



*Improvements Are Needed to
Ensure the Effectiveness of the
Privacy Impact Assessment Process*

February 27, 2013

Reference Number: 2013-20-023

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.



HIGHLIGHTS

IMPROVEMENTS ARE NEEDED TO ENSURE THE EFFECTIVENESS OF THE PRIVACY IMPACT ASSESSMENT PROCESS

Highlights

Final Report issued on February 27, 2013

Highlights of Reference Number: 2013-20-023 to the Internal Revenue Service Director, Privacy, Governmental Liaison, and Disclosure.

IMPACT ON TAXPAYERS

The Privacy Impact Assessment (PIA) process examines the risks and ramifications of using information technology to collect, maintain, and disseminate information in identifiable form about members of the public and agency employees. The IRS recognizes that privacy protection is both a personal and fundamental right of all taxpayers and employees.

WHY TIGTA DID THE AUDIT

This audit was initiated at the request of the IRS to evaluate its implementation of the privacy provisions of the E-Government Act of 2002, which requires agencies to conduct PIAs. In addition, the Consolidated Appropriations Act of 2005, Section 522, requires the Inspector General of each agency to evaluate privacy and data protection procedures. This review was part of our statutory requirements to annually review the adequacy and security of IRS technology and addresses the major management challenge of Security for Taxpayer Data and Employees.

WHAT TIGTA FOUND

The IRS has not established effective processes to ensure that the PIAs are completed timely, updated, and made publicly available and that privacy policies are posted on public websites for all required systems and collections of information. Further, in December 2011, the IRS implemented the Privacy Impact Assessment Management System (PIAMS) to automate the process of completing PIAs in a

more efficient and less time-consuming way. However, several key processes were not effectively automated. For example, privacy analysts must view numerous individual screens rather than scrolling through the information seamlessly, responses in the system are not grouped by topic or subject matter, and the automated e-mail notification function is not consistent.

WHAT TIGTA RECOMMENDED

TIGTA made 11 recommendations to the Director, Privacy, Governmental Liaison, and Disclosure, that included the following: 1) establish an annual reconciliation of PIA inventories with information systems and collections of information in the current production environment; 2) document and publicize the customer survey PIA completion process; 3) establish a PIA inventory control process to identify and review systems every three years as required; 4) automate the notification process to alert responsible officials when new or existing PIAs are required to be posted to the IRS public website; and 5) ensure that current and complete standard operating procedures are established and maintained for all PIA processes. TIGTA also recommended that IRS officials who develop third-party website information be directed to submit website proposal details and approval requests to the IRS New Media Governance Council and coordinate with website owners to post a link to the IRS privacy policy on these third-party websites.

The IRS agreed with nine of the recommendations but indicated that it had already implemented two recommendations by overhauling the PIAMS template and involving privacy analysts and other users in requirements gathering and testing of PIAMS functionality. TIGTA did not see evidence of these corrective actions and continues to believe that the PIAMS version, at the time of our review, could be improved to effectively automate the key privacy impact assessment processes.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

February 27, 2013

MEMORANDUM FOR DIRECTOR, PRIVACY, GOVERNMENTAL LIAISON, AND
DISCLOSURE

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

SUBJECT: Final Audit Report – Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process
(Audit # 201220009)

This report presents the results of our review of the Internal Revenue Service's (IRS) implementation of the privacy provisions of the E-Government Act of 2002.¹ This review was included in the Treasury Inspector General for Tax Administration's Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. The IRS requested we conduct this review.

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

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 or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services).

¹ Pub. L. No. 107-347, § 208, 116 Stat. 2899 (2002).



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Table of Contents

| | |
|---|---------|
| Background | Page 1 |
| Results of Review | Page 3 |
| Improvements Are Needed to Fully Address the Privacy Provisions of the E-Government Act of 2002..... | Page 3 |
| <u>Recommendations 1 and 2:</u> | Page 7 |
| <u>Recommendations 3 through 6:</u> | Page 8 |
| <u>Recommendations 7 and 8:</u> | Page 10 |
| <u>Recommendation 9:</u> | Page 11 |
| The Privacy Impact Assessment Management System Does Not Effectively Automate Key Privacy Impact Assessment Processes | Page 12 |
| <u>Recommendation 10:</u> | Page 13 |
| <u>Recommendation 11:</u> | Page 14 |
| | |
| Appendices | |
| Appendix I – Detailed Objective, Scope, and Methodology | Page 15 |
| Appendix II – Major Contributors to This Report | Page 18 |
| Appendix III – Report Distribution List | Page 19 |
| Appendix IV – Glossary of Terms..... | Page 20 |
| Appendix V – Management’s Response to the Draft Report | Page 23 |



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Abbreviations

| | |
|-------|---|
| IRS | Internal Revenue Service |
| OMB | Office of Management and Budget |
| PGLD | Privacy, Governmental Liaison, and Disclosure |
| PIA | Privacy Impact Assessment |
| PIAMS | Privacy Impact Assessment Management System |
| PII | Personally Identifiable Information |
| TIGTA | Treasury Inspector General for Tax Administration |



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Background

Within the Federal Government, privacy is defined as an individual's expectation that his or her personal information collected for official Government business will be protected from unauthorized use and access. From a legislative perspective, the topic of privacy is governed by several laws.

- The Privacy Act of 1974¹ regulates what personal information the Federal Government can collect about private individuals and how that information can be used.
- The E-Government Act of 2002² provides additional protection for personal information by requiring agencies to conduct Privacy Impact Assessments (PIA).³ The PIA is a process for examining the risks and ramifications of using information technology to collect, maintain, and disseminate information about members of the public and agency employees.
- The Consolidated Appropriations Act of 2005, Section 522,⁴ requires each agency to establish a Chief Privacy Officer who assumes the responsibility for privacy and data protection policy. This legislation also requires the Inspector General of each agency to evaluate the agency's use of information in identifiable form and the privacy and data protection procedures of the agency.

Privacy laws have significant ramifications for the Internal Revenue Service (IRS) because of its interactions with potentially every household in the United States. During Fiscal Year 2011, the IRS processed 143 million tax returns from individuals. The IRS processes and maintains sensitive information from these tax returns in computer systems for use by IRS employees to perform various jobs as administrators of the Internal Revenue Code.

Within the IRS, the Privacy, Governmental Liaison, and Disclosure (PGLD) organization has overall responsibility for privacy issues. The Privacy and Information Protection office, which is one of five offices under the PGLD organization, promotes the protection of individual privacy and integrates privacy into business practices, behaviors, and technology solutions. The specific group responsible for oversight of the PIA processes is the Privacy Compliance office.

