# TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

*Additional Efforts Are Needed to Ensure the Enterprise E-Mail Records Management Solution Meets All Requirements Before Deployment*

**August 7, 2017**

**Reference Number: 2017-20-039**

**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.

**ADDITIONAL EFFORTS ARE NEEDED TO ENSURE THE ENTERPRISE E-MAIL RECORDS MANAGEMENT SOLUTION MEETS ALL REQUIREMENTS BEFORE DEPLOYMENT**

# Highlights

### Final Report issued on August 7, 2017

Highlights of Reference Number: 2017-20-039 to the Internal Revenue Service Chief Information Officer and the Director, Privacy, Governmental Liaison and Disclosure.

## IMPACT ON TAXPAYERS

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 requires that agencies eliminate paper and use electronic recordkeeping to the fullest extent possible. Anticipated benefits include minimizing costs, operating more efficiently, improving documentation of agency actions and decisions, and transferring permanently valuable historical records to the NARA.

## WHY TIGTA DID THE AUDIT

The overall objective of this review was to evaluate the readiness of the IRS to establish the information technology capabilities to manage temporary and permanent e-mail records to comply with Memorandum M-12-18 by the December 31, 2016, deadline.

## WHAT TIGTA FOUND

In April 2016, the NARA issued the *Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18)* to provide clarification of the existing requirements that directly relate to e-mail management. The guidance provides questions to consider related to four e-mail management success criteria: policies, systems, access, and disposition.

According to TIGTA's evaluation of the IRS's project implementation status, 13 requirements (41 percent) related to the 32 individual questions associated with the four e-mail management success criteria remained under development at the time of the review. This included ensuring employee compliance with records management laws, regulations and policies; employee training; system storage and management issues; as well as access and retrieval issues. This is a significant number of requirements that still need to be fully developed and implemented before the IRS can successfully deploy its enterprise e-mail solution.

On September 30, 2016, the IRS reported to the NARA that it did not plan to fully deploy its enterprise e-mail solution until September 30, 2017, missing the mandated December 31, 2016, deadline by which Federal agencies must manage all e-mail records in an electronic format. Due to delays in developing and deploying the enterprise e-mail solution, the IRS will most likely not begin receiving any of the expected benefits of Federal records reform until the end of Calendar Year 2017, nearly a year after the initially mandated deployment date.

## WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS should ensure that the remaining e-mail management success criteria requirements are fully developed and implemented prior to or through deployment of its enterprise e-mail solution.

The IRS Chief Information Officer agreed to ensure that the requirements identified by the Chief Privacy Officer as fully meeting the NARA e-mail success criteria are implemented.

August 7, 2017

**MEMORANDUM FOR** CHIEF INFORMATION OFFICER
DIRECTOR, PRIVACY, GOVERNMENTAL LIAISON AND
DISCLOSURE

**FROM:**     Michael E. McKenney
        Deputy Inspector General for Audit

**SUBJECT:**    Final Audit Report – Additional Efforts Are Needed to Ensure the
        Enterprise E-Mail Records Management Solution Meets All
        Requirements Before Deployment (Audit # 201620015)

This report presents the results of our review to evaluate the readiness of the Internal Revenue
Service (IRS) to establish the information technology capabilities to manage temporary and
permanent e-mail records to comply with Memorandum M-12-18, *Managing Government
Records Directive*, by the December 31, 2016, deadline. This audit is included in our Fiscal
Year 2017 Annual Audit Plan and addresses the major management challenge of Achieving
Program Efficiencies and Cost Savings.

Management's complete response to the draft report is included as Appendix VII.

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

# *Table of Contents*

# *Abbreviations*

| | |
|---|---|
| C.F.R. | Code of Federal Regulations |
| EOps | Enterprise Operations |
| GAO | Government Accountability Office |
| IRM | Internal Revenue Manual |
| IRS | Internal Revenue Service |
| IT | Information Technology |
| NARA | National Archives and Records Administration |
| PGLD | Privacy, Governmental Liaison and Disclosure |
| PST | Personal Storage Table |
| TIGTA | Treasury Inspector General for Tax Administration |

# *Background*

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*.[1]  The Directive requires that Federal agencies eliminate paper and use electronic recordkeeping to the fullest extent possible.  The Directive is applicable to all executive agencies and to all Federal records, regardless of security classification or any other restriction.  The Directive stipulates 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 that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as they are needed.  Similarly, the Code of Federal Regulations (C.F.R.) requires Federal agencies to implement controls over Federal records in electronic information systems to ensure reliability, authenticity, integrity, usability, content, context, and structure.[2]  Further, the C.F.R. describes the following functionalities that are necessary for electronic recordkeeping:

> *By December 31, 2016, Federal agencies must manage both permanent and temporary e-mail records in an accessible electronic format.*

- 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 records 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

---

[1] See Appendix VI for a glossary of terms.
[2] 36 C.F.R. Section (§) 1236.10 (2011).

the migration of records and their associated metadata to new storage media or formats in order to avoid loss due to media decay or technology obsolescence.

- Execute disposition:  Identify and affect the transfer of permanent records to the NARA based on approved records schedules.  Identify and delete temporary records that are eligible for disposal.  Apply record holds or freezes on disposition.[3]

In April 2016, the NARA released *Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18)* to provide clarification of the existing requirements that directly relate to e-mail management and to summarize the statutory, regulatory, and NARA guidance.  Federal agencies should use this guidance internally to evaluate their progress in meeting the Directive's goals.  To have met the Directive's Calendar Year 2016 requirement of managing all e-mail electronically, each agency must have in place applicable records schedules, policies, and information technology systems to ensure that e-mail that are Federal records can be accessed, managed, and preserved until the appropriate disposition is applied.  The NARA categorized the e-mail management success criteria into the following four areas:  policies, systems, access, and disposition.

According to the NARA's April 2016 memorandum, "NARA has defined successful email management as having policies and systems in place to ensure that email records can be used, accessed, and have the appropriate disposition applied.  These success criteria reflect the complex challenges that agencies face in managing email.  NARA recognizes that agencies may be stronger in some aspects of email management than others.  Organizational complexity, schedule development, budgetary or procurement constraints may affect each agency's ability to meet specific criteria.  NARA also recognizes that managing email records effectively does not end on December 31, 2016.  For many agencies, full implementation of the success criteria for email management is an ongoing process that continues beyond this calendar year."

The mission of the Internal Revenue Service's (IRS) Office of Privacy, Governmental Liaison and Disclosure (PGLD) is to "preserve and enhance public confidence by advocating for the protection and proper use of identity information."[4]  Figure 1 shows the Office of PGLD organization chart as of August 2016.

