TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Some Components of the Privacy Program Are Effective; However, Improvements Are Needed

September 20, 2019

Reference Number: 2019-20-062

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

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

SOME COMPONENTS OF THE PRIVACY PROGRAM ARE EFFECTIVE; HOWEVER, IMPROVEMENTS ARE NEEDED

Highlights

Final Report issued on September 20, 2019

Highlights of Reference Number: 2019-20-062 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

An increased number of security breaches nationwide involving Personally Identifiable Information has contributed to the loss of millions of records over the past few years. Breaches involving Personally Identifiable Information are hazardous to both individuals and organizations and may result in identity theft, embarrassment, blackmail, loss of public trust, legal liability, or remediation costs.

WHY TIGTA DID THE AUDIT

One of the goals of the IRS's privacy program is to use assessments to limit Personally Identifiable Information collections to the least amount necessary to conduct its mission and so the agency may limit potentially negative consequences in the event of a data breach involving this sensitive information. This audit was initiated to determine the maturity level of the IRS's privacy program and to follow up on recommendations from a prior TIGTA audit report.

WHAT TIGTA FOUND

The IRS uses Privacy and Civil Liberties Impact Assessments to categorize and minimize the use of Personally Identifiable Information. However, the IRS does not have a complete inventory showing what systems currently contain or use Personally Identifiable Information.

While the assessment process is used to identify privacy risks for systems, the IRS has not fully integrated a continuous monitoring solution between the Cybersecurity function and the Privacy office that incorporates privacy and data breach response to provide ongoing, near real-time monitoring of privacy risks.

The IRS requires assessment updates every three years or sooner for new privacy risks. Our review determined that at the end of Fiscal Year 2018, 37 (21 percent) of the 173 assessments due to expire were not updated timely.

Finally, not all IRS employees were taking the mandatory privacy awareness training, and assessment preparers were not adequately trained.

WHAT TIGTA RECOMMENDED

TIGTA made six recommendations, including that the Chief Privacy Officer develop and maintain an inventory of the collection and use of Personally Identifiable Information; the Chief Information Officer implement a fully integrated information security continuous monitoring process that includes privacy risks; and the Chief Privacy Officer strengthen enforcement of the mandatory assessment review process by escalating expired assessments to management and make improvements to the privacy training program.

The IRS agreed with five of the six recommendations and partially agreed with one. The IRS stated that it recently created an inventory and can generate a current inventory when needed. The IRS plans to analyze the escalation process and revise as necessary to ensure that Privacy, Governmental Liaison, and Disclosure Office management is involved in the process; remind all IRS managers to ensure that employees have completed training; analyze the training courses and update as needed; and update guidance to require preparers of rejected Privacy and Civil Liberties Impact Assessments to complete the appropriate training.

The IRS partially agreed to implement a fully integrated information security continuous monitoring process that includes privacy risks, but will wait for further guidance to be finalized. TIGTA cited existing guidance already available to help incorporate privacy risks into the IRS information security continuous monitoring program.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 20, 2019

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Some Components of the Privacy Program Are Effective; However, Improvements Are Needed (Audit # 201720002)

This report presents the results of our review was to determine the maturity level of the privacy program and to follow up on recommendations from a prior Treasury Inspector General for Tax Administration audit report. The Consolidated Appropriations Act of 2005, Section 522,[1] requires the Inspector General to evaluate the agency's use of information in identifiable form and the privacy and data protection procedures. This review is included in our Fiscal Year 2019 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of Internal Revenue Service Resources.

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

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

[1] Pub. L. No. 108-447, 188 Stat. 2813, 5 U.S.C. 522a.

Table of Contents

Abbreviations

FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IRS	Internal Revenue Service
PCLIA	Privacy and Civil Liberties Impact Assessment
PGLD	Privacy, Governmental Liaison, and Disclosure Office
PIAMS	Privacy Impact Assessment Management System
PII	Personally Identifiable Information
TIGTA	Treasury Inspector General for Tax Administration

Background

The Internal Revenue Service (IRS) is responsible for ensuring the privacy, confidentiality, integrity, and availability of taxpayer and employee information. The Privacy, Governmental Liaison, and Disclosure (PGLD) office has overall responsibility for privacy issues. The Privacy Act of 1974[1] and the E-Government Act of 2002[2] provide guidance on:

- What personal information the Federal Government can collect about private individuals.
- How that information can be used.
- Requiring agencies to conduct privacy assessments that examine the risks and ramifications of using information technology to collect, maintain, and disseminate information in an identifiable form, such as Social Security Numbers, of members of the public and agency employees.