Beginning in December 2011, the IRS required business owners to submit all new PIAs through the new Privacy Impact Assessment Management System (PIAMS). The PIAMS is a series of

¹ 5 U.S.C. § 552a (a)(5) (1974).

² Pub. L. No. 107-347, § 208, 116 Stat. 2899 (2002).

³ See Appendix IV for a glossary of terms.

⁴ Pub. L. No. 108-447, 118 Stat. 2813, 5 U.S.C. § 522a (2004).



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

web pages that allow IRS employees to input required PIAs online. It provides Privacy and Information Protection subject matter experts with the capability to perform their quality review of the assessments in an automated system. The PIAMS allows business owners and developers to enter their PIAs early in the development stage. Further, business owners of legacy systems are also required to submit their PIAs into the same system.

During our annual audit planning efforts for Fiscal Year 2012, the IRS requested that the Treasury Inspector General for Tax Administration (TIGTA) conduct a review of the IRS PIA process to ensure it meets requirements set forth by the Office of Management and Budget (OMB).⁵ As part of the E-Government Act of 2002, the OMB requires agencies to: 1) conduct PIAs for information systems and collections and, in general, make them publicly available; 2) post privacy policies on agency websites used by the public; 3) translate privacy policies into a standard computer language to enable web browser readability; and 4) report annually to the OMB regarding compliance.

TIGTA previously issued an audit report in September 2006 on the IRS's Office of Privacy⁶ and found that the IRS was not complying with legislative privacy requirements. Specifically, we reported that the IRS can take further actions to ensure that PIAs have been conducted for all systems and applications that collect personal information and to enhance its processes to better monitor compliance with privacy policy and procedures. In addition, the PIAs were not always consistently conducted, and review results were not always properly documented. Lastly, the Office of Privacy did not conduct any compliance reviews on existing PIAs.

This review was performed at the IRS PGLD organization offices in Washington, D.C., and New Carrollton, Maryland. We performed the review during the period March through September 2012. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

⁵ OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Public Law 107-347 (Sept. 2003). This guidance applies to all executive branch departments and agencies and their contractors that use information technology or operate websites for purposes of interacting with the public.

⁶ TIGTA, Ref. No. 2006-20-166, *The Monitoring of Privacy Over Taxpayer Data Is Improving, Although Enhancements Can Be Made to Ensure Compliance With Privacy Requirements* (Sept. 2006).



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

Results of Review

Improvements Are Needed to Fully Address the Privacy Provisions of the E-Government Act of 2002

The IRS has emphasized privacy as an agency priority. One of the strategic foundations cited in the *IRS Strategic Plan 2009–2013* is to ensure the privacy and security of data and safety and security of employees. For this objective, the plan states:

Taxpayers are legally obligated to report information to the IRS, and we are obligated to protect that information. With increasing amounts of data processed, we will redouble our efforts to detect and prevent security threats. By securing infrastructure, data, and applications, we will manage access to taxpayer information so that we may provide quality and timely service while protecting taxpayers' information.

One of the strategies the IRS identifies for this objective is to promote public confidence and trust through the prevention and detection of security threats and the protection of Personally Identifiable Information (PII).

During our review, we found that the Privacy Compliance office analysts effectively conducted in-depth quality reviews of completed PIAs submitted by system and program owners. From a population of 202 available PIAs completed in Fiscal Years 2011 and 2012, we reviewed 27 hardcopy PIAs and 20 online PIAs from the PIAMS and found that all PIAs contained the required information, such as an analysis of how PII is processed by the system and a description of how security risks are mitigated. Further, the Privacy and Information Protection office complied with the updated privacy reporting requirements by preparing and submitting required reports to the Department of the Treasury.

Despite its commitment toward privacy and improvements from our prior review, the IRS continues to face challenges in meeting legislative privacy requirements. Specifically, we found that:

- PIAs have not been completed or updated for all systems or customer surveys where taxpayer or employee information have been collected and maintained.
- PIAs have not been posted to the IRS's public website.
- PIAs may not be completed and submitted for internal SharePoint collaboration sites.
- Privacy notices have not been posted on all external websites.
- Key PIA processes have not been documented in standard operating procedures.



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

The process to ensure that a PIA is completed, timely updated, and publicly posted for all required systems, collections of information, and collaborative sites is not effective

The PIA consists of a set of questions that help define how a system or collection of information affects taxpayer or IRS employee privacy and can help eliminate unanticipated weaknesses in a system when conducted during the planning and design phases. PIAs are required for information technology systems or projects that collect, maintain, or disseminate information about members of the public as well as electronic collections of information that include 10 or more persons. Additionally, PIAs are required to be performed and updated when a system change creates new privacy risks. This includes conversions of paper-based records systems to electronic systems, significant system management changes, and other system changes. To initiate the PIA process, the Privacy Compliance office provides system owners with a questionnaire to assess the system's privacy requirements and determine whether a major change has occurred. The owners of the new or updated system and their Information Technology organization counterpart complete the PIA as part of the Security Assessment and Authorization that is required for all systems.⁷ The system owners answer the PIA questions and submit results to the Privacy Compliance office for review and approval. In addition to the PIA for systems and applications, the Privacy Compliance office has prepared PIA templates for customer surveys, internal collaboration websites, and third-party external websites.

The IRS did not complete PIAs for all computer systems

The IRS has not established an effective process to ensure that a PIA is completed for all required computer systems that store or process PII. The E-Government Act of 2002 requires agencies to conduct a PIA before developing or procuring information technology systems or projects that collect, maintain, or disseminate information about members of the public or initiating a new electronic collection of information for 10 or more persons. Systems that store or process PII without a PIA could adversely impact public assurance that personal information is being adequately protected. PIAs are also required to be performed and updated when a system change creates new privacy risks. System owners are supposed to use a Major Change Determination template when recording system changes. Privacy Compliance office officials told us they plan to revise this template to include system retirements and name changes.

We initially identified 582 systems or collections of information on the current production environment⁸ that did not match the list of PIAs maintained by the Privacy Compliance office. From the 582 systems or collections of information, we selected a judgmental sample⁹ of 30 and

⁷ PIAs are part of the IRS information technology development process and should be completed for all new systems.

⁸ We used the IRS As-Built Architecture to identify these information systems and collections of information in the current production environment. The current production environment includes applications and data stores.

