TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Actions Have Been Taken to Improve the Privacy Program; However, Some Privacy Controls Have Not Been Fully Implemented and Assessed

June 14, 2023

Report Number: 2023-20-034

TIGTACommunications@tigta.treas.gov | www.tigta.gov

HIGHLIGHTS: Actions Have Been Taken to Improve the Privacy Program; However, Some Privacy Controls Have Not Been Fully Implemented and Assessed

Final Audit Report issued on June 14, 2023 **Report Number 2023-20-034**

Why TIGTA Did This Audit

The Privacy, Governmental Liaison and Disclosure Office administers privacy, disclosure, and identity assurance as well as policies, procedures, and initiatives throughout the IRS. It also coordinates privacy protection guidance and activities, responds to privacy complaints, and promotes data protection awareness.

The Consolidated Appropriations Act, 2005, requires the Inspector General of each respective agency to periodically evaluate the agency's use of information in identifiable form and privacy and data protection procedures.

This audit was initiated to assess the effectiveness of the implementation of new Federal requirements for privacy controls for information systems and organizations and follow up on prior TIGTA recommendations.

Impact on Tax Administration

Failure to fully implement and assess privacy controls exposes Personally Identifiable Information and tax information on IRS systems to potential unauthorized access, use, disclosure, disruption, modification, and destruction. In addition, incomplete and inaccurate reporting of privacy control assessments and the status of control implementation may result in unreliable information, which can lead to unidentified weaknesses that are not addressed.

What TIGTA Found

The IRS fully and effectively implemented the planned corrective actions for four of six prior TIGTA recommendations. The IRS developed an inventory of systems that collect and use Personally Identifiable Information, developed a new training course for preparers of Privacy and Civil Liberties Impact Assessments to capture system enhancements, monitored mandatory employee privacy awareness training for compliance, and strengthened the Privacy and Civil Liberties Impact Assessment review process.

However, the IRS fully implemented two planned corrective actions that were not effective. While the IRS updated its guidance to require preparers of rejected Privacy and Civil Liberties Impact Assessments to complete the appropriate privacy awareness training, it does not have a process in place to track preparers or the training taken to satisfy the requirement.

In addition, the IRS did not assess 388 of 529 privacy controls for 15 on-premise systems TIGTA selected for review. For the 141 privacy controls that were assessed, 95 were implemented; 41 were found to be not implemented, undefined, or missing; and five were not applicable. The IRS also misclassified 22 of 41 privacy controls as system-level controls instead of as inherited controls.

Further, the IRS did not implement and assess 768 privacy controls for eight cloud systems TIGTA selected for review. Finally, 3,881 of 18,688 contractors have not taken the required annual privacy awareness training.

What TIGTA Recommended

TIGTA recommended that the Chief Privacy Officer: 1) develop a process to track and ensure that preparers of rejected Privacy and Civil Liberties Impact Assessments complete the appropriate privacy awareness training; 2) prioritize the implementation of the remaining privacy controls not yet assessed; 3) correctly apply assessed privacy control results to all fields in the new assessment and monitoring system and capture them in the system security plans; and 4) implement privacy controls for cloud systems within one year from when updated Federal Risk and Authorization Management Program guidance is released. In addition, TIGTA recommended that the Human Capital Officer implement a process to track contractor privacy training compliance.

The IRS agreed with all five recommendations. The Chief Privacy Officer plans to develop a process to track preparers who are required to complete additional training; prioritize privacy controls that have not been assessed in accordance with the privacy controls assessment plan; review a sample of system security plans to ensure privacy control statuses are correct; and assess implemented controls within one year from the revision of the applicable control baselines for cloud systems. The Human Capital Officer plans to implement a process to monitor contractor mandatory briefing completion rates.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

June 14, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Actions Have Been Taken to Improve the Privacy Program; However, Some Privacy Controls Have Not Been Fully Implemented and Assessed (Audit # 202220003)

This report presents the results of our review to assess the effectiveness of the implementation of new Federal requirements in the National Institute of Standards and Technology, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020), and follow up on prior Treasury Inspector General for Tax Administration recommendations. This review is part of our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS [Internal Revenue Service] Resources*.

Management's complete response to the draft report is included as Appendix III. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background ..... Page 1

Results of Review ..... Page 2

Most Planned Corrective Actions Have Been Fully and Effectively Implemented ..... Page 2

Training for Preparers of Rejected Privacy and Civil Liberties Impact Assessments Is Not Enforced or Tracked, and Not All Privacy Controls Have Been Fully Implemented and Assessed ..... Page 7

Recommendation 1: ..... Page 7

Recommendations 2 and 3: ..... Page 10

Recommendation 4: ..... Page 11

Contractors Did Not Always Complete the Annual Privacy Awareness Training ..... Page 11

Recommendation 5: ..... Page 12

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 13

Appendix II – Outcome Measures ..... Page 15

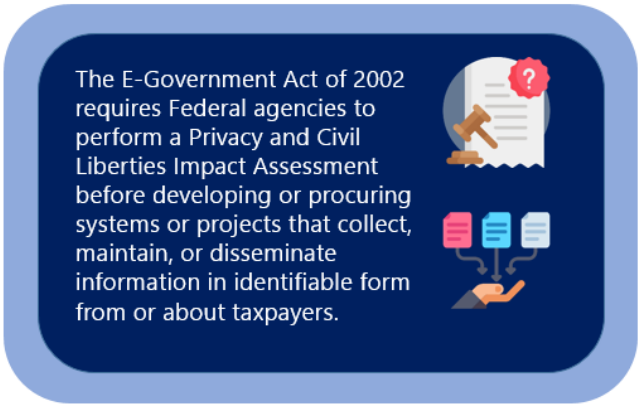
Appendix III – Management's Response to the Draft Report ..... Page 17

Appendix IV – Glossary of Terms Page.21

Appendix V – Abbreviations Page.23

Background

According to the Internal Revenue Service (IRS), the security and privacy of taxpayer and employee information is one of its highest priorities. The Privacy, Governmental Liaison and Disclosure (PGLD) Office administers privacy, disclosure, and identity assurance as well as policies, procedures, and initiatives throughout the IRS. The PGLD Office also coordinates privacy protection guidance and activities, responds to privacy complaints, and promotes data protection awareness. In addition, each IRS business unit is responsible for managing its own privacy, disclosure, identity assurance, and records management requirements based on Service-wide policies and procedures.