An agency's privacy assessments are designed to limit Personally Identifiable Information (PII)[3] collections to the least amount necessary to conduct its mission and so the agency may limit potential negative consequences in the event of a data breach involving PII. According to the Government Accountability Office, the increased number of security breaches involving PII has contributed to the loss of millions of records nationwide over the past few years.[4] Breaches involving PII are hazardous to both individuals and organizations. Individual harms may include identity theft, embarrassment, or blackmail. Organizational harms may include a loss of public trust, legal liability, or remediation costs. To appropriately protect the confidentiality of PII, the Consolidated Appropriations Act of 2005[5] 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 to evaluate the agency's use of information in identifiable form and the privacy and data protection procedures every two years.

In November 2013, the Department of the Treasury (hereafter referred to as the Treasury Department) issued guidance that expanded the scope of these privacy assessments to include questions about civil liberties.[6] Privacy and Civil Liberties Impact Assessments (PCLIA) are necessary to ensure that the Chief Privacy Officer is capable of gathering the information necessary to conduct the required privacy and civil liberties oversight. The IRS uses the online

[1] Pub. L. No. 93-579, 88 Stat. 1896, 5 U.S.C. § 552a.
[2] Pub. L. No. 107-347, 116 Stat. 2899, sec. 208.
[3] See Appendix IV for a glossary of terms.
[4] Government Accountability Office, GAO-08-343, *Protecting Personally Identifiable Information* (Jan. 2008).
[5] Pub L. No. 108-447, 118 Stat. 2268, 5 U.S.C. 522a
[6] Treasury Department, Treasury Directive Publication 25-07, *Privacy and Civil Liberties Impact Assessment Manual* (Nov. 2013).

Privacy Impact Assessment Management System (PIAMS) as a central repository for the creation and management of the PCLIAs. The PIAMS is comprised of a series of web pages that allow employees to input required PCLIAs online and provides PGLD office analysts with a centralized system to track and perform quality reviews.

In Fiscal Year (FY) 2015, we reported[7] that training and PIAMS system enhancements were needed. We recommended that the IRS:

- Provide training to stakeholders involved in the privacy assessment process.
- Revise policy for removal and deletion of the PCLIAs from the IRS public website.

The IRS and all Federal agencies are required to report metrics on their privacy program and PCLIA process annually in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).[8] The FISMA requires each agency Inspector General to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices, including the privacy program, of its respective agency. The FY 2018 *FISMA Reporting Metrics* evaluated the five function areas of the Cybersecurity Framework that are: Identify, Protect, Detect, Respond, and Recover. Figure 1 describes the five FISMA maturity levels used to evaluate the effectiveness of privacy programs.

Figure 1: FISMA Evaluation Maturity Levels

Maturity Level	Description
Level 1: *Ad-hoc*	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: *Managed and Measureable*	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: *Optimized*	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business needs.

Source: FY 2018 Inspector General FISMA Reporting Metrics.

[7] Treasury Inspector General for Tax Administration (TIGTA), Ref. No. 2015-20-079, *Stronger Access Controls and Further System Enhancements Are Needed to Effectively Support the Privacy Impact Assessment Program* (Sept. 2015).

[8] Pub. L. No. 113-283, 128 Stat. 30733. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

In September 2018, we rated the IRS Data Protection and Privacy program at Maturity Level 2 (*Defined*), which means policies, procedures, and strategy are formalized and documented but not consistently implemented.[9] We found that the IRS did not:

- Provide evidence to show that it reviews and removes unnecessary PII collections on a regular basis.
- Meet the *Consistently Implemented* maturity level because it is not checking outbound communications to detect encrypted exfiltration of information.
- Provide evidence to show that it updates its privacy program as a result of training exercises.

This review was performed with information obtained from the PGLD office in Philadelphia, Pennsylvania, during the period September 2018 through June 2019. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[9] TIGTA, Ref. No. 2018-20-082, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Sept. 2018).