⁹ A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

found that 13 (43 percent) are storing or processing PII and thus require a PIA. The business representatives for these 13 systems all told us that they were aware that these systems contained PII. When we raised this finding with Privacy Compliance office officials, they made a concerted effort to evaluate all known systems and collections of information and eventually determined that 184 systems and collections of information required a PIA but one could not be located. Prior to our audit, the Privacy Compliance office had not established a process to reconcile the total inventory of systems with those for which a PIA has been completed. The Privacy Compliance office completely relied on system owners to be fully aware of the details within the E-Government Act and the IRS PIA policy to complete PIAs.

The IRS did not update PIAs as required

According to IRS policy, all systems shall be reauthorized to operate whenever the system undergoes a significant change or every three years, whichever occurs first. To align with this reauthorization requirement, the Privacy Compliance office policy requires all existing PIAs to be reviewed and updated every three years at a minimum. However, the IRS has not established an effective process to ensure that PIAs are timely updated for all required systems that contain PII. Although the Privacy Compliance office maintains a PIA control listing for Fiscal Years 2008 through 2012 and the PIAMS has been operational since December 2011, neither the control listing nor the PIAMS identifies whether PIAs have reached the threshold of the mandatory three-year cycle for an update review. As a result, the Privacy Compliance office has no assurance that all PIAs requiring an update review will receive one.

We identified 162 PIAs on the Fiscal Year 2008 control listing and determined that 56 PIAs have no record of an update on the subsequent years' PIA control records. Our review of a statistical sample of 20 of the 56 PIAs determined that 11 (55 percent) did not have a subsequent update as required. After we shared this finding with the Privacy Compliance office, we were informed that a future enhancement to the PIAMS will provide the capability to identify PIAs that are nearing the three-year update threshold. Once implemented, this enhancement will help ensure that PIAs are updated as required on an ongoing basis.

The IRS did not complete PIAs for all customer surveys

Customer surveys are an important and useful tool for the IRS to measure program effectiveness, customer satisfaction, and delivery of services, but care must be taken to collect, use, disclose, or share PII during the survey process. The IRS has not established an effective process to ensure that PIAs are completed for surveys when necessary. The IRS business divisions submit their surveys to the Statistics of Income Division for review before sending them to the OMB for approval. However, the Statistics of Income Division did not review whether PII is being collected or maintained, nor did it assess privacy implications of the survey. In addition, this office did not share the survey with the Privacy Compliance office or require evidence of their review prior to processing the survey for approval.



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Although the Privacy Compliance office provides a website that includes survey PIA guidance, the survey owners determine whether they need to prepare and submit a PIA to the Privacy Compliance office for approval. We identified 130 IRS customer satisfaction surveys and cognitive research studies conducted during the period January 2011 to June 2012. The Privacy Compliance office received and processed only six survey PIAs during this time period. We determined that Privacy Compliance office personnel performed no reconciliation of surveys in its inventory and were not aware of the volume of IRS customer surveys. Further, the Privacy Compliance office has not developed a questionnaire for survey owners to assess their need for a PIA.

After we shared this finding with the IRS, it began implementing a new process whereby the Statistics of Income Division will route copies of all survey submissions to the Privacy Compliance office for review beginning August 2012. Once received, a Privacy Compliance office analyst will first review the survey within five business days to determine whether a PIA is necessary. If so, the Privacy Compliance office will work with the business operating division analysts within 15 business days to complete the PIA process and notify the Statistics of Income Division so the survey package can be forwarded to the Department of the Treasury and the OMB for review and approval. The Statistics of Income Division will also provide the Privacy Compliance office with a monthly listing of all surveys submitted to the division so that the Privacy Compliance office can verify that it reviewed all the survey submissions. On August 1, 2012, officials from the Privacy Compliance office and the Statistics of Income Division established an agreement between the two offices to ensure that all surveys are identified and reviewed for privacy requirements.

PIAs were not posted publicly on the IRS website

The OMB directs that information systems and collections of information containing taxpayer PII require a PIA and, if practicable, that the agency make the PIA publicly available through its website. The IRS, however, does not have an effective process to ensure that PIAs that contain taxpayer information are posted to its public website. We identified 80 PIAs with taxpayer PII that the IRS had not posted to its public website. These included 71 from the manual control listings and nine completed in the PIAMS.

Further, the PIAMS does not have the capability to identify and route the appropriate PIAs for eventual posting to the IRS public website, and the system does not have an alert to identify those PIAs that have not been posted to the public website. Currently, the Privacy Compliance office manually tracks PIAs through the website posting process, which is not effective. As a result, the public has no information about the security of their information in these affected systems or collections of information, and the IRS has therefore not complied with OMB instructions.



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

The IRS has not completed PIAs for internal collaboration sites

The IRS increasingly relies on digital forms of communication for computer-based real-time collaboration. Internal collaborative application websites (e.g., SharePoint) are established and configured for basic file sharing and team collaboration. These systems provide virtual space, enabling participants to communicate while also allowing for the sharing of applications and documents. Some of these features raise network and data security concerns and, therefore, proper security controls must be implemented.

The OMB requires the IRS to develop and implement PIA processes to ensure that a PIA is prepared for each system or collection of information that stores PII. Therefore, any SharePoint site that stores PII is required to have a PIA, and the Privacy Compliance office correctly states this requirement on its website. The Internal Revenue Manual, however, incorrectly states that collaborative application sites such as SharePoint that are established and configured for basic file sharing and team collaboration do not require a security authorization or a PIA. This erroneous statement in the Internal Revenue Manual may result in SharePoint site owners not submitting a PIA when PII is present, as required. The IRS has prepared a draft correction to the Internal Revenue Manual policy and has also included a reference to the Privacy Compliance office website instructions for SharePoint. The IRS does not have adequate assurance that it is complying with the privacy provisions set forth by the OMB because PII could be stored on SharePoint sites for which a PIA has not been conducted.

The Privacy Compliance office has prepared a draft SharePoint PIA questionnaire template in order to help expedite the compliance process for IRS collaboration sites. Once published, SharePoint site collaboration administrators who know PII will be on their sites will be able to respond to the template questions and forward the form to the Privacy Compliance office. The Privacy Compliance office will use those template responses to assess and mitigate any privacy risks. Sites without PII will not require a PIA. This will help facilitate the PIA determination process for SharePoint sites.