The E-Government Act of 2002 requires Federal agencies to perform a Privacy and Civil Liberties Impact Assessment (PCLIA), formerly known as a Privacy Impact Assessment, before developing or procuring systems or projects that collect, maintain, or disseminate information in identifiable form from or about taxpayers.[1] A PCLIA is a process of analyzing how sensitive but unclassified data, including Personally Identifiable Information (PII) and tax information, are used, collected, received, displayed, stored, maintained, protected, shared, managed, and disposed. The Privacy Impact Assessment Management System (PIAMS) is the central repository for PCLIAs. System owners must ensure that all new systems, systems under development, and systems undergoing major modifications that contain sensitive but unclassified data have a completed and approved PCLIA. The PGLD Office is responsible for reviewing, managing, and maintaining the inventory of PCLIAs.

In addition, the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020), establishes controls for information systems (hereafter referred to as systems) and organizations. The implementation of its standards and guidelines is mandatory for all Federal systems. Federal agencies are given up to one year to implement the standards and guidelines from the date of their issuance. NIST, SP 800-53, Revision 5, is designed to help organizations identify the security and privacy controls needed to manage risk and satisfy the security and privacy requirements of the Federal Information Security Modernization Act of 2014 (FISMA).[2] NIST, SP 800-53, Revision 5, is also designed for organizations to manage the privacy requirements of the Office of Management and Budget, the Federal Information Processing Standards, and the Privacy Act.[3] According to NIST, organizations can use the security and

[1] Pub. L. No. 107-347, 107-347, 116 Stat. 2899 § 208 (2002). See Appendix IV for a glossary of terms.

[2] Pub. L. No. 113-283, S. 2521.

[3] Pub. L. No. 93-579, 88 Stat. 1896, 5 U.S.C. § 552a.

privacy controls to protect from traditional and advanced persistent threats and privacy risks resulting from the processing of PII.

Assessment of the security and privacy controls helps to ensure that controls selected by agencies are implemented correctly, operating as intended, and effective in satisfying the requirements. Agencies must select specific security and privacy controls for assessment during any one-year period, *i.e.*, the annual assessment window. At the IRS, security and privacy controls are assessed during a three-year cycle, in which one third of all controls are assessed each year. The results of the control assessment are compiled into a system security plan (SSP) and provide an overview of the security and privacy requirements for the system as well as describe the controls in place or plans for meeting these requirements. System owners must submit a SSP annually or sooner if there are significant changes to the system.

Finally, the Consolidated Appropriations Act, 2005, requires the Inspector General of each respective agency to periodically evaluate the agency's use of information in identifiable form and privacy and data protection procedures.[4] In September 2019, we issued a report of the IRS's privacy program and made six recommendations.[5] The recommendations included:

1) Develop and maintain an inventory of systems that collect and use PII.
2) Update and maintain PIAMS training courses to capture the system's enhancements.
3) Ensure that all employees take the annual privacy awareness training.
4) Strengthen enforcement of the PCLIA review process.
5) Make PIAMS training courses mandatory for preparers of rejected PCLIAs.
6) Implement a fully integrated information security continuous monitoring process that includes privacy risks.

Results of Review

Most Planned Corrective Actions Have Been Fully and Effectively Implemented

As of July 2021, the IRS reported in the Joint Audit Management Enterprise System that it closed the planned corrective actions (PCA) for all six recommendations made in our prior report. The system is the Department of the Treasury's (hereafter referred to as the Treasury Department) web-based management controls database tracking system. It is used to track issues, findings, and recommendations extracted from Government Accountability Office, Treasury Office of Inspector General, and Treasury Inspector General for Tax Administration reports. It is also used to track the status of the PCAs for material weaknesses, significant deficiencies, existing reportable conditions, remediation plans, and action plans.

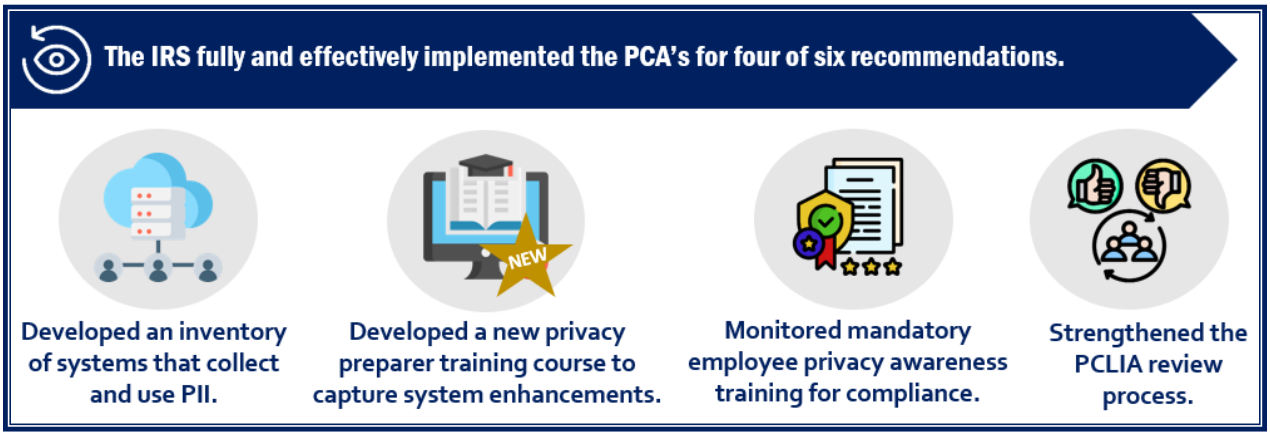
[4] Pub. L. No. 108-447, 118 Stat. 2809 § 522 (2004).

[5] Treasury Inspector General for Tax Administration, Report No. 2019-20-062, *Some Components of the Privacy Program Are Effective; However, Improvements Are Needed* (Sept. 2019).

