate nine of 48 Appeals paper case files that were closed in FY 2015 and thus could not support Appeals actions in reducing millions of dollars in proposed assessments. In an annual review of IRS Collection Due Process cases, we found seven instances of case files from FY 2016 for which the IRS was unable to locate paper files that should have been stored at IRS campus locations. The loss of these paper cases is of significant concern due to IRS requirements to retain Federal records and illustrates TIGTA's concerns about the IRS's ability to preserve paper records.

Management Statement: *We are concerned about the finding that Freedom of Information Act (FOIA) cases did not document what records were searched. While we agree with your recommendation to ensure the policy for documenting search efforts were followed, in general we believe adequate searches took place to facilitate appropriate record production to FOIA requestors.*

Office of Audit Comment: TIGTA's findings of inadequate search efforts relate only to 30 closed FOIA cases reviewed and cannot be projected generally to all FOIA cases, which is stated in the report. However, we found that, for 20 of 30 closed cases reviewed, the IRS did not follow its own policies that require it to document which employees searched for responsive records and what criteria were used in the search. Case studies also found instances in which search efforts were not adequate. In



Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested

four cases, the PGLD caseworker did not follow up with a lead to identify other potential custodians. For two of the four cases, the PGLD caseworker closed the case with a 'No Records' response to the requestor, and in the third case, which was still open at the time we reviewed the file, the IRS was not aware that there was an additional custodian with responsive records until a meeting between TIGTA and IRS Chief Counsel staff working the case was held in November 2016, at which point the case had been open for over 400 days.

Lastly, in the fourth case, the PGLD office caseworker did not reach all the custodians who had responsive records because the caseworker did not send the request to all the functional contacts of the business unit identified in the incoming request. Instead, the request was sent only to the revenue agent named in the request. The case later went to litigation, and the judge found an inadequate search effort on the part of the IRS. Additional responsive records were found in other business units after one of the senior Chief Counsel attorneys reviewed the request and expanded the search effort. Given these examples, we maintain our finding that some responses to requests for records did not ensure that all records were searched and produced.