---
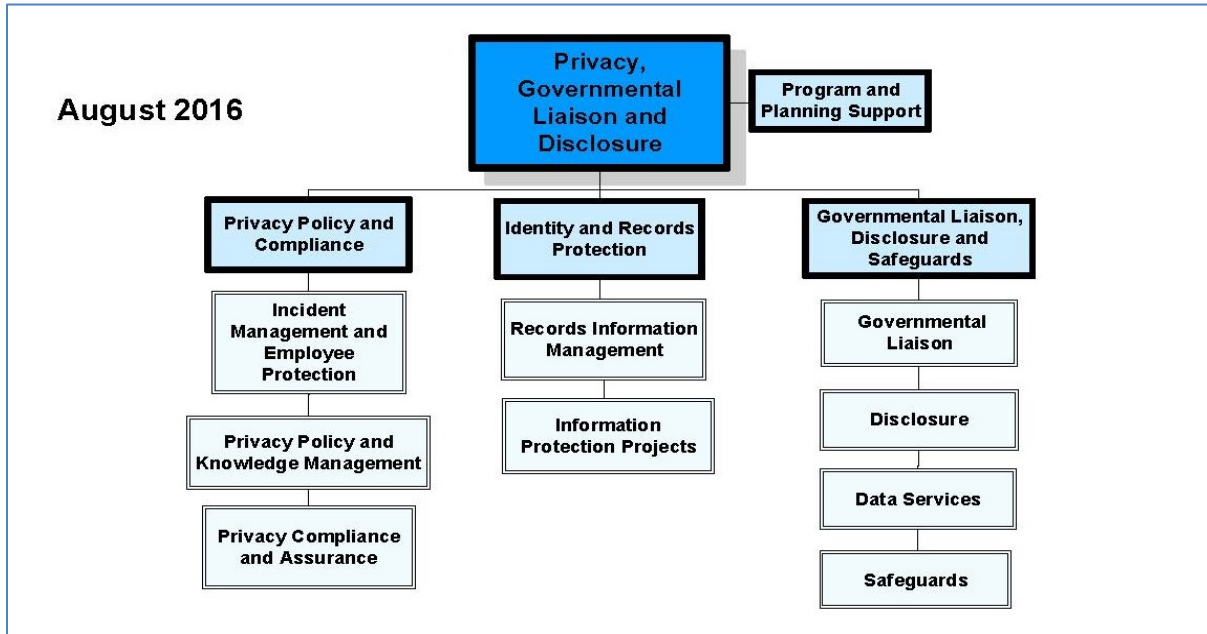
[3] 36 C.F.R. § 1236.20(b) (2011).
[4] Internal Revenue Manual 10.5.1.2, *Introduction to Privacy, Governmental Liaison and Disclosure (PGLD)* (June 2016).

**Figure 1: Office of PGLD Organization Chart**



Source: Office of PGLD management, August 2016.

The IRS created the Office of PGLD's Identity and Records Protection office in October 2014. This office is primarily responsible for developing records management policy and procedures and protecting taxpayer data through oversight of the Unauthorized Access and the Social Security Number Elimination and Reduction programs. Under the Identity and Records Protection office, the Records Information Management Program is responsible for ensuring that all IRS records are properly scheduled, archived, and disposed. This program supports the IRS mission by developing records policy and procedures; offering records management online resources; promoting information, guidance, and awareness of managing records; providing records management support to employees; supporting privacy, safeguards, and disclosure efforts by minimizing personally identifiable information and managing access; and assisting with records retention and disposition issues.

In November 2014, Office of PGLD management formed the Enterprise eRecords Management Team with approximately two dozen IRS stakeholders. The team was responsible for implementing Phase 1 of the e-mail records management initiative, which included identifying the needs of electronic records, policy gaps related to e-mail, and the management of unstructured data on IRS SharePoint sites. In June 2015, Office of PGLD management established the Enterprise Electronic Records Management Solution Project Management office to execute Phase 2 of the e-mail records management initiative. This office is developing best practices for actual eRecords solutions, user adoption, training, and updates to the Internal Revenue Manual (IRM) and other instructional material.

In addition, the IRS's Information Technology (IT) organization, working with the Enterprise Electronic Records Management Solution Project Management office, is involved in designing and implementing the e-mail records management solution. The IT organizations involved include Cybersecurity, Enterprise Operations (EOps), Enterprise Services, Strategy and Planning, and User and Network Services. These organizations provide support for architecture, design and implementation, security, and procurement to ensure that the information technology capabilities needed for the e-mail records management solution are in place. Further, within the EOps organization, the IRS established the Microsoft Initiatives Program office in February 2016. According to the IRS, its Microsoft Initiatives Program office has five initiatives, four of which support the electronic records management solution. Of these four, the Enterprise Exchange Upgrade Project directly relates to the IRS e-mail records management solution.

In July 2015, the IRS decided that the majority of its e-mail users would use the Microsoft Government Community Cloud and the remaining e-mail users in Criminal Investigation and the Office of Chief Counsel would use an on-premises e-mail solution. The IT organization initiated the Enterprise Exchange Upgrade Project with oversight from the IT Executive Oversight Team, consisting of management personnel from several IT organizations, including EOps, Enterprise Services, User and Network Support, and Cybersecurity.

By March 2016, the IRS had completed the cloud design and had appropriated funding for the cloud solution. Furthermore, the IRS had initiated requisitions for hardware, software, and additional contractor support. The Enterprise Exchange Upgrade Project was in Milestone One of the Enterprise Life Cycle when in March 2016, the IRS received a protest from the Government Accountability Office (GAO). A vendor, who is a leading reseller of Google products, filed a bid protest with the GAO against the IRS's decision to non-competitively select the Microsoft Corporation cloud-based e-mail as a service solution. The protestor requested that the GAO sustain their protest and grant remedies, which included requiring the IRS to abandon its sole source selection action, conduct a full and open competition, and award attorneys' fees and related protest costs. On June 14, 2016, the GAO sustained the protest and recommended that if the IRS had a requirement for a hybrid cloud-based solution, it should either acquire its needs competitively, or take the steps necessary to acquire its needs using other than competitive procedures.[5] The GAO also recommended that the IRS reimburse the protestor for the costs associated with filing and pursuing the protest. On January 5, 2017, the IRS paid the vendor $98,995 for reimbursement of protest related costs.

Subsequent to the vendor protest, the Treasury Inspector General for Tax Administration (TIGTA) reported significant issues with the IRS's procurement of its enterprise e-mail records management solution that would have severely affected its deployment.[6] Specifically, the IRS

---

[5] The IRS hybrid-cloud approach consisted of the majority of IRS e-mail in the Microsoft Government Community Cloud with the remaining e-mail managed on premises because the cloud does not meet enhanced requirements for Criminal Investigation and the Office of Chief Counsel.
[6] TIGTA, Ref. No. 2016-20-080, *Review of the Enterprise E-Mail System Acquisition* (Sep. 2016).

purchased subscriptions for an enterprise e-mail system that, as it turned out, it could not use. Because IRS executives made a management decision to consider the enterprise e-mail project an upgrade to existing software and not a new development project or program, the IT organization did not follow the IRM Enterprise Life Cycle guidance. The purchase was made without first determining project infrastructure needs, integration requirements, business requirements, security and portal bandwidth, and whether the subscriptions were technologically feasible on the IRS enterprise.

The IRS explained that in April 2016, the Chief Technology Officer, realizing the gravity of the situation and the IRS's commitments to Congress to implement the Office of Management and Budget and NARA Directive requirements by December 31, 2016, directed the IRS technical team to cease work on the cloud option and consider implementation of an on-premises e-mail upgrade strategy. According to the IRS, the on-premises solution required the IRS to identify, procure, install, and configure different hardware and software. As a result, the transition to an on-premises solution affected the Enterprise Exchange Upgrade Project planned deployment. The IRS considered these factors as well as technical dependencies in revising the Enterprise Exchange Upgrade Project deployment date to September 30, 2017. On September 27, 2016, IRS senior leadership signed a risk acceptance document acknowledging that it would not meet commitments made to Congress, the Department of Treasury, and the NARA, as well as recognizing the potential for increased scrutiny by Congress, taxpayers, oversight organizations, and other stakeholders as a result of this decision. In November 2016, the Infrastructure Executive Steering Committee approved the revised deployment date.