Tracking issues, findings, recommendations, and the status of the PCAs is mandatory to comply with the intent of the Government Accountability Office's *Standards for Internal Control in the Federal Government* (Sept. 2014), the Federal Managers Financial Integrity Act of 1982, Office of Management and Budget Circulars, and Treasury Department Directives.[6] In addition, the Treasury Department and its bureaus use the information contained in the Joint Audit Management Enterprise System to assess the effectiveness and progress in correcting internal control deficiencies and implementing audit recommendations.

We reviewed the artifacts supporting the implementation of the PCAs and found that the IRS fully and effectively implemented the PCAs for four of six recommendations. The IRS developed an inventory of systems that collect and use PII, developed a new privacy preparer training course to capture system enhancements, monitored mandatory employee privacy awareness training for compliance, and strengthened the PCLIA review process. Figure 1 presents the PCAs that were fully and effectively implemented.

Figure 1: The Four PCAs Fully and Effectively Implemented



Source: Treasury Inspector General for Tax Administration's analysis of the PCAs.

An inventory of systems that collect and use PII has been developed

We reported previously that the IRS did not have a complete inventory of systems that collect and use PII. The IRS agreed to create this inventory of systems in the PIAMS.

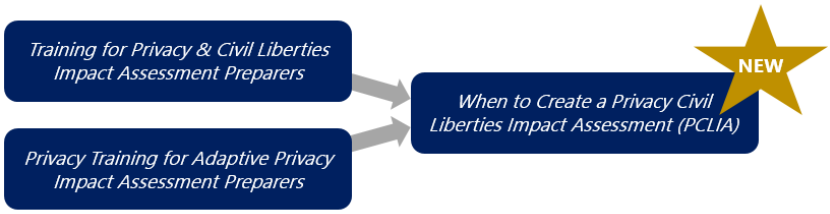
The IRS submitted two inventory lists, one manual and one PIAMS-generated, of systems that collect and use PII as well as a copy of the programing language used to generate the PIAMS list to support the closure of this PCA. Our review of the documentation determined that the IRS developed a capability in the PIAMS to generate a current inventory of systems that collect and use PII.

[6] 31 U.S.C. §§ 1105, 1113, and 3512 (2013).

To determine the accuracy of the inventory of systems, we obtained from the As-Built Architecture a list of all IRS systems requiring a PCLIA in the current production environment and compared it to the PIAMS inventory of systems that collect and use PII.[7] All 456 active systems in an As-Built Architecture report are included in the PIAMS as of February 2023.[8] In addition, we selected a judgmental sample of 39 systems identified in the As-Built Architecture that collect and use PII to determine whether the PCLIAs documented its system's use of PII and whether the systems were include in the PIAMS inventory.[9] All 39 systems documented the system's use of PII and were included in the PIAMS inventory. As a result, we determined that this PCA was fully and effectively implemented.

A new PCLIA preparer training course that includes system enhancements has been developed

We previously reported that the two privacy awareness training courses, *Training for Privacy & Civil Liberties Impact Assessment Preparers* and the *Privacy Training for Adaptive Privacy Impact Assessment Preparers*, developed in Calendar Year 2015 had not been updated since the implementation of the PIAMS even though the system underwent several enhancements. The IRS agreed to complete a review of the existing PCLIA training courses and update them as needed. In January 2021, the IRS developed a new training course, *When to Create a Privacy Civil Liberties Impact Assessment (PCLIA)*, to replace the two prior training courses and to support the closure of this PCA.



According to the new training course and PGLD Office personnel, the training course is for all PCLIA preparers regardless of the type of assessment, *e.g.*, Questionnaire (System PCLIA), Social Media, and Survey, being submitted and for owners of systems that collect and use PII or sensitive but unclassified data. The new training course provides guidance on what is a PCLIA, why and when a PCLIA must be completed, the PIAMS process, and users' roles and responsibilities. The new training course also provides a description of each type of PCLIA along with a Qualifying Questionnaire, *i.e.*, assesses whether a system collects or uses PII or sensitive but unclassified data, and Major Change Determination, *i.e.*, assesses whether a major system change occurred. In addition, the new training course includes a link to the *Privacy Impact Assessment Management System (PIAMS) User Guide* (Mar. 2016), which provides the system's enhancements. PGLD Office personnel stated that they included the system enhancement in the user guide rather than in the new training course because they have direct access to the user

[7] The As-Built Architecture is the authoritative repository of all of IRS's current production environment systems, which contains critical application and PCLIA information.

[8] We excluded applications with a status of archived, retired, or future.

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

guide and can more timely update it to reflect new PIAMS enhancements. As a result, we determined that this PCA was fully and effectively implemented.

Mandatory employee privacy awareness training is monitored to ensure compliance

We reported previously that the IRS did not ensure that all active employees complete the annual privacy awareness training. The IRS agreed to have the PGLD Office issue a Service-wide Leaders Alert communication reminding managers to ensure that all of their employees complete the annual privacy awareness training by the due date.

In April 2020, a Service-wide Leaders Alert was issued to managers informing them that the annual mandatory briefings (which include several mandatory training courses, including the *Privacy, Information Protection and Disclosure Briefing*) would be available on May 1, 2020, in the Integrated Talent Management System and must be completed by November 30, 2020.

In addition, in July 2021, the Human Capital Office developed and implemented a dashboard to help monitor the training progress of the mandatory briefings for existing employees. The dashboard provides information on the number of employees assigned to a specific training course and the training completion rate, including the number of employees who have and have not taken the training. In July 2022, a similar dashboard was developed and implemented to monitor the mandatory briefings assigned to newly hired employees. Both dashboards provide training statistics and progress by business unit or by the specific training course.

To assess the effectiveness of the PCA, we reviewed the training completion rates for the *Privacy, Information Protection and Disclosure Briefing* during FISMA Year 2022 (July 1, 2021, to June 30, 2022). With a goal of 97 percent, we found that 68,735 (98 percent) of 69,799 existing employees and 3,681 (99 percent) of 3,726 newly hired employees completed the assigned training.[10] As a result, we determined that this PCA was fully and effectively implemented.