Recommendations

The Director, PGLD, should:

Recommendation 1: Investigate all 184 information systems and collections of information identified and coordinate with system owners to complete the required PIAs.

Management's Response: The IRS agreed with this recommendation. The PGLD organization stated it will determine which of these 184 systems require a PIA and coordinate with system owners to receive the required PIAs by March 15, 2014.

Recommendation 2: Establish a) an annual reconciliation process in which the PIA inventory is reconciled with all information systems and collections of information in the current production environment; b) the completion of the planned revisions to the Major Change



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Determination template, which will help facilitate the annual reconciliation process; and c) a process to identify all completed and approved PIAs that have not been updated within three years and coordinate with system owners to review and update these PIAs as required.

Management's Response: The IRS agreed with this recommendation. The PGLD organization stated it has begun work on a PIA inventory reconciliation process and completed the planned revisions to the Major Change Determination template. A process will be added to the PIAMS to identify future PIAs that are not updated within three years. Additionally, the PGLD organization is working on a manual process to identify older PIAs, not yet in the PIAMS, which need to be updated. Once the outdated PIAs have been identified, the PGLD organization will coordinate with system owners to update these PIAs.

Recommendation 3: Document its new PIA customer survey processes in the Internal Revenue Manual or on the PGLD organization website.

Management's Response: The IRS agreed with this recommendation. The PGLD organization will document its new customer survey process in the Internal Revenue Manual or on the PGLD organization website.

Recommendation 4: Ensure that the 80 PIAs that TIGTA identified as well as any other PIAs currently not available to the public are redacted as necessary and posted to the IRS public website.

Management's Response: The IRS agreed with this recommendation. The PGLD organization conducted an analysis and posted nine of the 80 PIAs to the IRS public website. In addition, the PGLD organization determined several PIAs do not require posting for various reasons, such as 1) incomplete PIAs that were initially submitted but never completed by the customers and 2) documents were not full PIAs but were Qualifying Questionnaires or Major Change Determinations. The PGLD organization stated it would redact and post approximately 20 PIAs to the IRS public website.

Recommendation 5: Update the PIAMS with the functionality to automatically notify the PGLD organization and the IRS public website web master when actions are required on their part to process new or existing PIAs for public posting.

Management's Response: The IRS agreed with this recommendation and indicated the action to address our recommendation was on the PIAMS project plan during our audit. The PGLD organization also stated this recommendation was implemented on November 29, 2012.

Recommendation 6: Both a) ensure that the new PIA template for SharePoint sites is completed and published on the Privacy Compliance office website and b) issue a memorandum to all business operating divisions advising them of the PIA template for SharePoint sites.



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Management's Response: The IRS agreed with this recommendation. The PGLD organization stated it is updating the SharePoint PIA template and applicable policy and plans to issue an interim guidance memorandum to all business operating divisions advising them of the PIA template for SharePoint sites.

The Privacy Compliance office has not established effective processes to ensure that the IRS privacy notice is posted on third-party websites and to identify unauthorized websites

The OMB requires agencies, where feasible, to post their privacy notice on third-party websites and direct individuals to the agency's official website for their privacy policy. In addition, the OMB requires that the notice to be posted on the front page of the third-party website and that all practical steps be taken to ensure that the notice is conspicuous, salient, clearly labeled, written in plain language, and prominently displayed at all locations where the public might make PII available to the IRS.

The IRS has not established an effective process to ensure compliance with the OMB's third-party website requirement and to ensure that its privacy notice and a link to its privacy policy is posted on public websites used by IRS officials. We traversed the Internet and identified the following four unauthorized public websites that were created by IRS employees without the knowledge of the Privacy Compliance office.

1. **Twitter IRS Recruiter59** – This site was created by an IRS Human Capital Office employee to enable him or her to tweet about job announcements in the IRS.
2. **Twitter IRS Careers** – This site was also created by an IRS Human Capital office employee to enable him or her to tweet information about careers in the IRS.
3. **IRS LinkedIn** – This site is used by current and former IRS employees to share information. Once an individual is admitted access to the site, the new member can invite and grant access to other members of the public. The public could post its personal information on this site.
4. **GovLoop** – This site is a social network connecting Federal, State, and local government innovators and a resource to connect with peers, share best practices, and find career-building opportunities. One of the features of this site is blogging, where an IRS Human Capital Office employee has communicated and discussed careers, retirement, and other informational topics.

We informed the IRS about the four unauthorized websites, all of which were created before the IRS established its New Media Governance Council¹⁰ to approve third-party websites in December 2010. The two Twitter websites were created by employees in the IRS Human

¹⁰ The New Media Governance Council is located within the Communication and Liaison Division at the IRS.



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

Capital office who were not official communicators handling official IRS media. The Privacy Compliance office took corrective action and both Twitter websites were deactivated in September 2012. The IRS LinkedIn and GovLoop websites violate OMB policy because both allow the public to post PII but the IRS's privacy notice and a link to its privacy policy is not provided on the websites. The Privacy Compliance office told us that the IRS LinkedIn and GovLoop websites did not contain PII and, therefore, a privacy notice was not required on these websites. However, during our review, we found information about IRS employees and other PII on these websites.

The Privacy Compliance office was not aware of the need to monitor the Internet for unapproved third-party websites. Further, if the IRS privacy policy is not posted, the public might not be aware of the risks of sharing PII on third-party websites. Taxpayers could be jeopardizing their information on these websites without the understanding that the IRS is not responsible for security over these websites.

Recommendations

The Director, PGLD, should:

Recommendation 7: Issue a memorandum, in conjunction with the Communication and Liaison Division, to all IRS executives requesting they notify the New Media Governance Council with the details of any proposed third-party website activity for review and approval.

Management's Response: The IRS agreed with this recommendation. To raise awareness of the New Media Governance Council notification process, the PGLD organization will coordinate with the Communications and Liaison Division to issue a memorandum requesting IRS executives notify the New Media Governance Council of any proposed third-party website activity for review and approval.

Recommendation 8: Ensure that a process is implemented whereby the IRS a) monitors the Internet on a continual basis for unauthorized third-party websites and b) coordinates with website owners to post the IRS privacy notice and a link to the IRS privacy policy on other third-party and social media websites.

Management's Response: The IRS agreed with this recommendation. The PGLD organization will partner with the Communications and Liaison Division to develop a monitoring solution to detect unauthorized IRS social media sites. Through the New Media Governance Council and the PIA process, the IRS will ensure that authorized social media site owners post the required privacy notices.