This review was performed in the IT organization at the New Carrollton Federal Building in Lanham, Maryland, during the period November 2015 through February 2017. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

# *Results of Review*

The current e-mail environment serving the majority of the IRS consists of 66 Microsoft Exchange 2010 servers.  Known weaknesses of the current e-mail environment configuration include aging hardware, aging software, limited ability to archive and store records, as well as limited mailbox sizes.  While the IRS has one e-mail solution for the enterprise, there are three different implementations, one for the majority of the IRS, one for the Office of Chief Counsel, and a third for Criminal Investigation.  The infrastructure hardware is beyond its useful life, relying on refurbished parts that are hard to procure and cannot take advantage of new software features.  Vendor software support for Exchange 2010 ended on January 13, 2015, while extended support ends on January 4, 2020.  Archiving e-mail records is dependent on end users' actions; due to limited storage and e-mail size restrictions, users have been creating Personal Storage Table (PST) files on their hard disks, thus creating a local storage file of their e-mail records.[7]  The current environment does not allow the IRS to uniformly implement retention policies Service-wide.

The IRS on-premises e-mail solution will be implemented enterprise-wide, including the majority of the IRS, the Office of Chief Counsel, and Criminal Investigation.  E-mail records will be stored on 126 new Exchange servers.  The solution will use three software products: Microsoft Exchange 2016 (server), Active Directory Federation Service (users and privileges), and Office 365 Pro Plus (client).  The Exchange 2016 upgrade will enhance mailbox sizes and provide an archiving solution that will enable the IRS to implement standardized record retention policies.  The IRS on-premises e-mail solution will be implemented at a total estimated cost of $47 million in Fiscal Year 2017 and $62.8 million in Fiscal Year 2018, which includes hardware, software, licenses, networks, contractors, travel, and overtime costs.  See Appendix IV for the enterprise e-mail solution timeline.

The results of our review have identified areas in which internal controls over the system development of the Enterprise Exchange Upgrade Project need to be strengthened.  A significant number of NARA e-mail management requirements under the four e-mail management success criteria categories remained under development at the time of our review.  On September 30, 2016, the IRS reported to the NARA that it did not plan to fully deploy its enterprise e-mail solution until September 30, 2017, missing the mandated December 31, 2016, deadline by which Federal agencies must manage all e-mail records in an electronic format.  According to the IRS, as of May 10, 2017, it is on target to meet the revised enterprise e-mail solution deployment date.

---

[7] A PST is an Outlook data file that stores messages and other items on a computer.

## More Effort Is Needed to Meet the National Archives and Records Administration's E-Mail Management Success Criteria Requirements Prior to the Deployment of the Enterprise E-Mail Solution

Recognizing the difficulty in using traditional records management methods on the large volumes of e-mail produced by the Federal Government, the NARA introduced the Capstone approach in August 2013 to provide Federal agencies the option of using a more simplified and automated approach to managing their e-mail. The approach manages e-mail categorization and scheduling based on the work or position of the e-mail account owners within the organization. To meet the requirements of the Directive, the IRS plans to implement the Capstone approach for about 190,000 mailboxes for three groups of users, including approximately 40 senior agency officials with permanent retention, approximately 200 senior managers with temporary retention of 15 years, and the remaining end users with temporary retention of seven years.[8] E-mail records subject to eDiscovery litigation holds are retained until the litigation holds are removed.[9] The benefits of the Capstone approach include that it:

- Increases the amount of e-mail with permanent value transferred to the NARA.

- Reduces the burden on individual end users.

- Reduces reliance on print-and-file practices.

- Allows for systematic destruction of temporary e-mail based on an approved NARA disposition authority.

To help implement the electronic recordkeeping functionalities in the C.F.R., the NARA issued the *Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18)* to provide clarification of the existing requirements that directly relate to the e-mail management success criteria.[10] The NARA defined successful e-mail management as having policies and systems in place to ensure that e-mail records can be used, accessed, and the appropriate disposition applied. The NARA also states in this guidance that it views the use of these "success criteria" as fundamental to successful electronic management of e-mail. The appendices of this guidance provide the following additional information on managing e-mail records.

- Appendix A, *Questions to Discuss on Email Management Success Criteria*, provides questions to consider related to specific requirements of the four e-mail management

---

[8] The 190,000 mailboxes consist of 80,000 inactive, 105,000 active, and 5,000 for the IRS's Criminal Investigation. These numbers include the three groups of users the IRS has identified under the Capstone approach, as well as group mail boxes.
[9] Electronic discovery, or eDiscovery for short, refers to the search, identification, collection, preservation, and processing of electronically stored information in the custody of the IRS. Typical sources of such information are Outlook mailboxes, removable media, workstations, databases, and home directories.
[10] 36 C.F.R. § 1236.20(b) (2011).

success criteria categories.  With the answers to these questions, agencies can assess their progress towards meeting the requirement of managing all e-mail in an electronic format.

- Appendix B, *Spreadsheet of Requirements for Email Management*, provides a compilation of records management requirements as they apply to e-mail records.  Each requirement includes the source statute, regulation, or NARA guidance.  The requirements are organized by the e-mail management success criteria and the parts of the records management life cycle.

To evaluate the IRS's progress in meeting the Directive's goals and to assess the overall readiness of the enterprise e-mail solution and related policies, the audit team developed a data collection instrument that incorporated the requirements of the 32 questions from Appendix A of the *Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18)* related to the four e-mail management success criteria categories.  The audit team held several meetings with IRS management to discuss the NARA provided success criteria and related requirements, as well as obtained further clarifying information.  The audit team recorded the IRS's responses, evaluated the clarifying information, and determined whether the specific criteria were in place or still under development.[11]  See Figure 2 for a summary of TIGTA's evaluation of the IRS's project implementation status that concludes:

- 17 "Yes" responses out of 32 (53 percent):  A "Yes" response indicates that the requirements of the NARA e-mail management success criteria are in place and are being accomplished through existing policy or with the current Exchange 2010 solution.

- 13 "Under Development" responses out of 32 (41 percent):  An "Under Development" response indicates that the IRS is developing related policy or developing the Exchange 2016 solution in order to meet the requirements of the NARA e-mail management success criteria.

- 2 "Not Applicable" responses out of 32 (6 percent):  A "Not Applicable" response indicates that the requirements of the NARA e-mail management success criteria are not relevant to the IRS's e-mail environment.

---

[11] See Appendix V for the implementation status of the e-mail management success criteria requirements as of January 31, 2017.

**Figure 2: IRS Implementation Status of the NARA E-Mail Management Success Criteria Requirements**

| NARA E-Mail Management Success Criteria Requirements Implementation Status as of January 31, 2017 | | | | | |
|---|---|---|---|---|---|
| Success Criteria Category | Yes | Under Development | No | Not Applicable | Total Questions |
| Policies | 8 | 2 | 0 | 1 | 11 |
| Systems | 3 | 6 | 0 | 1 | 10 |
| Access | 1 | 5 | 0 | 0 | 6 |
| Disposition | 5 | 0 | 0 | 0 | 5 |
| Total Responses | 17 | 13 | 0 | 2 | 32 |

*Source: TIGTA's evaluation of the IRS's status in implementing the e-mail management success criteria requirements as of January 31, 2017.*

Based on our evaluation of the IRS's implementation status, 13 requirements related to the 32 (41 percent) individual questions associated with the four e-mail management success criteria remained under development as of January 31, 2017. This is a significant number of requirements that still need to be fully developed and implemented before the IRS can successfully deploy its enterprise e-mail solution. Figure 3 shows the 13 requirements that were still under development at the time of our review.