The PCLIA review process has been strengthened

We reported previously that some PCLIAs are not timely reassessed. During our 2019 review of 173 systems with expiring PCLIAs, the assessments for 123 (71 percent) systems were timely updated, 37 (21 percent) systems were not timely updated, and 13 systems were retired. We also reported that there were no formal procedures to elevate the expired PCLIAs to system owner management. The IRS agreed to analyze the escalation process in their internal procedures and revise, as necessary, to ensure that PGLD Office management is involved in the process.

In February 2020, the IRS updated the escalation process in its standard operating procedures. Our review of the standard operating procedures determined that a process is in place to track the expiration of the PCLIAs. The standard operating procedures include a notification and an escalation process that involve business unit and PGLD Office personnel and management when the PCLIAs are not timely reassessed. Specifically, e-mails concerning PCLIA reassessment and renewal are sent at 90, 60, and 30 calendar days prior to the expiration of the PCLIA. The initial e-mail at 90 calendar days prior to the expiration of the PCLIA is sent to the PCLIA preparer and business unit program manager. If no response is received, the matter is referred to the lead privacy analyst at 60 calendar days and the privacy manager at 30 calendar days prior to the

[10] Newly hired employees are defined as employees hired on or after July 1, 2021.

expiration of the PCLIA for additional business unit contacts and coordination before subsequent e-mails are sent. In addition, the privacy manager can elevate the matter to the Associate Director of Privacy Compliance and Assurance, who may initiate contact with the business unit senior manager or executive.

In August 2022, during our audit, the PGLD Office further updated and renamed its standard operating procedures. The new procedures increased the time to notify business unit personnel of expiring PCLIAs and further defined the management escalation process. The initial e-mail is now sent at 120 calendar days prior to the expiration of the PCLIA and is sent to the PCLIA preparer and subject matter expert with a copy to the privacy analyst. If no response is received, subsequent e-mails are sent and notifications to business unit personnel are escalated to include the program manager at 90 calendar days and the system owner at 60 calendar days prior to the expiration of the PCLIA. Similarly, notifications to PGLD Office management are also escalated to include the privacy manager and the privacy executive, *e.g.*, the Associate Director of Privacy Compliance and Assurance. We determined that the e-mail sent at 60 calendar days prior to the expiration of the PCLIA also included a statement that if the PCLIA is not renewed by the due date, the matter will be elevated for immediate action which may include immediate shutdown of the system.

If there is still no response after 10 calendar days from the e-mail sent at 60 calendar days prior to the expiration of the PCLIA, the privacy manager will refer the matter to the Associate Director of Privacy Compliance and Assurance. The Associate Director will e-mail the business unit executive responsible for the reassessment and renewal of the PCLIA. If there is no response after another 10 calendar days, the matter is referred to the Director, Privacy Policy and Compliance, who will contact the business unit director.

To evaluate any improvement in the timeliness of reassessed PCLIAs resulting from the two updated standard operating procedures, we obtained a PIAMS report of the PCLIAs expiring from January 2022 through February 2023 and reviewed the timeliness of reassessments. The results of our review of the two standard operating procedures were:

- From January through November 2022 when the standard operating procedures issued in February 2020 were in effect, we found that of 132 systems with expiring PCLIAs, the assessments for 97 (73 percent) systems were timely updated, 27 (20 percent) systems were not timely updated, and eight systems were retired.[11] The days late ranged from one to 175 calendar days, averaging 53 calendar days.
- From December 2022 through March 2023 when the updated standard operating procedures issued in August 2022 were in effect, we found that of 28 systems with expiring PCLIAs, the assessments for 26 (93 percent) systems were timely updated, one system was being reviewed, and one system was retired. The PCLIA for the one system being reviewed had an assessment expiration date of February 2023.

As a result of our review, we determined that this PCA was fully and effectively implemented.

[11] We extended the review period from January through November 2022 because the effects of the updated standard operating procedures would not be fully reflected for PCLIA compliance until four months (120 calendar days from when first e-mail is sent out notifying business unit personnel of expiring PCLIAs) after the standard operating procedures were issued.

Training for Preparers of Rejected Privacy and Civil Liberties Impact Assessments Is Not Enforced or Tracked, and Not All Privacy Controls Have Been Fully Implemented and Assessed

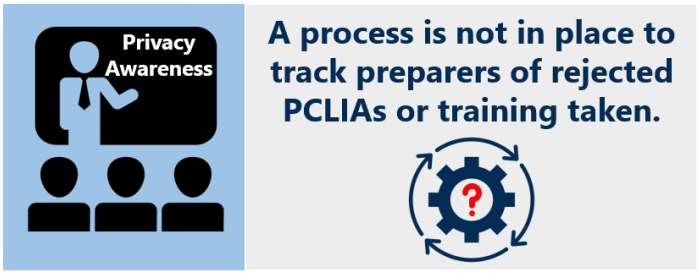
While the IRS fully and effectively implemented the PCAs for four of six recommendations, two PCAs fully implemented were not effective. The training for preparers of rejected PCLIAs is not enforced or tracked, and not all privacy controls have been fully implemented and assessed.

Training for preparers of rejected PCLIAs is not enforced or tracked

We reported previously that the IRS did not make PIAMS-specific training mandatory for PCLIA preparers. The IRS agreed to require preparers of rejected PCLIAs to complete the appropriate privacy awareness training and to update its guidance to reflect this additional requirement.

The IRS submitted standard operating procedures dated November 2020 to support the closure of this PCA. Our review of the procedures determined that they were updated with guidelines on when to reject a PCLIA during the review process. Specifically, the PCLIAs should be rejected for major errors, such as a serious lack of information, incomplete answers, or responses that do not match known facts about the system. When a PCLIA is rejected, the PCLIA preparer is directed to complete the appropriate privacy awareness training prior to resubmitting the assessment per the updated guidance.