Results of Review

There Is No Complete Inventory of Systems That Maintain Personally Identifiable Information

In accordance with FY 2018 FISMA metrics, we evaluated the PGLD office privacy program and determined it was operating at Maturity Level 2 (*Defined*). The PGLD office communicated the privacy program and related policies and procedures for the protection of PII that is collected, used, maintained, shared, and/or disposed by its information systems. The FISMA, however, considers Maturity Level 4 (*Managed and Measureable*) as an effective level of security for Federal agencies. The PGLD office established roles and responsibilities for the effective implementation of the organization's privacy program and determined the resources and optimal governance structure needed to implement its privacy program effectively. To comply with applicable laws and regulations governing privacy, system owners or designees are required to submit the PCLIAs through the PIAMS. However, while the PCLIA process allows the IRS to categorize, minimize, and apply the appropriate safeguards regarding the use of PII, the IRS does not have an effective inventory of the systems that contain or use PII.

According to the National Institute of Standards and Technology,[10] organizations should identify all PII residing in their environment because an organization cannot properly protect PII it does not know about, and[11] organizations should take due care to update the inventories by identifying linkable data that could create PII. A best practice of gathering information for PII inventories includes extracting the following information from the PCLIAs for information systems containing PII:

- Name and acronym for each system identified.
- Types of PII contained in that system.
- Classification of level of sensitivity of all types of PII, as combined in that information system.
- Classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed.

[10] National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (Apr. 2010).
[11] National Institute of Standards and Technology Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).

According to PGLD office officials, in Calendar Year 2014, the Treasury Department requested an inventory of PII from the PGLD office. However, the inventory provided has not been maintained or updated.

An inventory of systems containing PII would allow the PGLD office and the Cybersecurity function to know which systems could affect the public in the event of a breach. An inventory could also support the *Data Breach Response Plan* efforts to help identify which systems and PII are affected by a particular breach. Without a PII inventory, an organization might struggle to implement effective administrative, technical, and physical security policies and procedures to protect PII and to mitigate risks of PII exposure.

The PGLD office does not actively review PII collections on a regular basis to remove unnecessary PII. The PGLD office relies on the business operating divisions to conduct reviews of the PCLIAs in the PIAMS every three years to ensure that the information is current, to identify and remove unnecessary PII collections, and to meet FISMA requirements. These PCLIAs are collected in the PIAMS, but we determined that the PIAMS itself is not a complete PII inventory of systems that currently contain or use PII that aligns with National Institute of Standards and Technology inventory guidance.

Recommendation

Recommendation 1: The Chief Privacy Officer should develop and maintain an inventory of the collection and use of PII in IRS systems.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS agreed with the importance of having the ability to produce an inventory of systems that contain and use PII. The IRS stated it recently created such an inventory using the PIAMS and instituted a capability in the PIAMS that will allow the IRS to generate a current inventory at any point it is needed.
>
> ***Office of Audit Comment:*** During audit fieldwork, the IRS did not have an inventory of systems that contain PII. The IRS also did not provide us with the inventory or demonstrate the capability mentioned in its response.

The Data Breach Response Plan Is Not Fully Integrated With Information Security Continuous Monitoring Efforts

The PGLD office monitors and analyzes quantitative performance metrics for the effectiveness of its *Data Breach Response Plan*, such as total number of breaches and median cycle time from breach to sending a data loss notification letter. The PGLD office ensures that data supporting privacy performance metrics are obtained accurately, consistently, and in a reproducible format. The IRS conducts annual tabletop exercises of the *Data Breach Response Plan* to practice a coordinated response to a breach to further refine and validate the plan and to

identify potential weaknesses. The PGLD office also tracks performance metrics as part of the annual tabletop exercise, such as internal communication processes, third-party response procedures, and the overall effectiveness of the breach response exercise. In FY 2018,[12] we reported that the privacy program's *Data Breach Response Plan* was operating at the FISMA Maturity Level 4 (*Managed and Measurable*), which is considered an effective level of security.

While the *Data Breach Response Plan* was operating at an effective level in FY 2018, a FISMA Level 5 (*Optimized*) maturity requires a fully integrated continuous monitoring solution between the Cybersecurity function and the PGLD office that incorporates privacy and data breach response to provide ongoing, near real-time monitoring of privacy risks. Because information security continuous monitoring is a security control, the Cybersecurity function is primarily responsible for its development. Cybersecurity function officials stated that privacy and security are two separate but parallel data processes that are not fully coordinated within the IRS.