**Figure 3: E-Mail Management Success Criteria Requirements Under Development**

| Question | Requirements Under Development as of January 31, 2017 |
|---|---|
| **Policies** | |
| P7 | Perform periodic audits to make sure employees comply with records management laws, regulations, and policies. |
| P10 | Train all IRS account holders on the requirement to copy or forward to official accounts Federal records that were created, received, or transmitted in personal or non-official e-mail accounts. |
| **Systems** | |
| S1 | Use system to store and manage e-mail messages. |
| S3 | Manage e-mail outside of the originating system in a dedicated records management system. |
| S4 | Maintain the content, context, and structure of the records. |
| S5 | Associate e-mail records with the creator, their role, and their agency. |
| S6 | Retain the components of e-mail messages including labels that identify each part of the header, the message content, and any attachments. |
| S9 | Migrate e-mail from one system to another, or to an e-mail archiving application to ensure consistent access. |
| **Access** | |
| A1 | Use, retrieve, and interpret e-mail records throughout the entire NARA-approved retention period. |
| A2 | Access e-mail from current and departed employees. |
| A3 | Use digital signatures or encryption technology for e-mail, where e-mail can be used and retrieved across the record life cycle. |
| A5 | Perform a federated search (the way that search tools combine keywords to find the best results) across multiple e-mail accounts or multiple systems to find e-mail needed for agency business. |
| A6 | Prevent unauthorized access, modification, or destruction of e-mail records. |

*Source: TIGTA's evaluation of the IRS's status in implementing the e-mail management success criteria requirements as of January 31, 2017.*

Due to delays in developing and deploying the enterprise e-mail solution, the IRS will most likely not begin receiving any of the expected benefits of Federal records reform until the end of Calendar Year 2017, nearly a year after the initially mandated deployment date. According to the Directive, these benefits include minimizing costs, operating more efficiently, improving documentation of agency actions and decisions, and transferring permanently valuable historical records to the NARA.

## Recommendation

**Recommendation 1:**  The Chief Information Officer, with support from the Director, Privacy, Governmental Liaison and Disclosure, should ensure that the remaining requirements associated with the NARA e-mail management success criteria are fully developed and implemented prior to or through deployment of the IRS's enterprise e-mail solution.

> **Management's Response:**  The IRS partially agreed with the recommendation in the draft report.  The IRS Chief Information Officer will ensure that the requirements identified by the Chief Privacy Officer as fully meeting the NARA email success criteria are implemented.  The IRS noted that some of the criteria cannot be met until deployment or migration.

> **Office of Audit Comment:**  TIGTA made a minor edit to the original recommendation in this report to clarify that some of the e-mail management success criteria requirements will not be met until deployment of the enterprise e-mail solution.

## Risk Management Roles and Responsibilities, Risk Identification, and Risk Mitigation Control Issues Raised During the Audit Were Addressed

Office of Management and Budget guidance governing all Federal agencies recommends that agencies consider information security, privacy, and records management for all resource planning and management activities throughout the Enterprise Life Cycle so that risks are appropriately managed.[12]

Although the Enterprise Exchange Upgrade Project manager reported that project risks were tracked within ProSight, the ProSight report we reviewed in June 2016 did not have any project risks identified.  The IRS's Enterprise Life Cycle guidance contains a *Risk Mitigation Planning and Execution Procedure*, dated October 2014, which is applicable to all IT organizations, contractors, and other stakeholders who manage, directly support, or provide oversight to projects that effect IRS business change.  The guidance provides the systematic instructions on how to implement the risk mitigation planning and execution process.  Activities include determining the mitigation approach, developing the mitigation plan, and estimating the cost of the mitigation including labor and materials.

Project risk mitigation was not sufficient for the Enterprise Exchange Upgrade Project.  A July 2016 *IT Executive Oversight Team Weekly Discussion Notes and Actions* included only two high-level risks.  However, risk mitigation actions were not well defined and did not include

---

[12] Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource* (July 2016).

detailed mitigation plans. In addition, accountable owners were not identified, due dates were not specified, and the cost of mitigation actions was not estimated.

Risk management controls concerning risk roles and responsibilities, risk identification, and risk mitigation were not sufficiently designed and implemented, which would have significantly affected the IRS's readiness to deploy any enterprise e-mail solution. Further, a Risk Management Plan had not been initially developed and approved by IT organization management for the Enterprise Exchange Upgrade Project. Specifically, IT management officials responsible for the design, development, and deployment of the enterprise e-mail solution had not fully complied with the Enterprise Life Cycle risk management guidance for identifying project risk roles and responsibilities, identifying project risks, and mitigating existing risks. Without improvement to its risk management program, the IRS could not ensure that it had a complete understanding of key risks to its enterprise e-mail solution and to what extent they could be mitigated.

**Management Action:** We initially raised these issues with IRS management on July 28, 2016. As of January 31, 2017, the IRS has implemented controls to define risk roles and responsibilities; identify risks and risk owners; and manage risk impact, probability of occurrence, criticality, and mitigation strategies for the Enterprise Exchange Upgrade Project.

# *Detailed Objective, Scope, and Methodology*

The overall objective of this review was to evaluate the readiness of the IRS to establish the information technology capabilities to manage temporary and permanent e-mail records to comply with the Memorandum M-12-18, *Managing Government Records Directive*, by the December 31, 2016, deadline.[1]  To accomplish this objective, we:

A.  Reviewed and evaluated whether the IRS's 2016 Enterprise Exchange Upgrade Project has implemented sufficient project oversight for its enterprise e-mail solution.

   1.  Analyzed meeting minutes that document decisions related to funding, staffing, development path, project status, management reporting, and risk management.

   2.  Evaluated the project's Risk Management Plan, risk monitoring activities, and the effectiveness of its risk mitigation efforts.

B.  Reviewed and evaluated whether the IRS's approach has ensured sufficient project management for the enterprise e-mail solution.

   1.  Evaluated the status of the IRS implementing the Capstone approach for senior officials and executives.

   2.  Evaluated the status of the IRS expanding the Capstone approach to all e-mail users.

   3.  Documented the project's key milestones and timeline.  We evaluated the reasonableness of the timeline planned for deploying the enterprise e-mail solution by the December 31, 2016 deadline.

C.  Reviewed and evaluated the IRS's progress in implementing the NARA's *Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18)*.

   1.  Developed a data collection instrument using the 32 questions in Appendix A of the *Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18)* for the four e-mail management success criteria (policies, systems, access, and disposition).

   2.  Interviewed IRS management, obtained clarifying information, reviewed and evaluated the status of the IRS responses.

---

[1] See Appendix VI for a glossary of terms.

### *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 objective: IRS policies and procedures for electronic records management, risk management, and project management. We evaluated these controls by: 1) interviewing IRS staff from the Office of PGLD, and the EOps and Enterprise Services organizations; 2) analyzing meeting minutes, risk reports, and project management documentation; and 3) assessing how the IRS plans to implement the Capstone approach to manage e-mail records.