We requested from the PGLD Office a list of preparers who submitted PCLIAs that were rejected, along with information of when and what privacy awareness training was taken, for Fiscal Years 2020 and 2021. However, the PGLD Office was unable to provide the information. PGLD Office personnel stated that they do not have a process in place that tracks the preparers of rejected PCLIAs or the training taken to satisfy the requirement. As a result, we determined that while this PCA was fully implemented, the corrective action taken was not effective because a process was not established to identify and track preparers of rejected PCLIAs or the training taken.



Protecting taxpayer privacy and safeguarding PII is a public trust. By not ensuring that preparers of rejected PCLIAs complete the appropriate privacy awareness training, the IRS risks preparers not identifying systems that collect and use PII and not efficiently and properly preparing the PCLIAs as required by law.

Recommendation 1: The Chief Privacy Officer should develop a process to track and ensure that preparers of rejected PCLIAs complete the appropriate privacy awareness training as required.

Management's Response: The IRS agreed with this recommendation. The Chief Privacy Officer will develop a process to track preparers who are required to complete additional training, ensuring the training is completed.

Not all privacy controls have been fully implemented and assessed

We reported previously that the IRS's *Data Breach Response Plan* (May 2018) was not fully integrated with information security continuous monitoring. The IRS agreed that once NIST, SP 800-53, Revision 5, was released, the Information Technology organization's Cybersecurity function would integrate the privacy controls into the security assessments and continuous monitoring methodology.

To assess the effectiveness of the implementation of NIST, SP 800-53, Revision 5, privacy controls, we selected a judgmental sample of 23 of 220 systems from the FISMA Master Inventory List for review. Of the 23 systems selected for review, 15 systems are operating on-premise and eight systems are operating in the cloud. In addition, we identified 96 privacy controls from NIST, SP 800-53, Revision 5, under the responsibility, solely or in part, of the PGLD Office.

On-premise systems

Our review of the privacy controls in the SSP for each of the 15 on-premise systems determined that 911 of 1,440 [96 controls x 15 systems] privacy controls are inherited controls. An inherited control is a control that is implemented at a shared common functionality level and has no system-level responsibility. We did not include inherited privacy controls in our review. Therefore, we reviewed 529 privacy controls.[12] Our review of the SSPs also determined that 388 (73 percent) of 529 privacy controls were not assessed, and only 141 (27 percent) of the privacy controls were assessed during FISMA Year 2022.

Further analysis of the SSPs and assessment documentation for the 141 assessed privacy controls found that:

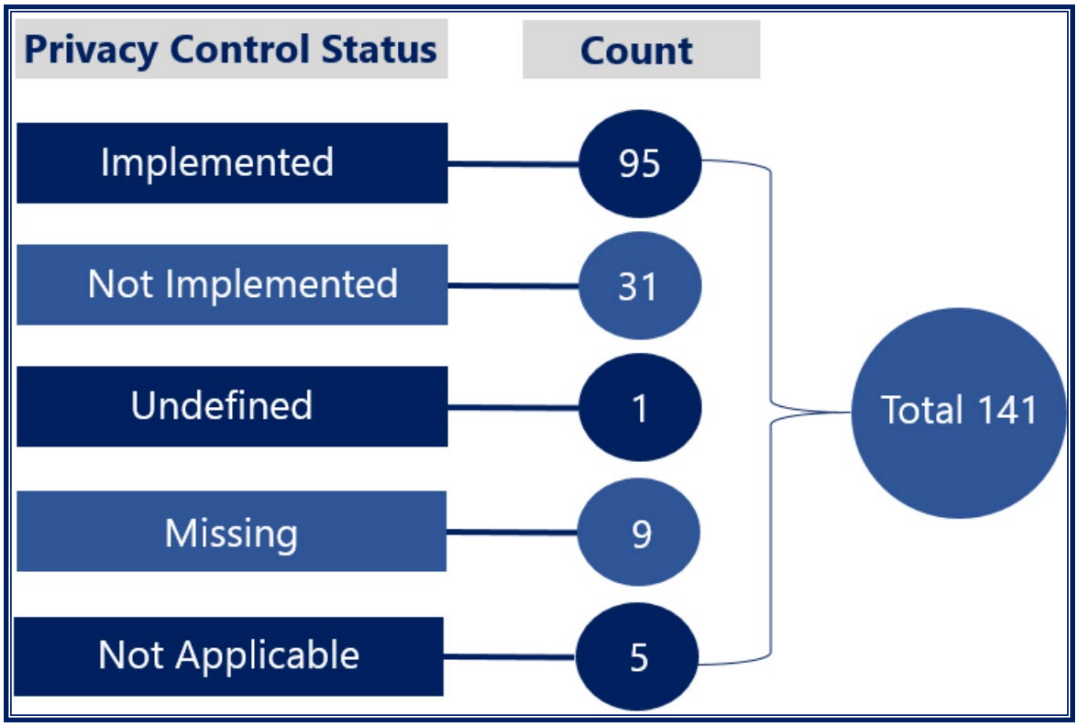
- 95 privacy controls were implemented.
- 41 privacy controls were either not implemented, undefined, or missing.[13]
- 5 privacy controls were not applicable.

Figure 2 presents the results of our analysis for on-premise systems.

[12] Our review of privacy controls included hybrid controls, in which the control is part inherited and part operating at the system level. We reviewed only the portion of the privacy control at the system level.

[13] A control with: a not implemented status is a control that has been assessed and failed; an undefined status is a control that was found to be not assessed; and a missing status is when a control or its status was not included in the SSP.

Figure 2: Status of Privacy Control Assessment for On-Premise Systems



Source: Treasury Inspector General for Tax Administration's analysis of privacy controls between the SSPs and assessment documentation for on-premise systems.

We discussed the results with PGLD Office personnel and they stated that 17 privacy controls with a not implemented status and five privacy controls with a missing status should have been classified as inherited controls. Therefore, 22 of 41 privacy controls were misclassified in the SSPs and should have been identified as inherited controls.

PGLD Office personnel stated that NIST, SP 800-53, Revision 5, privacy controls have not been fully implemented and assessed primarily due to a lack of resources.[14] PGLD Office personnel also stated that as part of FISMA testing, privacy controls are assessed during a three-year cycle, in which only one-third of all controls are assessed each year. FISMA Year 2022 was the first year for implementing and assessing NIST, SP 800-53, Revision 5, privacy controls. In addition, PGLD Office personnel stated that this was also the first year of using a new assessment and monitoring system to capture the results of the privacy control assessments. As a result, not all the privacy controls classified as inherited were correctly applied to all fields in the new assessment and monitoring system and captured in the SSP.