When a breach is identified, an e-mail is sent to the PGLD office and a breach response team is assembled to assess the severity of the risk; however, continuous monitoring technology is not available to be used by the PGLD office to determine the location and nature of the breach. The PGLD office reported that the number of data loss breaches in FY 2017 and FY 2018 were 3,348 and 3,373, respectively. It currently takes 19 calendar days to notify individuals affected by a breach. The implementation of continuous monitoring of privacy risks would assist the PGLD office's ability to dynamically identify and measure the security implications for privacy and breach response, and more timely notify breach victims.

The Cybersecurity function has ownership of the Information Security Continuous Monitoring program, but it is necessary for the PGLD office to collaborate with the Cybersecurity function to implement a coordinated continuous monitoring strategy that includes privacy risks. According to PGLD office executives, the PGLD office plans to collaborate extensively with the Cybersecurity function on information security continuous monitoring when the National Institute of Standards and Technology Special Publication 800-53 is revised. The revised version is expected to include a new continuous monitoring control for joint monitoring of security and privacy controls. Further collaboration efforts would allow the IRS to achieve FISMA Maturity Level 5 (*Optimized*).

The Calendar Year 2019 *IRS Information Security Continuous Monitoring Program Plan*[13] states that in the event of the loss or theft of an information technology asset, the Cybersecurity function sends a summary notification to the PGLD office. The plan also states that the PGLD office relies upon the Cybersecurity function for lost or stolen information technology assets

[12] TIGTA, Ref. No. 2018-20-082, *Federal Information Security Modernization Act Report for Fiscal Year 2018* (Sept. 2018).
[13] IRS, *IRS Information Security Continuous Monitoring Program Plan* (June 2019).

only; all other incidents are reported online and automatically uploaded into the E-trak system.[14] The E-trak system is used to input and track incidents of disclosures, losses, and thefts and has no systemic monitoring capability. However, until the Information Security Continuous Monitoring program is fully integrated between the Cybersecurity function and the PGLD office, the PGLD office is unable to monitor controls on an ongoing basis or assess its effectiveness against internal or external threats to privacy in its environment.

According to the FISMA,[15] an organization's *Data Breach Response Plan* should be integrated with other areas such as incident response, risk management, continuous monitoring, continuity of operations, and other business areas, as appropriate. Furthermore, the organization should employ automation to monitor potential privacy incidents and take immediate action to mitigate the incident and provide protection to the affected individuals. In addition, the Office of Management and Budget[16] states that while security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identify and manage security and privacy risks and comply with applicable requirements.

Recommendation

Recommendation 2**:** The Chief Information Officer should implement a fully integrated information security continuous monitoring process that includes privacy risks.

> ***Management's Response:*** The IRS partially agreed with this recommendation. While the PGLD office and the Cybersecurity function continue to work to determine the optimal maturity level, once National Institute of Standards and Technology Special Publication 800-53 Revision 5 is finalized, the Cybersecurity function will integrate the privacy-related security controls, enhancements, and objectives, as recommended by the publication, into security assessments and continuous monitoring methodology.
>
> ***Office of Audit Comment:*** Existing guidance in both the FISMA and the National Institute of Standards and Technology Special Publication 800-137[17] is already available to begin this work. These documents provide guidance for information security continuous monitoring strategy and program implementation that can be used to incorporate privacy risks without further delay.

[14] The E-trak system is a web-based document tracking application that assists IRS leadership and business operating divisions to timely and effectively manage their responses to issues raised by taxpayers, IRS employees, the Government Accountability Office, TIGTA, and others.
[15] FISMA, *FY 2018 Inspector General FISMA Reporting Metrics* (May 2018).
[16] Office of Management and Budget, *Circular A-130 Managing Federal Information as a Strategic Resource* (July 2016).
[17] National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (Sept. 2011).