**Additional Efforts Are Needed to Ensure the Enterprise E-Mail
Records Management Solution Meets All Requirements Before
Deployment**

Appendix II

# *Major Contributors to This Report*

Danny R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information
Technology Services)
Bryce Kisler, Director
Gwendolyn McGowan, Director
Carol Taylor, Audit Manager
Lynn Ross, Lead Auditor
Charlene Elliston, Senior Auditor
Wallace Sims, Senior Auditor
Allen Henry, Program Analyst

## *Report Distribution List*

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

# Enterprise E-Mail Solution Timeline

| Month/Year | Event |
|---|---|
| June 2015 | The IRS initiated a project to upgrade its enterprise e-mail system infrastructure and software to comply with Memorandum M-12-18, *Managing Government Records Directive*.[1] |
| July 2015 | The IT organization selected a hybrid e-mail solution that included the Microsoft Government Community Cloud for the majority of users and an on-premises e-mail solution for Criminal Investigation and the Office of Chief Counsel. |
| November 2015 | The IT organization formed the Microsoft Initiatives Program office within the EOps organization. |
| February 2016 | The Microsoft Initiatives Program office becomes operational. The Enterprise Exchange Upgrade Project is one of five initiatives managed by this office. |
| March 2016 | On March 7, 2016, a protest was filed with the GAO against the IRS decision to non-competitively select the Microsoft Corporation cloud-based e-mail as a service solution. The protestor requested that the GAO sustain this protest and grant remedies, which included the IRS abandoning its sole-source action, conducting a full and open competition, and awarding attorneys' fees and related protest costs. |
| April 2016 | In April 2016, the Chief Technology Officer directed the IRS technical team to cease work on the cloud option and consider implementation of an on-premises e-mail upgrade strategy.<br><br>On April 28, 2016, the IRS technical team confirmed Microsoft Exchange 2016 was the best solution to meet the requirements of Memorandum M-12-18. |

---

[1] See Appendix VI for a glossary of terms.

| | |
|---|---|
| June 2016 | On June 14, 2016, the GAO sustained the vendor's protest. |
| | On June 29, 2016, the Chief Technology Officer resigned from the IRS due to a lapse in a 1998 statute that allowed for a higher pay band for select positions at the tax agency.[2] |
| | On June 30, 2016, the Enterprise Exchange Upgrade Project timeline for the enterprise e-mail solution indicated the project would not meet the December 31, 2016, deadline. |
| July 2016 | On July 13, 2016, the IRS announced a new Chief Information Officer. |
| | On July 28, 2016, the Enterprise Exchange Upgrade Project met with the EOps Executive Steering Committee to request approval to exit Enterprise Life Cycle Milestone Zero. |
| September 2016 | Changing to an on-premises e-mail solution caused the Enterprise Exchange Upgrade Project to change the planned deployment date to September 30, 2017. |
| | As of September 30, 2016, the license/hardware/network equipment contracts for the Enterprise Exchange Upgrade Project were awarded. |
| November 2016 | As of November 4, 2016, the hardware and network equipment for the Enterprise Exchange Upgrade Project was received by the IRS. |
| | As of November 18, 2016, the rack/server build and setup was completed. |
| December 2016 | As of December 2, 2016, the Enterprise Exchange Upgrade Project test plan was completed. |
| January 2017 | As of January 11, 2017, the Enterprise Exchange Upgrade Project technical team was in the process of installing and configuring the Exchange application. |

*Source: IRS provided Enterprise E-mail Solution timeline documentation.*

---

[2] The IRS subsequently changed the title of the Chief Technology Officer to the Chief Information Officer.

# *Analysis of E-Mail Management Success Criteria Requirements*

To evaluate the IRS's progress in meeting the goals set forth in Memorandum M-12-18, *Managing Government Records Directive*, and to assess the overall readiness of the enterprise e-mail solution and related policies, the audit team developed a data collection instrument that incorporated the 32 questions from Appendix A of the *Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18)* related to the four e-mail management success criteria (policies, systems, access, and disposition).[1]  Conclusions were based on the implementation status of the e-mail management success criteria requirements as of January 31, 2017.

| # | E-Mail Management Success Criteria Requirement Related Questions | Implementation Status as of January 31, 2017 | IRS and TIGTA Comments |
|---|---|---|---|
| **POLICIES [P]** Agency-wide policies and training must inform all staff of their responsibilities for managing e-mail records.  Policies should be developed with all relevant stakeholders and should address the requirements of the Federal Records Act, 36 C.F.R. Chapter XII Subchapter B, and NARA guidance. | | | |
| P1 | Has the IRS developed, disseminated, and implemented an approved e-mail policy throughout the agency? | Yes | In December 2014, the IRS issued *Interim Records Retention Policy on E-mail for IRS Executives*.  The NARA approved a *Records Disposition Authority* for the IRS in October 2015, *e.g.*, where senior officials' e-mail will be retained permanently, managers' e-mail will be retained for 15 years, and end users' e-mail will be retained for 7 years. <br><br> The IRS has an enterprise-wide records management policy, IRM 1.15.6, *Records and Information Management, Managing Electronic Records* (November 2016) that covers the creation, maintenance, use, and disposition of Federal records created using IRS electronic information systems and personal computers, including e-mail. |

---

[1] See Appendix VI for a glossary of terms.

| | | | In November 2016, the IRS published updated guidance to supersede IRM 1.15.6.6, *Standards for Managing Electronic Mail Records*, that provides procedures for an account-based approach for managing IRS e-mail records. Under the account-based approach, the IRS manages e-mail records based on the role of the e-mail account user and/or office, rather than on the content of each e-mail record. The Exchange 2016 solution for records disposition will be automated based on a role-based approach. |
|---|---|---|---|
| P2 | Have the relevant IRS stakeholders been identified that are involved in the policy creation process? | Yes | The Office of PGLD's Records office is assigned the responsibility for policy creation. Policy creation involves the Office of Chief Counsel, the IT organization, and multiple IRS business unit representatives. The Governance Committee/Board Structure for the Enterprise Exchange Upgrade Project is comprised of the:<br><br>- IRS IT Executive Oversight Team.<br>- Technical Review Board.<br>- Associate Chief Information Officer Executive Steering Committee.<br>- IT/PGLD Executive Committee.<br>- Investment Management Change Control Board.<br>- Chief Technology Officer Monthly Briefing.<br>- EOps Executive Steering Committee Infrastructure Executive Steering Committee. |
| P3 | Does the IRS have an NARA-approved disposition schedule in place that applies to e-mail that are Federal records? | Yes | The IRS has a *Records Disposition Authority* that the NARA approved in October 2015. |
| P4 | Does the enterprise e-mail solution provide for policies and procedures to access e-mail in response to information requests? | Yes | Policies and procedures to access e-mail in response to information requests exists within the IRS IT Enterprise Services organization's eDiscovery Program.<br><br>**TIGTA Comments:** The IRS's *High Level Requirements for eRecords* document, dated July 1, 2015, includes requirements for searching that:<br><br>- The user, creator, or system must be able to label and categorize the record so that it can be: |

| | | | - Associated with an approved retention schedule. |
| | | | - Searched by key criteria, such as creator/owner, date, title, subject matter, and purpose. |
| | | | - Available for eDiscovery or Freedom of Information Act searches. |
| P5 | Does the enterprise solution provide policies and procedures to protect against unintended loss of e-mail records? | Yes | The Office of PGLD issued guidance on separating employee clearance, and was included in the September 2016 updates to IRM 1.15.5, *Records and Information Management, Relocating/Removing Records*. |
| P6 | Does the IRS perform periodic reviews of records management policies with all relevant stakeholders? | Yes | The Office of PGLD collaborated with stakeholders including the IT organization, Office of Chief Counsel, Agency-Wide Shared Services, and Human Capital Office to develop the electronic messaging and separating employee clearance policies. |
| P7 | Does the IRS perform periodic audits to make sure employees comply with records management laws, regulations, and policies? | Under Development | The Office of PGLD conducts periodic reviews of records management policies that it includes in the annual self-assessments that are sent to the NARA. The IRS has an annual review process that occurs between the PGLD Records Specialists and the Information Resource Coordinators in the IRS business units. Annually, the Records Specialists conduct inventories of records and provide training on records management policies. **TIGTA Comments:** The IRS provided the Draft *Standard Operating Procedure for Conducting Records Program Reviews*. We reviewed the records reviews completed at the end of September 2016. These documents did not validate that the IRS performed periodic reviews of records management policies with <u>all</u> relevant stakeholders. As a result, further actions may be needed after the e-mail management solution is implemented in Fiscal Year 2017. |
| P8 | Does the IRS have the policies, technological means, and procedures to place legal holds on e-mail records or accounts? | Yes | Policies exist to place legal holds on e-mail records or accounts. IRM 34.7.1.1.4.3.1, *Litigation Hold Procedures* (February 2016), contains guidance for litigation holds on e-mail. **TIGTA Comments:** IRM 34.7.1.1.4.3.1 contains guidance for litigation holds on e-mail. The IRS's *High Level Requirements for eRecords* document, dated July 1, 2015, includes requirements for declaring, capturing, and organizing that: |