[14] The NIST requires Federal agencies to implement its standards and guidelines within one year of its issuance date.

The Chief Privacy Officer should:

Recommendation 2: Prioritize the implementation of the remaining NIST, SP 800-53, Revision 5, privacy controls not assessed in FISMA Year 2022 to ensure adherence to Federal requirements.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Privacy Officer is currently adding resources to their review teams and will prioritize the privacy controls that they have not assessed in accordance with the overall privacy controls assessment plan.

Recommendation 3: Ensure that all assessed privacy control results are correctly applied to all fields in the new assessment and monitoring system and captured in the SSPs.

> **Management's Response:** The IRS agreed with this recommendation. At the conclusion of FISMA Year 2024 (July 1, 2023, to June 30, 2024), the Chief Privacy Officer will review a sample of SSPs to ensure the correct status for the privacy controls.

Cloud systems

The IRS did not implement and assess NIST, SP 800-53, Revision 5, privacy controls for the eight cloud systems selected for review. This resulted in 768 [96 controls x eight systems] privacy controls that were not implemented and assessed. Cloud systems are required to follow Federal Risk and Authorization Management Program (FedRAMP) guidance, which is still operating under NIST, SP 800-53, Revision 4, *Security and Privacy Controls for Information Systems and Organizations* (Apr. 2013). FedRAMP is a Governmentwide program that promotes the adoption of secure cloud services across the Federal Government by providing a standardized approach to security and risk assessments.

The FedRAMP Program Management Office, which resides within the General Service Administration, is in the process of revising all applicable control baselines for cloud systems to align with NIST, SP 800-53, Revision 5. Cybersecurity function personnel stated that the FedRAMP Program Management Office has delayed the release of the updated control baselines with the latest information that the control baselines would be released by December 2022. As of February 2023, the updated control baselines had not yet been released. According to its website, the FedRAMP Program Management Office has completed developing the draft control baselines and is in the process of updating the baselines based upon public comments, and will then release the final implementation plan. The final implementation plan will include the final version of the updated control baselines, associated documentation and templates, an implementation guide, and a compliance timeline.

As a result, while this PCA was fully implemented, the corrective actions taken were not effective. Failure to fully implement and assess privacy controls exposes PII and tax information on the IRS's on-premise and cloud systems to potential unauthorized access, use, disclosure, disruption, modification, and destruction. In addition, incomplete and inaccurate reporting of privacy control assessments and the status of control implementation may result in unreliable information, which can lead to unidentified weaknesses that are not addressed.

Recommendation 4: The Chief Privacy Officer should ensure that privacy controls for cloud systems are implemented within one year from when updated FedRAMP guidance is approved and released. However, if this is not feasible, the privacy controls should be implemented following the current established continuous monitoring testing plan.

Management's Response: The IRS agreed with this recommendation. Within one year from when the FedRAMP revises the applicable control baselines for cloud systems, the Chief Privacy Officer will assess how the controls are implemented per the continuous monitoring testing plan.

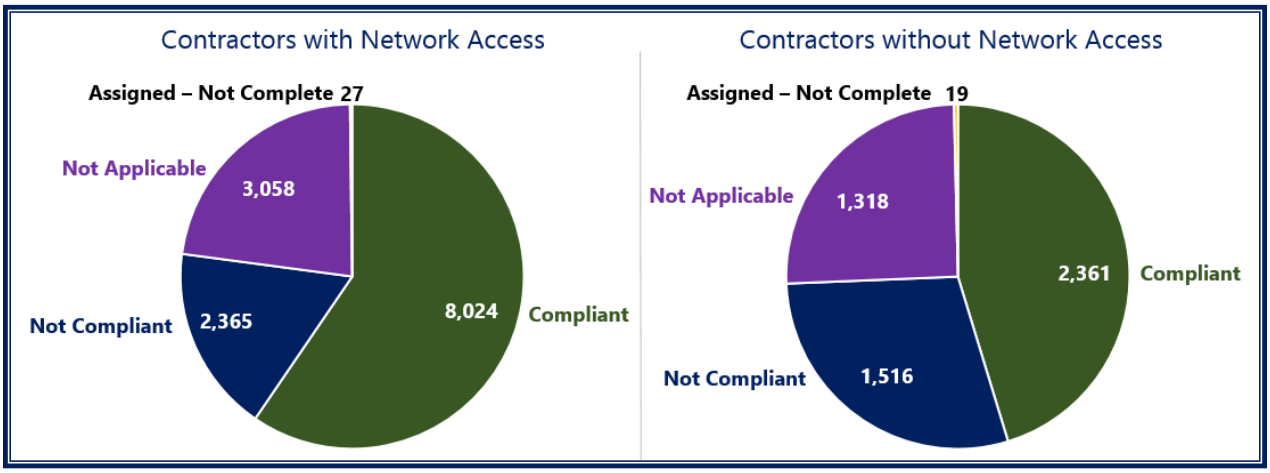
Contractors Did Not Always Complete the Annual Privacy Awareness Training

Our review of a FISMA Year 2022 year-end privacy awareness training compliance report of IRS contractors found that 3,881 (21 percent) of 18,688 contractors have not taken the required annual privacy awareness training. Specifically, 2,365 contractors with network access and 1,516 contractors without network access did not take the privacy awareness training.[15] We also found that 14,807 contractors have taken, are not required to take, or still have time to complete the privacy awareness training.[16] Figure 3 provides the results of our analysis of contractors who have and have not taken the privacy awareness training.

[15] Contractors with network access possess credentials to log onto IRS systems.

[16] The number of contractors are calculated as follows: 10,385 (8,024+2,361) Compliant + 4,376 (3,058+1,318) Not Applicable + 46 (27+19) Assigned – Not Complete. "Assigned – Not Complete" are contractors that had not completed, but still have time to complete, the privacy awareness training.