Some Privacy and Civil Liberties Impact Assessments Are Not Being Reassessed Timely

The PGLD office relies on the business operating divisions to conduct reviews of the PCLIAs in the PIAMS every three calendar years to ensure that the information is current, and to identify and remove unnecessary PII collections. We determined the PIAMS contained 441 system PCLIAs at the end of FY 2018. Of these PCLIAs, 173 (39 percent) were due to expire by the end of FY 2018. Of these 173 PCLIAs due to expire, we determined that:

- 123 (71 percent) were updated timely.
- 37 (21 percent) were not updated timely.
- 13 (8 percent) were retired.

The IRS requires PCLIA updates every three calendar years or sooner for new privacy risks due to a major system change.[18] The PIAMS generates automated notifications to system owners of upcoming PCLIA expirations at 90-, 60-, and 30-calendar days before the PCLIA expires. However, there are no formal procedures to elevate the expired PCLIAs to system owner management. PGLD office officials stated that PCLIA preparation should be a collaborative team process that uses subject matter experts to answer system specific questions, and that the system owner alone should not complete the PCLIA. By not ensuring that systems remain current, the IRS cannot ensure that protections for privacy and other civil liberties are being enforced on its systems that collect and disseminate PII.

According to the PGLD Standard Operating Procedure for expiring PCLIAs, after the 90-, 60-, and 30-calendar day e-mails, privacy analysts and managers can follow up with an e-mail and call for possible elevation.[19] If the PGLD office does not receive a response from a system owner after seven calendar days, a PGLD office analyst reaches out to alternative points of contact to work on the expiring PCLIA. Ultimately, the system owner has responsibility for PCLIA preparation and maintenance. PCLIA preparation should be a collaborative team process with system technical experts, business process experts, and the PGLD office. The mandatory review of the PCLIAs is part of the E-Government Act of 2002 with a privacy objective that complements the *National Strategy to Secure Cyberspace*.[20] As the National Strategy indicates, security programs that strengthen protections for privacy and other civil liberties, together with strong privacy policies and practices in Federal agencies, will ensure that information is handled in a manner that maximizes both privacy and security.

[18] Internal Revenue Manual 10.5.2, *Privacy and Information Protection, Privacy Compliance and Assurance Program* (Dec. 2016).
[19] IRS, *PCLIA 3-Year Review Expiring Report Standard Operating Procedure* (2018).
[20] Executive Office of the President of the U.S., *The National Strategy to Secure Cyberspace* (2003).

Recommendation

Recommendation 3**:** The Chief Privacy Officer should ensure that the PGLD office strengthens its enforcement of the mandatory PCLIA review process by escalating expired PCLIAs to management for immediate attention or move to take the system offline.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS agreed that reviewing processes to ensure that they remain the most efficient is essential to a healthy privacy program. In order to ensure that all necessary actions are in progress to update the PCLIAs, the IRS will analyze the escalation process in the internal procedures and revise as necessary to ensure that PGLD office management is involved in the process.

The Privacy Training Program Needs Improvement

Some employees did not take the mandatory privacy awareness training

PGLD office officials stated that the privacy awareness training is administered on an annual basis. Adjustments to the annual training program are made at the beginning of each year before being added to the Enterprise Learning Management System. Although the IRS provides training to employees, it does not ensure that all employees have taken the training. In FY 2018, the Human Capital Office identified 88,410 instances in which employees were required to take the mandatory privacy awareness training. However, based on a comparison of the Human Capital Office list of full-time and full-time seasonal employees and those who completed the mandatory privacy awareness training in FY 2018, we found 468 employees delinquent in completing the mandatory training by more than 80 calendar days. We also found 1,313 individuals who completed the training but were not included in the initial list of 88,410 employees required to take the mandatory privacy awareness training.

The IRS does not ensure that all active employees complete the annual privacy awareness training. While the Internal Revenue Manual states that the PGLD office is responsible for implementing privacy awareness training, PGLD office officials stated that it is the business operating division's responsibility to ensure that their employees take the training. The business operating division uses notifications from the Enterprise Learning Management System to track individuals who need to take required training. The Enterprise Learning Management System will send notifications to students and their managers 14 and seven calendar days prior to the required due date and every seven calendar days after the required due date has passed until the training component is removed or completed. PGLD office and business unit managers do not always follow up as needed to ensure that annual privacy awareness training is received. The PGLD office also stated that seasonal workers are a challenge because the training starts in July after most of the seasonal workers are no longer employed.