Key PIA processes are not documented in standard operating procedures

According to the Government Accountability Office, assessing the effectiveness of internal controls includes a determination that written policies and procedures have been developed and



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

are in place for all activities.¹¹ Privacy Compliance office management has not ensured that complete and up-to-date written guidelines in the form of standard operating procedures have been prepared for the Privacy Compliance office analysts who perform assessment, review, and processing of PIAs submitted both manually and electronically through the PIAMS. During our on-site observation of the PIA assessment and completion process, Privacy Compliance office analysts prepared informal guidelines for TIGTA to follow for both the manual PIAs and those in the PIAMS due to the lack of formal written guidelines.

The PGLD organization identifies the roles and responsibilities for privacy, information protection, and data security (including PIAs) in the Internal Revenue Manual, but these guidelines lack the granularity and specific detailed procedures for PIA assessment, review, and processing. The Internal Revenue Manual is the official source of procedures, guidelines, policies, and delegations of authority relating to administration and operations, and subordinate procedural guidance (standard operating procedures, desk procedures, *etc.*) is used to provide detailed instructions for implementing and complying with the Internal Revenue Manual requirements. Written standard operating procedures are important because Privacy Compliance office analysts are responsible for a variety of critical tasks that include performing assessments of all PIAs submitted. If problems are identified with a PIA submission, the analysts notify and communicate with the system owners to assist them in making the necessary corrections. When the assessment is completed and all data are correct, the analysts ensure that the PIAs receive approval by the Associate Director, Privacy Compliance. They also ensure that the approved PIAs get routed to the Disclosure office for redaction, when applicable, before eventual publication on the IRS public website. However, these important tasks are not detailed in complete and updated written guidelines. If the experienced analysts leave the Privacy Compliance office, there could be an adverse impact on the quality and timeliness of PIA processing.

Recommendation

Recommendation 9: The Director, PGLD, should ensure that current and complete standard operating procedures are established for all PIA processing procedures, including reviewing and approving PIAs, updating PIAs, and reconciling PIAs to other IRS system inventories.

Management's Response: The IRS agreed with this recommendation. The PGLD organization has developed standard operating procedures for the PIA review process and is currently drafting comprehensive PIA processing procedures.

¹¹ Government Accountability Office (formerly the General Accounting Office), GAO-01-1008G, *Internal Control Standards: Internal Control Management and Evaluation Tool* (Aug. 2001).



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

The Privacy Impact Assessment Management System Does Not Effectively Automate Key Privacy Impact Assessment Processes

The purpose of the PIAMS is to allow IRS system owners to electronically input responses to questions about PII to create required PIAs and then allow the Privacy Compliance office subject matter experts the ability to analyze the data requirements for the systems in an electronic format rather than the paper-based format used previously. The PIAMS consists of a series of web pages that allow IRS employees to input required PIAs online. The PIAMS also allows business owners and developers to enter their PIAs early in the development stage. Business owners of legacy systems are also required to submit their PIAs via the PIAMS. According to stated system objectives, the PIAMS is supposed to facilitate a more efficient method of completing the PIA, replacing the manual paper-based process.

We found the PIAMS does not effectively automate the review component of the PIA process. Privacy Compliance office management did not ensure that analysts, who are the subject matter experts on PIAs, were fully involved in the establishment of the PIAMS processes. Additionally, the PIAMS was not effectively tested by the system owners or the analysts who perform quality reviews of the assessments in the PIAMS. Privacy Compliance office analysts told us that they are not satisfied with PIAMS functionality and they still must perform some manual processes that the PIAMS either does not complete effectively or does not have the capability to address. The analysts simply do not consider the PIAMS to be more efficient than the manual PIA process that the system was intended to replace.

Based on our observations and analyses, we came to the same conclusion. We identified several key processes that were not effectively automated by the PIAMS. Examples include:

- The original manual PIA template allowed Privacy Compliance office analysts to easily skim the system owners' answers to the 19 questions posed. However, the new electronic PIA template in the PIAMS contains 32 questions in 11 separate sections and 27 different computer screens online. Each screen must be viewed separately because the PIAMS does not afford a scrolling feature. The Privacy Compliance office analysts told us they print the entire PIA from the PIAMS before conducting their quality review, thereby returning it to a manual process of review.
- The order of questions in the PIAMS template hinders the review of the PIA. For example, a key question for determining the need for a PIA is whether the system under review contains PII. In the PIAMS, this PII question is not asked until question eight of 32. Another key question regards whether a System of Records Notice is required for the system and whether the system contains 10 or more records with PII. These answers are not addressed until questions 30 and 31, respectively.
- Many of the electronic questions allow the system owner to input only simple yes or no answers. However, the previous PIA template required the system owner to provide



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

narrative explanations and details to facilitate a more thorough understanding of the system.

- The PIAMS does not always send e-mail notifications to the Privacy Compliance office official who is required to approve the PIA after the Privacy Compliance office analyst completes his or her review. Other important e-mail notifications are not always sent to officials who are required to take actions, such as Disclosure office analysts who must redact the PIA before it is posted to the IRS public website. These notifications currently must be performed outside of the PIAMS.

At the request of the Privacy Compliance office, MITRE Corporation (MITRE) consultants met with Privacy Compliance office officials in July 2012 and, in conjunction with analyst suggestions, proposed PIAMS template changes. The analysts and MITRE regrouped, modified, and re-ordered the PIAMS questions to eliminate unnecessary information and reduce the level of effort required by the Privacy Compliance office reviewers. The revised questions include more detailed selections replacing yes or no responses in some questions, and the original 32 PIAMS questions are reduced to 22 questions with several sub-questions and better reporting capability. We reviewed the MITRE results and believe they substantiate claims made by Privacy Compliance office analysts that problems exist with the current state of the PIAMS.

Recommendations

The Director, PGLD, should:

Recommendation 10: Assess the recommended PIAMS template modifications submitted by MITRE, as well as the necessity, feasibility, and prioritization of the planned PIAMS updates listed in the current project plan.

Management's Response: The IRS stated it independently took action on this recommendation prior to our making the recommendation. The PGLD organization stated that a team of IRS analysts and management, with MITRE's assistance, overhauled the PIAMS template in response to user feedback. The PGLD organization also stated the PIAMS template was rewritten and rearranged into an effective, comprehensive electronic assessment of privacy risks. Lastly, the PGLD organization stated it reprioritized several updates to the PIAMS based on customer feedback and its own evaluations and will continue to do so.