Figure 3: Privacy Awareness Training Compliance of Contractors with and without Network Access[17]



Source: Treasury Inspector General for Tax Administration's analysis of privacy awareness training compliance report for FISMA Year 2022.

According to *NIST [National Institute of Standards and Technology] Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0* (Jan. 2020), an organization's workforce and third parties engaged in data processing should be provided privacy awareness training. Internal Revue Manual 10.5.1, *Privacy and Information Protection, Privacy Policy* (Feb. 2022), also requires that all personnel, including contractors, complete privacy awareness training requirements annually.

We believe that the large percentage of contractors that have not taken the privacy awareness training is due to lack of management oversight. Cybersecurity function personnel stated that the Deputy Commissioner for Operations Support has begun an initiative to integrate contractor training and monitoring into existing Human Capital Office training operations, such as developing a dashboard for contractors similar to the employee training dashboard. Failure to ensure that contractor privacy awareness training is taken places the IRS at greater risk and could lead to potential mishandling or inadvertent disclosure of PII and taxpayer data.

Recommendation 5: The Human Capital Officer should implement a process to track and monitor compliance with privacy training requirements for all contractors.

Management's Response: The IRS agreed with this recommendation. The Human Capital Officer will implement a process to monitor contractor mandatory briefing completion rates in the same manner as employee mandatory briefing completion rates, by providing business units access to completion status dashboards and reports, and sending automated communications to the contractors and contracting officer's representatives of completion status.

[17] "Not Compliant" are contractors that did not complete the privacy awareness training.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the effectiveness of the implementation of new Federal requirements in the NIST, SP 800-53, Revision 5, and follow up on prior Treasury Inspector General for Tax Administration recommendations. To accomplish our objective, we:

- Determined whether the PCAs for our prior report recommendations have been fully and effectively implemented by reviewing Federal and IRS policies and procedures for closing the PCAs, documentation uploaded to the Joint Audit Management Enterprise System to support the closure of the PCAs, and additional documents to assess whether the PCA effectively corrected the reported deficiencies. We also interviewed PGLD Office and Human Capital Office personnel.
- Determined whether systems that collect and use of PII were properly documented in a PCLIA and included in the PIAMS inventory for a judgmental sample of 39 systems from a population of 456 systems identified in the As-Built Architecture.[1] We selected a judgmental sample because we did not plan to project to the population.
- Determined whether the PGLD Office implemented NIST, SP 800-53, Revision 5, privacy controls for a judgmental sample of 23 systems from a list of 220 FISMA systems that collect and use PII by reviewing the SSPs and assessment documentation. We selected a judgmental sample because we did not plan to project to the population.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's Cybersecurity function located at the New Carrollton Federal Building in Lanham, Maryland, and the PGLD Office and Human Capital Office located at the IRS Headquarters in Washington, D.C., during the period April 2022 through March 2023. 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.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Louis Lee, Director; Kanika Kals, Acting Audit Manager; Daniel Preko, Acting Audit Manager; Jason Rosenberg, Acting Audit Manager; Benedict Kim, Lead Auditor; and Danielle Synnestvedt, Senior Auditor.

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

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: NIST, SP 800-53, Revision 5; FedRAMP guidance; and IRS policies and procedures related to PCA closure, privacy awareness training requirements, implementing privacy controls, and PII collection and use management. We evaluated these controls by interviewing Cybersecurity function personnel as well as PGLD Office and Human Capital Office personnel. We also reviewed relevant documentation.

Appendix II

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Protection of Resources – Potential; 1,197 privacy controls were not assessed or had a status of not implemented, undefined, or missing (see Recommendations 2 and 4).

Methodology Used to Measure the Reported Benefit:

Our review of the privacy controls in the SSP for each of 15 on-premise systems determined that 911 of 1,440 [96 controls x 15 systems] privacy controls are inherited controls. We did not review the inherited privacy controls. Therefore, we reviewed 529 privacy controls.[1]

Our review of the SSPs also determined that **388** (73 percent) of 529 privacy controls were not assessed and only 141 (27 percent) of the privacy controls were assessed during FISMA Year 2022. Further analysis of the SSPs and assessment documentation for the 141 assessed privacy controls found that **41** privacy controls were either not implemented, undefined, or missing.[2]

In addition, the IRS did not implement and assess NIST, SP 800-53, Revision 5, privacy controls for the eight cloud systems selected for review. This resulted in **768** [96 controls x eight systems] privacy controls that were not implemented and assessed.

In total, 1,197 [388+41+768] privacy controls were not assessed or had a status of not implemented, undefined, or missing.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 22 privacy controls were misclassified and should have been identified as inherited controls in the SSPs (see Recommendation 3).

Methodology Used to Measure the Reported Benefit:

Our analysis of the SSPs and assessment documentation for the 141 privacy controls assessed during FISMA Year 2022 found that 41 privacy controls were either not implemented, undefined, or missing. We discussed the results with PGLD Office personnel and they stated that 17 privacy controls with a not implemented status and five privacy controls with a missing status should

[1] Our review of privacy controls included hybrid controls, in which the control is part inherited and part operating at the system level. We reviewed only the portion of the privacy control at the system level.

[2] A control with: a not implemented status is a control that has been assessed and failed; an undefined status is a control that was found to be not assessed; and a missing status is when a control or its status was not included in the SSP.

have been classified as inherited controls. Therefore, 22 of 41 privacy controls were misclassified and should have been identified as inherited controls.

Appendix III

Management's Response to the Draft Report

CHIEF PRIVACY OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

May 25, 2023

MEMORANDUM FOR HEATHER M. HILL
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kathleen E. Walters
Chief Privacy Officer

SUBJECT: Draft Audit Report - Actions Have Been Taken to Improve the Privacy Program; However, Some Privacy Controls Have Not Been Fully Implemented and Assessed (Audit # 202220003)

Thank you for the opportunity to respond to the above-referenced draft audit report. The IRS continues to prioritize the protection of taxpayer information and strives daily to improve our processes so that the confidence of the public is maintained.