The Internal Revenue Manual states all employees and contractors must complete annual and role-based training, information protection, and disclosure training requirements.[21] According to the IRS Privacy Program Plan, the Chief Privacy Officer is responsible for implementing and managing privacy policies and creating awareness. The plan also states that the PGLD office is responsible to provide outreach, education, training, and reports promoting privacy, records, and disclosure priorities. The mandatory privacy awareness training educates employees on privacy principles. Protecting taxpayer privacy and safeguarding confidential tax information is a public trust. By not ensuring that all employees complete the mandatory privacy awareness training, the IRS cannot maintain the public's trust for safeguarding taxpayer information.

PCLIA preparers are not adequately trained

In our FY 2015 report, we recommended that the PGLD office provide training to stakeholders involved in the assessment process to ensure that no sensitive information is documented in the assessments. In Calendar Year 2015, the PGLD office developed Course 61760 "*Privacy Training for Privacy & Civil Liberties Impact Assessment Preparers,*" and Course 61922 "*Privacy Training for Adaptive Privacy Impact Assessment Preparers.*" Both training courses provide an overview of the PIAMS. These PIAMS courses, however, have not been updated since their implementation even though the system itself has undergone several enhancements. The IRS stated that these courses were not updated due to a lack of resources.

In addition, the IRS has not made PIAMS-specific courses mandatory for PCLIA preparers. We found that of the 117 rejected PCLIAs we reviewed, 102 (87 percent) submitting employees did not take Course 61760 and 110 (94 percent) had not taken Course 61922. We also found one employee who took one of the training courses and still had five rejected PIAMS submissions.

The Internal Revenue Manual establishes the privacy framework for privacy compliance and assurance programs and activities, and states that specific responsibilities apply to the roles of individuals who prepare, maintain, and approve the PCLIAs.[22]

Recommendations

The Chief Privacy Officer should ensure that the PGLD office:

Recommendation 4**:** Coordinates with the business operating divisions to ensure that all employees take the annual privacy awareness training as required.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS agreed that annual privacy awareness training is essential for a healthy privacy program. The PGLD office will issue a Service-wide Leaders Alert communication prior to the

[21] Internal Revenue Manual 10.5.1, *Privacy and Information Protection, Privacy Policy* (Mar. 2018).
[22] Internal Revenue Manual 10.5.2, *Privacy and Information Protection, Privacy Compliance and Assurance Program* (Dec. 2016).

training completion date reminding managers to ensure that all of their employees have completed the training.

Recommendation 5***:*** Updates and maintains PIAMS training courses to capture PIAMS enhancements.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will complete an analysis of Course 61760 "*Privacy Training for Privacy & Civil Liberties Impact Assessment Preparers"* and Course 61922 "*Privacy Training for Adaptive Privacy Impact Assessment Preparers*" to determine if changes are needed and then implement the changes to the courses.

Recommendation 6: Makes completion of PIAMS training courses mandatory for preparers of rejected PCLIAs.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS agreed that preparers of rejected PCLIAs should be required to complete the appropriate training. The IRS will update its guidance to reflect this additional step.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine the maturity level of the privacy program and to follow up on recommendations from a prior Treasury Inspector General for Tax Administration (TIGTA) audit report.[1] To accomplish our objective, we:

I. Determined the maturity level of the privacy program.

   A. Obtained and reviewed information regarding the privacy program for the protection of PII that is collected, used, maintained, shared, and disposed of by information systems.

   B. Determined the effectiveness of the *Data Breach Response Plan*[2] to respond to privacy events.

   C. Determined whether privacy awareness training is provided to all individuals, including role-based privacy training.

II. Determined whether the planned corrective actions for TIGTA Audit Report 2015-20-079 recommendations have been effectively implemented.

   A. Requested from TIGTA's Management Planning and Workforce Development Division the Form 13872, *Planned Corrective Action Status Update for TIGTA and other Reports*, and any supporting documents for the closed planned corrective actions.