Office of Audit Comment: We did not see evidence that the PIAMS template was overhauled, rewritten, or rearranged to address the deficiencies that we and MITRE identified. We continue to believe the PIAMS version, at the time of our review, could be improved to ensure that PIA processes are more efficient than the manual PIA processes the system was supposed to replace.



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Recommendation 11: Gather, document, and assess the system requirements from PGLD organization analysts and other officials who use the PIAMS and implement requirements changes as necessary, and test newly implemented user requirements to ensure that the intended efficiency benefits are achieved.

Management's Response: The IRS stated it independently took action on this recommendation prior to our making the recommendation. The PGLD organization indicated that since November 2011 it has conducted information gathering on PIAMS requirements from PGLD organization analysts and other users. In addition, the PGLD organization stated it holds weekly PIAMS status update meetings with analysts, the developer, and the Contracting Officer's Representative to ensure an effective process. As a result of the meetings, the PGLD organization stated it implements changes to the PIAMS as necessary and performs testing with the PGLD organization analysts and customers.

Office of Audit Comment: The evidence we reviewed indicates the deficiencies in the PIAMS resulted from a lack of requirements gathering and testing by the PGLD organization analysts, who are the subject matter experts on PIAs. We continue to believe the PIAMS version, at the time of our review, could be improved to effectively automate the key privacy impact assessment processes.



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the IRS's processes to implement the OMB privacy provisions of the E-Government Act of 2002.¹ To accomplish our overall objective, we:

- I. Determined whether the IRS has established effective policies, plans, and procedures to ensure that a PIA² is properly completed for each required system.
 - A. Evaluated the PIA policies, plans, and procedures to ensure compliance with the key standards specified in OMB Memorandum M-03-22,³ including initial PIA assessment, preparation, submission, quality review, approval, publication, and updates.
 - B. Interviewed PGLD organization officials to identify the controls they implemented to ensure that a PIA is completed and updated for all required systems.
 - C. Assessed the adequacy of the PIA determination process for surveys.
 - D. Evaluated processes to ensure that a PIA is completed for each SharePoint site that stores PII.
 - E. Obtained downloads of the PIAs accounted for by the PGLD Privacy Compliance office in the PIAMS and in Fiscal Years 2008 through 2012 PIA inventory manual control listings.
 - F. Determined whether the PGLD Privacy Compliance office's processes ensure that a PIA is completed for all systems that require a PIA.
 1. Obtained a download of the IRS system inventories that contained a total of 823 systems.
 2. Identified 582 systems in the inventories that did not match systems in the PIA listings.

¹ Pub. L. No. 107-347 (2002), sec. 208.

² See Appendix IV for a glossary of terms.

³ OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Public Law 107-347 (Sept. 2003). This guidance applies to all executive branch departments and agencies and their contractors that use information technology or operate websites for purposes of interacting with the public.



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

3. Selected a judgmental sample⁴ of 30 unmatched systems from the 582 systems in Step I.F.2. to identify active systems that should have a PIA.
 4. Interviewed the business representatives for the 30 unmatched systems in our judgmental sample and determined whether they were aware that a PIA was required based on the E-Government Act of 2002.
 5. At the end of our fieldwork, we worked with IRS officials to cull down the number of systems needing a PIA from 582 to 184 systems.
- G. Determined whether redacted copies of all PIAs are made available on the IRS.gov public website, except where prohibited for security reasons.
1. Compared the PIAs posted on the IRS.gov public website to the PGLD organization's PIA control listings and the independent inventory listing to identify those not posted.
 2. Determined the validity of the reasons for the PGLD organization not posting any PIAs to the IRS.gov public website.
- H. Conducted an on-site observation of the PIAMS and the procedures performed by the PGLD organization analysts who process and review the PIAs. We conducted a manual reconciliation of all records in the PIAMS.
- I. Determined whether PGLD organization processing ensures that PIAs are properly approved, current, complete, accurate, and in compliance with OMB and E-Government Act provisions.
1. Selected a statistical sample of 25 PIAs from the PIA listings and 18 PIAMS PIAs based on a ± 5 percent precision rate, 2 percent error rate, and 95 percent confidence level. We also judgmentally selected three surveys and one social media PIAs.
 2. Selected a statistical sample of 20 Fiscal Year 2008 PIAs with no three-year update, based on a ± 5 percent precision rate, 2 percent error rate, and 95 percent confidence level.
 3. Determined whether the selected PIAs were properly approved, complete, and accurate and whether the PIA answered the required questions that define how a system affects taxpayer or IRS employee privacy.
- II. Determined whether the IRS posted a privacy policy on their public third-party websites and whether the policy complies with OMB requirements.

⁴ A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

- III. Determined whether the IRS submitted required privacy information in Fiscal Year 2011 to the Department of the Treasury, based on the updated reporting requirements for the Federal Information System Management Act, Section D, Senior Agency Official for Privacy report.

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 the following internal controls were relevant to our audit objective: OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*; the Department of the Treasury's Publication 25-07, *Privacy Impact Assessment Manual* (dated August 2008); and related Internal Revenue Manual guidelines and processes followed by the IRS to implement the privacy provisions of the E-Government Act of 2002. We evaluated these controls by interviewing IRS officials in the PGLD office and other IRS offices that have duties and responsibilities for implementing the privacy provisions. We also analyzed pertinent documentation and observed the operation of the PIAMS.



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)

Kent T. Sagara, Director

W. Allen Gray, Audit Manager

Jena R. Whitley, Acting Audit Manager

George L. Franklin, Lead Auditor

Midori Ohno, Senior Auditor

Sam Mettauer, Information Technology Specialist



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Director, Office of Research, Analysis, and Statistics RAS
Director, Office of Privacy, Governmental Liaison, and Disclosure OS:P
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, User and Network Services OS:CTO:UNS
Director, Privacy and Information Protection, OS:P:PIP
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
 Office of Privacy, Governmental Liaison, and Disclosure OS:P
 Director, Risk Management Division OS:CTO:SP:RM