| | | | - The user, creator, or system must be able to label and categorize the record so that it can be:<br><br>- Associated with an approved retention schedule.<br><br>- Searched by key criteria, such as creator/owner, date, title, subject matter, and purpose.<br><br>- Available for eDiscovery or Freedom of Information Act searches.<br><br>The system must allow designation of records for litigation or other administrative holds. |
|---|---|---|---|
| P9 | Does the IRS have policies in place regarding the use of personal or non-official e-mail accounts? | Yes | On June 21, 2016, the Office of PGLD issued an Emergency Interim Guidance memorandum, *Using IRS and Personal E-mail Accounts*. The memorandum included links to IRM 10.5.1, *Privacy and Information Protection, Privacy Policy* (June 2016). |
| P10 | Have you trained all IRS account holders on the requirement to copy or forward to official accounts, any Federal records created, received, or transmitted in personal or non-official e-mail accounts? | Under Development | The IRS has developed records management mandatory training. Employees generally had until September 30, 2016, to complete the mandatory training. However, as of January 31, 2017, the last group of employees still needed to complete this training. |
| P11 | Does the IRS comply with the requirements for managing security classified information in e-mail accounts and systems? | Not Applicable | The IRS does not use or have classified information. |

**SYSTEMS [S]** Agencies must have systems in place that can produce, manage, and preserve e-mail records in an acceptable electronic format until disposition. Additionally, systems must support the implementation of agency policies and provide access to e-mail records throughout their life cycle.

| | | | |
|---|---|---|---|
| S1 | What systems does the enterprise e-mail solution use to store and manage e-mail messages? | Under Development | The current system is Exchange 2010, which does not meet the NARA Capstone requirements.<br><br>The future system is Exchange 2016, which will implement e-mail archiving that complies with the NARA Capstone requirements. E-mail will be stored on the Enterprise Exchange Upgrade Project servers. |
| S2 | Have responsibilities been assigned for the enterprise solution systems that | Yes | The EOps organization manages day-to-day e-mail operations and access to e-mail. End users are able to request and receive permission to use e-mail |

| | | | |
|---|---|---|---|
| | manage e-mail, how e-mail is accessed, and how disposition is carried out? | | services.  For eDiscovery requests, the Office of Chief Counsel submits access requests to the EOps organization to retrieve end users' e-mail, as needed.  The Exchange 2010 solution uses audit logs.  The Exchange 2016 solution will use audit logs and rights management.  |
| | | | The EOps organization also manages e-mail disposition.  The Exchange 2010 solution to manage disposition of e-mail is manual and performed by end users.  The Exchange 2016 solution to manage disposition of e-mail will be automated based on role-based grouping, *e.g.*, senior officials' e-mail will be retained permanently, managers' e-mail will be retained for 15 years, and end user' e-mail will be retained for seven years. |
| S3 | Does the IRS manage e-mail outside of the originating system in a dedicated records management system? | Under Development | The NARA defines an electronic recordkeeping system as an electronic information system that meets an agency's recordkeeping needs.  At a high level, the NARA has defined an electronic recordkeeping system as an electronic information system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition (36 C.F.R. § 1236.20).  |
| | | | The IRS stated that e-mail will be managed within the Exchange 2016 originating system, which is a dedicated records management system that will satisfy the requirements of 36 C.F.R. § 1236.  |
| | | | **TIGTA Comments:**  The IRS's *High Level Requirements for eRecords* document, dated July 1, 2015, includes requirements that agencies must not use an electronic mail system to store the recordkeeping copy of electronic mail messages identified as Federal records unless that system has all of the features specified in 36 C.F.R. § 1236.20. |
| S4 | Does the enterprise e-mail solution maintain the content, context, and structure of the records? | Under Development | The Exchange 2016 solution will maintain the content, context, and structure of the records.  |
| | | | **TIGTA Comments:**  The IRS's *High Level Requirements for eRecords* document, dated July 1, 2015, includes requirements that:  |
| | | | - The names of senders, all addressee(s), and the date the message was sent must be preserved for each electronic mail record, in order for the context of the message to be understood. |

| | | | |
|---|---|---|---|
| | | | - Attachments to electronic mail messages that are an integral part of the record must be preserved as part of the electronic mail record.<br><br>Some e-mail systems provide calendars and task lists for users, which may meet the definition of a Federal record and should be managed accordingly. |
| S5 | Can the enterprise e-mail solution associate e-mail records with the creator, their role, and their agency? | Under Development | The Exchange 2016 e-mail solution will associate e-mail records with the creator, their role, and their agency.<br><br>**TIGTA Comments:** The IRS's *High Level Requirements for eRecords* document, dated July 1, 2015, includes requirements regarding declaring, capturing, and organizing that:<br><br>- The user, creator, or system must be able to identify and file the record copy within the electronic environment.<br>- The user, creator, or system must be able to label and categorize the record so that it can be:<br>  - Associated with an approved retention schedule.<br>  - Searched by key criteria, such as creator/owner, date, title, subject matter, and purpose.<br>  - Available for eDiscovery or Freedom of Information Act searches. |
| S6 | Does the enterprise e-mail solution retain the components of e-mail messages including labels that identify each part of the header, the message content, and any attachments? | Under Development | The Exchange 2016 e-mail solution will retain the components of e-mail messages including labels that identify each part of the header, the message content, and any attachments.<br><br>**TIGTA Comments:** The IRS's *High Level Requirements for eRecords* document, dated July 1, 2015, includes requirements for components that:<br><br>- The names of the sender, addressee(s), and date must be preserved for each e-mail record in order for the context of the message to be understood.<br>- Attachments to e-mail messages that are an integral part of the record must be preserved.<br><br>Some e-mail systems provide calendars and task lists for users, which may meet the definition of a Federal record and should be managed accordingly. |
| S7 | Are departing employees' e-mail records preserved in accordance with | Yes | The Exchange 2010 solution involves a manual retention process. The EOps organization referred to a recently developed *Separating Employee Checklist* |

|  |  |  | that shows how records are captured for departing employees.<br><br>The Exchange 2016 solution will be an automated retention process, where e-mail records will be kept in accordance with the disposition schedule, including e-mail for separated employees. The Exchange 2016 solution for disposition will be automated based on role-based grouping, *e.g.*, senior officials' e-mail will be retained permanently, managers' e-mail will be retained for 15 years, and end users' e-mail will be retained for seven years. |
| S8 | Can the enterprise e-mail solution provide the full names of the sender and addressee(s) with the transfer-level documentation?[2] | Yes | The IRS does not use nicknames for e-mail. The full header information is transferred to the NARA with the e-mail message. |
| S9 | With the enterprise e-mail solution, can e-mail be migrated from one system to another, or to an e-mail archiving application, to ensure consistent access?[3] | Under Development | The IRS is not using an external archiving system. The IRS does not have enough storage capability to use the archiving features of Exchange 2010.<br><br>The IRS will migrate to Exchange 2016 using the Exchange Migration Wizard tool. This process will discover PST files, which will be moved to Exchange 2016. The IRS does not expect any data loss to occur during the migration as headers, metadata, and attachments will be migrated. There are logs that will show what was migrated and where it was migrated. There is no requirement to upgrade Outlook. |
| S10 | Does the IRS use e-mail systems to transmit classified information? | Not Applicable | The IRS does not use or have classified information. |

**ACCESS [A]** E-mail records must remain usable and retrievable throughout their life cycle. Access supports an agency's ability to carry out its business functions. Access should address internal agency needs and accommodate responses to requests for information.