   B. Evaluated the effectiveness of the planned corrective actions regarding training available to PIAMS users.

   C. Evaluated the implementation of the planned corrective actions for ensuring adequate review and replacement of expired PCLIAs.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: IRS policies, procedures, and processes for PCLIA preparation and reporting, privacy training, data breach incident response,

[1] TIGTA, Ref. No. 2015-20-079, *Stronger Access Controls and Further System Enhancements Are Needed to Effectively Support the Privacy Impact Assessment Program* (Sept. 2015).
[2] See Appendix IV for the glossary of terms.

and handling of PII. We reviewed the e-Government Act 2002,[3] the Privacy Act of 1974,[4] and the FISMA Inspector General Metrics and evaluated IRS processes against these standards. We evaluated these controls by interviewing management officials and reviewing standard operating procedures, training records, and data breach response documentation.

[3] Pub. L. No. 107-347, 116 Stat. 2899, sec. 208.
[4] Pub. L. No. 93-579, 88 Stat. 1896, 5 U.S.C. § 552a.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Jena Whitley, Director
Myron Gulley, Audit Manager
Corey Brown, Lead Auditor
Kasey Koontz, Senior Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Chief Information Officer
Chief Privacy Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Director, Privacy and Policy Compliance
Director, Enterprise Audit Management

Appendix IV

Glossary of Terms

Term	Definition
Cybersecurity Function	Responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Data Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence in which a person other than an authorized user accesses or potentially accesses PII, or an authorized user accesses or potentially accesses PII for other than an authorized purpose.
Data Breach Response Plan	Outlines the methodology the IRS will use to categorize breaches and determine the appropriate response based on guidance.
Federal Information Security Modernization Act	Focuses on improving oversight of Federal information security programs by requiring Federal agencies to develop, document, and implement an agencywide information security program that provides security for the information and information systems that support the operations and assets of the agency.
Information Security Continuous Monitoring	Maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Personally Identifiable Information	Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, and mother's maiden name.
Privacy and Civil Liberties Impact Assessment	A process analyzing and documenting how PII and Sensitive but Unclassified information are used, collected, received, displayed, stored, maintained, protected, shared, and managed.

Term	Definition
Privacy Impact Assessment Management System	The central repository for the creation and management of the PCLIAs.
Tabletop Exercise	To practice a coordinated response to a breach to further refine and validate the response plan and to identify potential weaknesses.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF PRIVACY OFFICER

September 12, 2019

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Edward T. Killen for Marietta M. Downing
Chief Privacy Officer

SUBJECT: Draft Audit Report - Some Components of the Privacy Program Are Effective; However, Improvements Are Needed (Audit # 201720002)

Thank you for the opportunity to respond to the above-referenced draft audit report. The IRS is committed to protecting the privacy of taxpayer information and is proud of the maturity and accomplishments of its privacy program. We agree with your assessment that threats to privacy have increased in recent years as massive private sector data breaches exposed significant amounts of personal information that can be used to commit fraud. Accordingly, the IRS continues to refine our processes and increase protections afforded to taxpayers. One important protection is ensuring IRS systems only contain the information needed to achieve their stated purpose. IRS Privacy and Civil Liberties Impact Assessments (PCLIA) ensure that only information needed to perform tax administration is collected and when the information is no longer needed it is properly disposed of in accordance with statute and regulation. The IRS PCLIA was cited as a "Best Practice" in Senate Committee Report 107-174 and continues to be recognized as a model for excellence as evidenced by requests for IRS presentations at international conferences as to the effectiveness of our methods and sharing best practices with other federal agencies.

This audit focused on Federal Information Security Modernization Act of 2014 (FISMA) provisions that apply to the IRS privacy program. While FISMA is important to determining the effectiveness of the IRS privacy and security programs, the FISMA components reviewed do not make up the totality of the IRS privacy program. From the analysis of new technologies and their privacy implications, to the digital delivery of services and internal compliance review of IRS processes, the IRS privacy program is multi-faceted and innovative in its approach to protecting privacy. Indeed, the culture inside IRS is one that values privacy in every day work and strives to protect sensitive information.

In our response to this audit report we agree with many of the concepts and goals put forth by the audit team as recommendations and agree with all but one of the recommendations. The disagreement centers around different interpretations of requirements from the National Institute of Standards and Technology and the Office of Management and Budget. While we generally agree with the requirements stated, we also believe our current system and processes achieve the desired outcome. For example, the collaboration between security and privacy disciplines has always been a key to maintaining an effective privacy program. Inside the IRS, the Privacy and IT functions have always collaborated closely to protect taxpayer information. This collaboration will not only continue, it will increase as we strive to implement new technologies to better serve taxpayers.