Protecting taxpayer information requires coordination throughout the IRS. In an environment that is rapidly transitioning to digital content, it is critical that IRS Information Technology (IT) and the Privacy, Governmental Liaison and Disclosure (PGLD) organization work together to safeguard taxpayer information. An example of this coordination is the implementation of the National Institute of Standards and Technology (NIST) security and privacy controls as defined in Special Publication 800-53 revision 5. Finalized in late 2020, the security and privacy controls provide a roadmap for implementing and assessing systems. The IRS developed a plan to integrate IT and PGLD resources to assess systems on a continuous basis to ensure compliance with the NIST standards.

While the IRS has planned to fully access all systems to include cloud environments, a lack of resources in the last few years prevented the IRS from fully assessing the privacy controls on all systems, as noted in your draft report. To maximize the effectiveness of available resources, the IRS focused on major systems that contained the bulk of the sensitive information maintained by the IRS. In light of the additional funding the IRS received in August 2022 and recognizing the importance of assessing the privacy controls, additional resources have been allocated to the privacy program and we anticipate that we will be able to fully assess all systems in calendar year 2024. We therefore agree with all recommendations included in the draft report. We do not have any concerns with Outcome Measures as noted in Appendix II of the draft report.

Protecting privacy is not an end state, rather it is an ever evolving mandate that is foundational to everything we do at the IRS. Privacy principles are built into every system we operate and in every process our employees use to interact with taxpayers. Our unwavering commitment to taxpayers is that we will continue to place the upmost importance on protecting their information.

If you have any questions, please contact me at 202-317-4082, or a member of your staff may contact Peter C. Wade, Director Privacy Policy and Compliance, at 470-639-3479.

Attachment
TIGTA Audit 202220003

Recommendation 1: The Chief Privacy Officer should develop a process to track and ensure that preparers of rejected PCLIAs complete the appropriate privacy awareness training as required.

Corrective Action: The IRS agrees with the recommendation and will develop a process to track preparers who are required to complete additional training, ensuring the training is completed.

Implementation Date: December 15, 2023

Responsible Official(s): Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Director, Privacy Policy and Compliance

Recommendation 2: The Chief Privacy Officer should prioritize the implementation of the remaining NIST, SP 800-53, Revision 5, privacy controls not assessed in FISMA Year 2022 to ensure adherence to Federal requirements.

Corrective Action: The IRS agrees with this recommendation. We are currently adding additional resources to our review teams and will prioritize the privacy controls that we have not assessed in accordance with the overall privacy controls assessment plan.

Implementation Date: July 31, 2024

Responsible Official(s): Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Director, Privacy Policy and Compliance

Recommendation 3: The Chief Privacy Officer should ensure that all assessed privacy control results are correctly applied to all fields in the new assessment and monitoring system and captured in the SSPs.

Corrective Action: The IRS agrees with this recommendation. At the conclusion of the Federal Information Security and Modernization Act (FISMA) 2024 cycle we will review a sample of system security plans (SSPs) to ensure the correct status for the privacy controls.

Implementation Date: August 31, 2024

Responsible Official(s): Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Director, Privacy Policy and Compliance

Recommendation 4: The Chief Privacy Officer should ensure that privacy controls for cloud systems are implemented within one year from when updated FedRAMP guidance is approved and released. However, if this is not feasible, the privacy controls should be implemented following the current established continuous monitoring testing plan.

Corrective Action: The IRS agrees with this recommendation. Within one year from when the Federal Risk and Authorization Management Program (FedRAMP) revises the applicable control baselines for cloud systems we will assess how the controls are implemented per the continuous monitoring testing plan.

Implementation Date: June 30, 2025

Responsible Official(s): Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Director, Privacy Policy and Compliance

Recommendation 5: The Human Capital Officer should implement a process to track and monitor compliance with privacy training requirements for all contractors.

Corrective Action: The IRS agrees with this recommendation. The Human Capital Officer will implement a process to monitor contractor mandatory briefing completion rates in the same manner as employee mandatory briefing completion rates, by providing Business Units access to completion status dashboards and reports, and sending automated communications to the contractors and Contracting Officer's Representatives of completion status.

Implementation Date: October 15, 2023

Responsible Official(s): Chief Learning Officer, HCO

Appendix IV

Glossary of Terms

Term	Definition
Baseline	The set of controls that are applicable to information or an information system to meet legal, regulatory, or policy requirements as well as address protection needs for the purpose of managing risk.
Cloud System	A system based upon a model for enabling on-demand network access to a shared pool of configurable information technology capabilities and resources, *e.g.*, networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Cybersecurity Function	A function within the IRS Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Integrated Talent Management System	One system that consolidates several human resource systems and includes four primary human resource management modules: Learning; Performance Management; Succession Planning; and Workforce Planning.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
On-Premise System	Runs on computers on the premises of the organization using the software, rather than at a remote facility such as a cloud.
Personally Identifiable Information	Information that, either alone or in combination with other information, can be used to uniquely identify an individual. Examples of PII include name, Social Security Number, date of birth, place of birth, address, and biometric record.
Privacy and Civil Liberties Impact Assessment	An analysis of how information in an identifiable form is collected, stored, protected, shared, and managed. The process also provides a means to assure compliance with all applicable laws and regulations governing taxpayer and employee privacy.
Privacy Impact Assessment Management System	A series of web pages that supports the performance, documentation, and management of PCLIAs. It serves as the central repository for all PCLIAs.
Sensitive But Unclassified	Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 U.S.C. § 552a (the Privacy Act of 1974), which could result from inadvertent or deliberate disclosure, alteration, or destruction.

Term	Definition
System Security Plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Appendix V

Abbreviations

FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
PCA	Planned Corrective Action
PCLIA	Privacy and Civil Liberties Impact Assessment
PGLD	Privacy, Governmental Liaison and Disclosure
PIAMS	Privacy Impact Assessment Management System
PII	Personally Identifiable Information
SP	Special Publication
SSP	System Security Plan

To report fraud, waste, or abuse,
contact our hotline on the web at www.tigta.gov or via e-mail at oi.govreports@tigta.treas.gov.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at www.tigta.gov/form/suggestions.

Information you provide is confidential, and you may remain anonymous.