---

[2] What agencies must provide to the NARA when transferring permanent records to the archives, in addition to the records themselves, includes descriptions, indices, or metadata to be included with the permanent records.
[3] Ensuring that the electronic record is available to whoever needs it, whenever it is needed, in the same manner as originally intended.

| A1 | Can the IRS use, retrieve, and interpret e-mail records throughout the entire NARA-approved retention period?[4] | Under Development | The existing Exchange 2010 solution cannot perform this function. |
|---|---|---|---|
| | | | The Exchange 2016 solution will have this functionality. The IRS stated that the full name details for e-mail transferred to the NARA are contained within the metadata. |
| | | | **TIGTA Comments:** The IRS's *High Level Requirements for eRecords* document, dated July 1, 2015, includes requirements for searching that: |
| | | |   - The user, creator, or system must be able to label and categorize the record so that it can be: |
| | | |     - Associated with an approved retention schedule. |
| | | |     - Searched by key criteria, such as creator/owner, date, title, subject matter, and purpose. |
| | | |     - Available for eDiscovery or Freedom of Information Act searches. |
| | | | The system should possess extensive search functionality, which is capable of crawling and indexing mailbox databases for multiple mailbox searches when eDiscovery requests are received, including the ability to search across encrypted e-mail. |
| A2 | Is the IRS able to access e-mail from current and departed employees? | Under Development | The Exchange 2010 solution involves a manual retention process. EOps organization officials referred to a recently developed *Separating Employee Checklist* that shows how records are captured for departing employees. |
| | | | The Exchange 2016 solution will be an automated retention process, where e-mail records will be kept in accordance with the disposition schedule, including e-mail for separated employees. The Exchange 2016 solution for disposition will be automated based on role-based grouping, *e.g.*, senior officials' e-mail will be retained permanently, managers' e-mail will be retained for 15 years, and end users' e-mail will be retained for seven years. |
| A3 | If the enterprise e-mail solution uses digital signature or encryption technology, is e-mail usable | Under Development | Enterprise Services organization officials stated that the eDiscovery policy requires e-mail to be encrypted using Microsoft encryption. |

---

[4] To help understand in order to use the information.

| | | | |
|---|---|---|---|
| | and retrievable across the life cycle? | | **TIGTA Comments:** The IRS's *High Level Requirements for eRecords* document, dated July 1, 2015, includes a requirement for searching that:<br><br>- The system should possess extensive search functionality, which is capable of crawling and indexing mailbox databases for multiple mailbox searches when eDiscovery requests are received, including the ability to search across encrypted e-mail.<br><br>The IRS's *Vision/Scope Document for Exchange Server 2016 Upgrade* document, dated May 23, 2016, includes a requirement that includes the capability to support basic search terms and decrypt e-mail. |
| A4 | If the enterprise e-mail solution is stored on local or removable media, can e-mail be retrieved and searched when responding to an information request? | Yes | The Enterprise Services organization's eDiscovery Program has a procedure, *IT eDiscovery Workflow Procedure*, dated August 19, 2016, concerning local or removable media.<br><br>The Exchange 2010 solution requires the IRS to identify whether the employee has a local or removable media source, and if so, the EOps organization collects and retains the removable media.<br><br>The Exchange 2016 solution will implement archiving and store e-mail on the Enterprise Exchange Upgrade Project servers; removable media will no longer be used. |
| A5 | Is the enterprise e-mail solution able to perform a federated search?[5] | Under Development | The Office of PGLD stated a federated search is not required by the C.F.R. or the NARA, but it is a capability that the IRS will have in the future with the Exchange 2016 solution.<br><br>**TIGTA Comments:** The IRS's *High Level Requirements for eRecords* document, dated July 1, 2015, includes requirements for searching that:<br><br>- The user, creator, or system must be able to label and categorize the record so that it can be:<br>  - Associated with an approved retention schedule.<br>  - Searched by key criteria, such as creator/owner, date, title, subject matter, and purpose. |

---

[5] The way search tools combine keywords to find the best results across multiple e-mail accounts or multiple systems to find e-mail needed for agency business.

| | | | |
|---|---|---|---|
| | | | - Available for eDiscovery or Freedom of Information Act searches.<br><br>The system should possess extensive search functionality, which is capable of crawling and indexing mailbox databases for multiple mailbox searches when eDiscovery requests are received, including the ability to search across encrypted e-mail. |
| A6 | Can the enterprise e-mail solution prevent unauthorized access, modification, or destruction of e-mail records? | Under Development | The Exchange 2016 solution will have this capability through the use of audit logs and rights management.<br><br>The IRS's *High Level Requirements for eRecords* document, dated July 1, 2015, includes requirements for preserving, maintaining security, and managing access that:<br><br>- 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.<br><br>- Ensure that all records in the system are retrievable and usable for as long as needed to conduct agency business.<br><br>- Develop procedures to migrate records and related metadata to stable storage media and sustainable formats on a periodic basis in accordance with record cut-offs. |

**DISPOSITION [D]** The IRS must have a NARA-approved schedule in place to be able to carry out the disposition of permanent and temporary e-mail records using either agency-specific schedules or the *General Records Schedule: E-mail Managed Under a Capstone Approach.*

| | | | |
|---|---|---|---|
| D1 | Does the IRS have NARA-approved disposition schedules in place that identify the systems where Federal e-mail records are held? | Yes | The IRS has a *Records Disposition Authority* that the NARA approved in October 2015. |
| D2 | Has the IRS analyzed existing disposition schedules to determine if they apply to e-mail records? Has the IRS identified gaps in the disposition schedules? | Yes | The IRS has a *Records Disposition Authority* that the NARA approved in October 2015 that addressed the identified gaps. |

| D3 | Has the IRS established procedures to associate e-mail records with projects or case files? | Yes | IRM 1.15.6, *Records and Information Management, Managing Electronic Records* establishes policy regarding the creation, maintenance, retention, and disposition of electronic records, including e-mail. Additional guidance to further clarify expectations is found in IRM 1.15.6.6.1(2) d, *IRS Account-based Approach Explained* (November 2016). The guidance requires that e-mail records be manually retained with related records, *i.e.*, when business needs require e-mail records to be retained with other records, such as part of a case file, the end user should forward or copy these e-mail records to the appropriate recordkeeping system (SharePoint site, file share, or paper file). The records are subsequently maintained according to the *Records Disposition Authority.* |
| --- | --- | --- | --- |
| D4 | Has the IRS developed training to inform employees of their responsibilities for managing records in e-mail accounts in accordance with approved disposition authorities? | Yes | The IRS has developed records management mandatory training. Employees generally had until September 30, 2016, to complete the mandatory training. However, as of January 31, 2017, the last group of employees still needed to complete this training. |
| D5 | Is the IRS transferring permanent e-mail records to the NARA in accordance with approved records schedules and applicable laws, regulations, and NARA transfer guidance? | Yes | Record transfers are occurring in accordance with the *Records Disposition Authority* instructions. |

*Additional Efforts Are Needed to Ensure the Enterprise E-Mail Records Management Solution Meets All Requirements Before Deployment*