The IRS has never viewed its privacy program as an end state to be achieved; rather the program strives for continuous improvement. Protecting taxpayer privacy is a vital and ever-evolving program that will change as new technologies and threats emerge. The IRS is deeply committed to protecting taxpayers' privacy in support of our voluntary tax system and will continue to place significant resources in our privacy program to achieve this mission.

If you have any questions, please contact me at 202-317-6449, or a member of your staff may contact Peter C. Wade, Director Privacy Policy and Compliance, at 470-639-3479.

Attachment

Attachment
TIGTA Audit 201720002

Recommendation 1: The Chief Privacy Officer should develop and maintain an inventory of the collection and use of PII in IRS systems.
Corrective Action: The IRS agrees with the importance of having the ability to produce an inventory of systems that contain and use PII. We recently created such an inventory using our PIAMS system. We have instituted a capability in PIAMS that will allow us to generate a current inventory at any point it is needed.

Implementation Date: Implemented

Responsible Official(s): Not applicable

Recommendation 2: The Chief Information Officer should implement a fully integrated information security continuous monitoring process that includes privacy risks.
Corrective Action: The IRS partially agrees with this recommendation. As TIGTA references in the report, IRS rates as having an effective level of security regarding its Data Breach Response Plan. While Privacy and Cybersecurity continue to work to determine the optimal maturity level, once NIST Special Publication 800-53 revision 5 is finalized Cybersecurity will integrate the privacy related security controls, enhancements and objectives, as recommended by the publication, into security assessments and continuous monitoring methodology.

Implementation Date: July 15, 2021

Responsible Official(s): ACIO IT Cybersecurity

Recommendation 3: The Chief Privacy Officer should ensure that the PGLD office strengthens its enforcement of the mandatory PCLIA review process by escalating expired PCLIAs to management for immediate attention or move to take the system offline.
Corrective Action: The IRS agrees reviewing processes to ensure they remain the most efficient is essential to a healthy privacy program. The current process, as explained in the audit report, has set follow up periods (90, 60 and 30 days) where PGLD analysts engage with system owners and subject matter experts to submit updates to the PCLIA. This process is effective and we note that TIGTA did not find any instances where the update to an expiring PCLIA was not in the process of being completed. In order to ensure that all necessary actions are in progress to update PCLIAs, we will analyze the escalation process in our internal procedures and revise as necessary to ensure that PGLD management is involved in the process.

Implementation Date: January 30, 2020

Responsible Official(s): Director, Privacy Policy and Compliance

Recommendation 4: The Chief Privacy Officer should ensure that the PGLD office coordinates with the business operating divisions to ensure all employees take the annual privacy awareness training as required.
Corrective Action: The IRS agrees that annual privacy awareness training is essential for a healthy privacy program. As evidenced in the audit report, over 99% of IRS employees completed the training in 2019 cycle. The existing process where the HCO provides completion updates to business units has proven to be very effective. However, to address this recommendation PGLD will issue a Servicewide Leaders' Alert communication prior to the training completion date reminding managers to ensure all of their employees complete the training.

Implementation Date: July 30, 2020

Responsible Official(s): Director, Privacy Policy and Compliance

Recommendation 5: The Chief Privacy Officer should ensure that the PGLD office updates and maintains PIAMS training courses to capture PIAMS enhancements.
Corrective Action: The IRS agrees with this recommendation. We will complete an analysis of Course 61760 "*Privacy Training for Privacy & Civil Liberties Impact Assessment Preparers,*" and Course 61922 "*Privacy Training for Adaptive Privacy Impact Assessment Preparers*", to determine if changes are needed and then implement the changes to the courses.

Implementation Date: October 31, 2020

Responsible Official(s): Director, Privacy Policy and Compliance

Recommendation 6: The Chief Privacy Officer should ensure that the PGLD office makes completion of PIAMS training courses mandatory for preparers of rejected PCLIAs.
Corrective Action: The IRS agrees that preparers of rejected PCLIAs should be required to complete the appropriate training. IRS will update its guidance to reflect this additional step.

Implementation Date: October 31, 2020

Responsible Official(s): Director, Privacy Policy and Compliance