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Appendix IV

Glossary of Terms

| Term | Definition |
|---|--|
| As-Built Architecture | An integral part of the IRS's Enterprise Architecture dedicated to documenting the Current Production Environment (applications, data stores, infrastructure, data interfaces) and related organizations, locations, technology platforms, <i>etc.</i> |
| Federal Information Security Management Act | A part of the E-Government Act of 2002 that consolidates many security requirements and guidance into an overall framework for managing information security. |
| Fiscal Year | A 12-consecutive-month period ending on the last day of any month, except December. The Federal Government's fiscal year begins on October 1 and ends on September 30. |
| Information Technology | Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. |
| Internal Revenue Manual | The single, official source of IRS instructions to staff. Instructions to staff are procedures, guidelines, policies, and delegations of authority and other such instructional materials relating to the administration and operation of the IRS. |
| MITRE Corporation (MITRE) | Hired by the IRS as a Federally Funded Research and Development Center to assist with the systems modernization effort. |
| New Media Governance Council | Serves as an advisory body for oversight and coordination and for providing input and guidance on major decisions relating to development and implementation of new media channels. |



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

| Term | Definition |
|--|--|
| Office of Management and Budget (OMB) | The OMB's predominant mission is to assist the President in overseeing the preparation of the Federal budget and to supervise administration in Executive Branch agencies. The OMB evaluates the effectiveness of agency programs, policies, and procedures. The OMB oversees and coordinates the Administration's procurement, financial management, information, and regulatory policies. |
| Office of Privacy, Governmental Liaison, and Disclosure (PGLD) | The mission of the PGLD organization is to preserve and enhance public confidence by advocating for the protection and proper use of identity information. The PGLD organization consists of five offices: Governmental Liaison and Disclosure; Office of Safeguards; Online Fraud Detection and Prevention; Privacy and Information Protection; and Program and Planning Support. |
| Personally Identifiable Information (PII) | Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. |
| Privacy Impact Assessment (PIA) | An analysis of how information is handled: (1) to ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. |
| Privacy Impact Assessment Management System (PIAMS) | A series of web pages that allows customers to input responses to questions about PII. The PIAMS also allows the Privacy subject matter experts the ability to analyze the data requirements for the particular system in an electronic format. |



Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process

| Term | Definition |
|------------------------------------|--|
| Privacy Notice | A brief description of how the agency’s privacy policy will apply in a specific situation. The privacy notice should notify individuals before they engage with an agency and should be provided on the specific web page or application where individuals have the opportunity to make PII available to the agency. |
| Privacy Policy | A single, centrally located statement about an agency’s general privacy practices that is accessible from an agency’s official homepage. It should be a consolidated explanation of the agency’s general privacy-related practices that pertain to its official website and its other online activities. |
| Senior Agency Official for Privacy | The Director, PGLD, serves as the IRS Senior Agency Official for Privacy, having overall responsibility for accounting to the Department of the Treasury, the OMB, and other regulatory agencies regarding the IRS’s implementation of information privacy protections, including full compliance with Federal laws, regulations, and policies relating to information protection. |
| Statistics of Income Division | The mission of the Statistics of Income Division is to collect, analyze, and disseminate information on Federal taxation for the Department of the Treasury’s Office of Tax Analysis, congressional committees, the IRS in its administration of the tax laws, other organizations engaged in economic and financial analysis, and the general public. |
| System of Records Notice | The Privacy Act requires publication of a System of Records Notice in the Federal Register for all Systems of Records in the agency for which personal information about individuals is retrieved by unique individual identifiers. |
| Third-Party Website | Web-based technologies that are not exclusively operated or controlled by a Government entity and often are not part of an official Government domain. |



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Appendix V

Management's Response to the Draft Report




PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

JAN 28 2013

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Rebecca A. Chiaramida 
Director, Privacy, Governmental Liaison and Disclosure

SUBJECT: Draft Audit Report – Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process (Audit
201220009)

Thank you for the opportunity to respond to the above referenced draft audit report. Ensuring the privacy and security of data is a top priority for the IRS and a fundamental component of ensuring the public trust in the tax system and promoting voluntary compliance.

The IRS is a model for privacy practices within the federal government and remains at the forefront of government privacy initiatives. In 1995, the IRS created the first Privacy Impact Assessment (PIA), which was adopted in 2000 by the Federal Chief Information Officer's (CIO) Council as a best practice for all governmental agencies. In the early 2000s, the IRS initiated the Enterprise Life Cycle (ELC), a project management methodology consisting of standardized processes, and integrated the PIA as a required step of the ELC. Congress subsequently incorporated the PIA into the E-Government Act of 2002 and Committee Reports cite the IRS's PIA process as the model for this legislation. In response to the Consolidated Appropriations Act of 2005, the IRS became one of the first bureaus within the Department of the Treasury (Treasury) to appoint a Senior Agency Official for Privacy. We developed some of the first adaptive PIAs for surveys, social media, and collaborative software sites. Additionally, the IRS is 100 percent compliant for PIAs on systems reportable under the Federal Information Systems Management Act.

In December 2011, we implemented the PIA Management System (PIAMS), a significant achievement that has been recognized as a privacy best practice. The IRS deployed the PIAMS to eliminate paper PIAs and reduce burden for all users. We have demonstrated the system to several other federal agencies, and Treasury plans to use the PIAMS as a model for PIA management in its other bureaus.



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

2

We are continuously evaluating the PIAMS and looking for ways to further improve its functionality. As a result, we have already implemented, or are in the process of implementing, many of the recommendations outlined in this report.

If you have any questions, please contact me at (202) 622-2988, or a member of your staff may contact Tracey Showman, Director, Privacy and Information Protection, at (202) 622-8387.

Attachment



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

Attachment

Draft Audit Report – Improvements Are Needed to Ensure the Effectiveness of the
Privacy Impact Assessment Process
(Audit # 201220009)

RECOMMENDATION 1: Investigate all 184 systems and collections of information identified and coordinate with system owners to complete the required PIAs.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The list provided by TIGTA requires some additional analysis, as not all systems or applications listed on the IRS As-Built Architecture require a PIA. We will determine which of these 184 systems require a PIA and coordinate with the system owners to ensure that PIAs are received in the Office of Privacy Compliance by the implementation date.

IMPLEMENTATION DATE: March 15, 2014

RESPONSIBLE OFFICIAL: Director, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

RECOMMENDATION 2: Establish a) an annual reconciliation process in which the PIA inventory is reconciled with all systems and collections of information in the current production environment; b) the completion of the planned revisions to the Major Change Determination template, which will help facilitate the annual reconciliation process; and c) a process to identify all completed and approved PIAs that have not been updated within three years and coordinate with system owners to review and update these PIAs as required.