**Appendix VI**

# *Glossary of Terms*

| Term | Definition |
|------|-----------|
| **Active Directory Federation Service** | A standards-based service that allows the secure sharing of identity information between trusted business partners (known as a federation) across an extranet. |
| **Chief Information Officer (formerly Chief Technology Officer)** | Leads the IT organization and advises the IRS Commissioner about information technology matters, manages all IRS information system resources, and is responsible for delivering and maintaining modernized information systems throughout the IRS. |
| **Client** | The client part of a client-server architecture.  Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. |
| **Data Collection Instrument** | A questionnaire used by the audit team to capture IRS responses for analysis. |
| **Enterprise Life Cycle** | Establishes a set of repeatable processes and a system of reviews, checkpoints, and milestones that reduce the risks of system development and ensure alignment with the overall business strategy. |
| **Enterprise Operations Organization** | The IT organization that provides server and mainframe computing services for IRS business entities and taxpayers. |
| **Executive Steering Committee** | A committee with oversight responsibilities for investments, including validating major investment business requirements and ensuring enabling technologies are defined, developed, and implemented. |
| **Extranet** | An intranet that can be partially accessed by authorized outside users, enabling businesses to exchange information over the Internet securely. |
| **Federal Record** | All recorded information, regardless of physical form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business, including information created, manipulated, communicated, or stored in digital or electronic form. |

| Term | Definition |
|---|---|
| **Government Accountability Office** | An independent, nonpartisan agency that works for Congress that investigates how the Federal Government spends taxpayer dollars. |
| **Information Technology** | Includes computers, ancillary equipment, software, firmware, services, and related resources. |
| **Infrastructure** | The hardware, software, and network resources and services required for the existence, operation, and management of an enterprise information technology environment. It allows an organization to deliver information technology solutions and services to its employees, partners, and customers and is usually internal to an organization and deployed within owned facilities. |
| **Internal Revenue Manual** | The IRS's primary source of instructions to its employees relating to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities. |
| **Metadata** | The elements of information that answer the questions "who, what, where, when, and why" regarding electronic records. Metadata elements provide administrative, descriptive, and technical information that describe the structure and content of electronic records. |
| **Microsoft Exchange** | Microsoft server software that enables the sending and receiving of e-mail and is designed to interoperate with an end user client software application such as Microsoft Outlook. |
| **Microsoft Government Community Cloud** | Uses Microsoft Office 365 Software as a service solution that includes Microsoft Office, e-mail, and collaboration software from Microsoft's Cloud Server. Microsoft Office 365 provides desktop functionalities and is available by subscription. |
| **Milestones** | A phase of system development with a scheduled milestone exit review process where management must decide to go or not to go to the next development phase. |
| **National Archives and Records Administration** | Federal agency that provides public access to Federal Government records. |
| **Office of Management and Budget** | Federal agency that oversees the preparation and administration of the Federal budget and coordinates Federal procurement, financial management, information, and regulatory policies. |

| Term | Definition |
|---|---|
| **Office of Privacy, Governmental Liaison and Disclosure** | The IRS organization that advocates for the protection and proper use of identity information, consisting of four offices: Privacy Policy and Compliance; Identity and Records Protection; Governmental Liaison, Disclosure, and Safeguards; and Program and Planning Support. |
| **Project** | A group of tasks to accomplish a specific objective, with a beginning and ending date that is planned, monitored, and measured; follows a life cycle process; and results in deliverables or end products. |
| **ProSight** | A database tool designed with specific tracking, reporting, and decision-making features used to monitor projects. |
| **Risk** | An uncertain event or condition that, if it occurs, has a negative effect on the project. |
| **Server** | A computer that carries out specific functions (*e.g.*, a file server stores files, a print server manages printers, and a network server stores and manages network traffic). |
| **Stakeholders** | A group of individuals that is affected by, or in some way is accountable for, the outcome and undertaking. Stakeholders may include project members, suppliers, customers, end users, and others. |
| **System** | A set of interdependent components that perform a specific function and are operational. Information technology systems may also include software, hardware, and processes. |

# Management's Response to the Draft Report

**DEPARTMENT OF THE TREASURY**
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CHIEF INFORMATION OFFICER

JUN 2 9 2017

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM:           S. Gina Garza
                Chief Information Officer

SUBJECT:        Draft Audit Report – Additional Efforts Are Needed to Ensure the
                Enterprise E-Mail Records Management Solution Meets All
                Requirements Before Deployment (Audit # 201620015)

Thank you for the opportunity to review your draft audit report. We appreciate the positive response by your team to IRS comments during the course of the audit. We also appreciate the acknowledgement that IRS now has controls in place to manage risks for the Enterprise Exchange Upgrade (EEU) project.

The IRS is committed to meeting the Office of Management and Budget (OMB) Managing Government Records Directive (M-12-18) as well as the National Archive and Records Administration (NARA) goals and criteria. The IRS has put forth substantial effort to ensure the IRS On-Premise E-mail Records Management solution complies with NARA e-mail management criteria.

As noted in the audit, there are three distinct email domains in the IRS: IRS Main, Chief Counsel and Criminal Investigations. The separate smaller domains of Chief Counsel and Criminal Investigation are already conducting email archiving and retention. For the IRS Main domain to achieve OMB M-12-18, IRS has established and configured Exchange 2016 to meet the success criteria.

Since the time of the audit, IRS has made great progress; We successfully completed approximately 35% of the activities needed to become compliant. IRS anticipates we will meet our revised baseline schedule to migrate all IRS Main Domain users by September 30, 2017.

Additionally, we are pleased to report that NARA recently assessed our success criteria toward full compliance with the Managing Government Records Directive (M-12-18) and has rated the IRS at a "low risk of not managing e-mail effectively." Per your audit report, TIGTA concluded that IRS has addressed 19 of the requirements associated with the NARA success criteria, and the remaining 13 requirements needing to be fully developed and implemented 'prior to deployment' of the IRS's enterprise e-mail solution. IRS contends that the remaining 13 will be met prior to or upon deployment of our solution.

In NARA's April 2016 Criteria for Managing E-mail Records in Compliance with the Managing Government Records Directive (M-12-18), NARA acknowledges the challenges agencies face and recognizes effective management of e-mail records is an ongoing process. The IRS is now doing an assessment on all three (3) domains to ensure and confirm we will be compliant. Barring any unforeseen complications, including any from those assessments, IRS will have a fully configured and implemented solution addressing all NARA success criteria.

In closing, we want to stress that IRS remains committed to meeting our September 30, 2017 deadline to be NARA compliant. We continue to value TIGTA's insight, support and guidance in these efforts. If you have any questions, please contact me at (202) 317-5000 or Debra Fairweather, IT Program Oversight Coordination, at (202) 317-6458.

Attachment

Attachment

Draft Audit Report – Additional Efforts Are Needed to Ensure the Enterprise E-Mail Records Management Solution Meets All Requirements Before Deployment (Audit # 201620015)

**RECOMMENDATION 1**
The Chief Information Officer, with support from the Director, Privacy, Governmental Liaison and Disclosure, should ensure that the remaining requirements associated with the NARA e-mail management success criteria are fully developed and implemented prior to deployment of the IRS's enterprise e-mail solution.

**CORRECTIVE ACTION:**   The IRS partially agrees with TIGTA's recommendation. The Chief Information Officer (CIO) will ensure the requirements identified by the Chief Privacy Officer as fully meeting the NARA email success criteria are implemented. Please also note, the IRS gives exception to the phrase "prior to deployment" because some of the criteria are met upon deployment or migration.

**IMPLEMENTATION DATE:** December 30, 2017

**RESPONSIBLE OFFICIAL(S):** Associate Chief Information Officer, Enterprise Operations

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.