CORRECTIVE ACTION: The IRS agrees with this recommendation. We have already begun work on a PIA inventory reconciliation process, and we have completed the planned revisions to the Major Change Determination template. We are adding to the PIA Management System (PIAMS) a process for identifying future PIAs that are not updated within three years. We are also working on a manual process to identify older PIAs not yet in PIAMS that need to be updated. Once we identify those PIAs that have not been updated for three years, we will coordinate with the system owners to ensure they complete a PIA in PIAMS by the implementation date.

IMPLEMENTATION DATE: March 15, 2014

RESPONSIBLE OFFICIAL: Director, Privacy, Governmental Liaison and Disclosure



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

2

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

RECOMMENDATION 3: Document its new PIA customer survey processes in the Internal Revenue Manual or on the PGLD organization website.

CORRECTIVE ACTION: The IRS agrees with this recommendation. We will document our new customer satisfaction survey PIA process on the PGLD organization website.

IMPLEMENTATION DATE: April 15, 2013

RESPONSIBLE OFFICIAL: Director, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

RECOMMENDATION 4: Ensure that the 80 PIAs that the TIGTA identified as well as any other PIAs currently not available to the public are redacted as necessary and posted to the IRS public website.

CORRECTIVE ACTION: The IRS agrees with this recommendation. We have now posted nine of the PIAs – those that were in the PIAMS – to the IRS public website. After doing additional analysis, we have determined that not all of the 71 manual inventory items identified by TIGTA require posting. For example, some of the items on the manual control listing TIGTA referenced were not full PIAs but were Qualifying Questionnaires or Major Change Determinations. Others were incomplete PIAs, initially submitted but never completed by the customers. A few more were previously posted but were more than three years old, so they were removed. We will ensure that the approximate 20 remaining PIAs, as well as any other PIAs currently not available to the public, will be redacted as necessary and posted to the IRS public website.

IMPLEMENTATION DATE: October 15, 2013

RESPONSIBLE OFFICIALS: Director, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

RECOMMENDATION 5: Update the PIAMS with the functionality to automatically notify the PGLD organization and the IRS public website web master when actions are required on their part to process new or existing PIAs for public posting.



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

3

CORRECTIVE ACTION: The IRS agrees with this recommendation. This action was on the PIAMS project plan during TIGTA's audit and was implemented on November 29, 2012.

IMPLEMENTATION DATE: Implemented

RESPONSIBLE OFFICIALS: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION 6: Both a) ensure that the new PIA template for SharePoint sites is completed and published on the Privacy Compliance office website and b) issue a memorandum to all business operating divisions advising them of the PIA template for SharePoint sites.

CORRECTIVE ACTION: The IRS agrees with this recommendation. We are in the process of updating the SharePoint PIA template and policy, and plan to issue an interim guidance memorandum to all business operating divisions.

IMPLEMENTATION DATE: August 15, 2013

RESPONSIBLE OFFICIALS: Director, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

RECOMMENDATION 7: Issue a memorandum, in conjunction with the Communication and Liaison Division, to all IRS executives requesting they notify the New Media Governance Council with the details of any proposed third-party website activity for review and approval.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The New Media Governance Council notification process is already a requirement in social media guidance for all IRS employees on the internal website. However, to raise awareness, the IRS Office of Privacy, Government Liaison and Disclosure will partner with the Communications and Liaison Division to issue a memorandum.

IMPLEMENTATION DATE: May 15, 2013

RESPONSIBLE OFFICIALS: Director, Privacy, Governmental Liaison and Disclosure and Director, Communications and Liaison

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

4

RECOMMENDATION 8: Ensure a process is implemented whereby the IRS a) monitors the Internet on a continual basis for unauthorized third-party websites and b) coordinates with website owners to post the IRS privacy notice and a link to the IRS privacy policy on other third-party and social media websites.

CORRECTIVE ACTION: The IRS agrees with this recommendation. Through the New Media Governance Council and the PIA process, the IRS already ensures authorized social media site owners post the required privacy notices. To ensure a process to detect unauthorized IRS social media sites, the IRS Office of Privacy, Government Liaison and Disclosure will partner with the Communications and Liaison Division to develop a monitoring solution.

IMPLEMENTATION DATE: July 15, 2013

RESPONSIBLE OFFICIALS: Director, Privacy, Governmental Liaison and Disclosure and Director, Communications and Liaison

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

RECOMMENDATION 9: The Director, PGLD, should ensure that current and complete standard operating procedures are established for all PIA processing procedures, including reviewing and approving PIAs, updating PIAs, and reconciling PIAs to other IRS system inventories.

CORRECTIVE ACTION: The IRS agrees with this recommendation. We have developed standard operating procedures for the PIA review process, and we are currently drafting comprehensive PIA processing procedures.

IMPLEMENTATION DATE: December 15, 2013

RESPONSIBLE OFFICIALS: Director, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN: Establish a timeline of necessary actions that incorporates expected outcomes and dates to successfully accomplish stated tasks.

RECOMMENDATION 10: Assess the recommended PIAMS template modifications submitted by the MITRE Corporation, as well as the necessity, feasibility, and prioritization of the planned PIAMS updates listed in the current project plan.

CORRECTIVE ACTION: The IRS had independently taken action on this issue prior to receiving this recommendation. A team of IRS analysts and management, with MITRE's assistance, overhauled the PIAMS template in response to user feedback,



*Improvements Are Needed to Ensure the
Effectiveness of the Privacy Impact Assessment Process*

5

rearranging and rewriting it into an effective, comprehensive electronic assessment of privacy risks. Assessment of the necessity, feasibility, and prioritization of planned PIAMS updates is an ongoing process. We have reprioritized several updates based on customer feedback and our own evaluations and will continue to do so.

IMPLEMENTATION DATE: Implemented

RESPONSIBLE OFFICIALS: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION 11: Gather, document, and assess the system requirements from PGLD analysts and other officials who use the PIAMS and implement requirements changes as necessary, and test newly implemented user requirements to ensure the intended efficiency benefits are achieved.

CORRECTIVE ACTION: The IRS had independently taken action on this issue prior to receiving this recommendation. Since November 2011, we increased our focus on gathering PIAMS requirements from PGLD analysts and other users. We hold weekly PIAMS status update meetings with PGLD analysts, the developer, and the Contracting Officer's Representative to ensure an effective process. As a result of these meetings, we implement changes as necessary. Additionally, we perform testing of newly implemented user requirements with PGLD analysts and customers.

IMPLEMENTATION DATE: Implemented

RESPONSIBLE OFFICIALS: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A