Internal Revenue Service

Privacy Program Plan

December 21, 2020

Internal Revenue Service
Privacy Program Plan

I. Purpose

This document serves as the IRS Privacy Program Plan, as described and required by the US Office of Management and Budget (OMB). This plan is a companion to the "Privacy, Governmental Liaison and Disclosure (PGLD) Business Plan," which covers the goals and strategy for PGLD.

II. Background

OMB Circular A-130 "Managing Information as a Strategic Resource" has an appendix "Responsibilities for Managing Personally Identifiable Information" that describes the organization's role in protecting Personally Identifiable Information (PII) through a privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks.[1]

Further, A-130 requires a *Privacy Program Plan* that provides an overview of the agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy (SAOP) and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy requirements.[2]

Major updates to the 2018 version of the IRS Privacy Program Plan:

- The Treasury Privacy and Civil Liberties Office issued the Treasury Privacy Program Plan in May 2020. IRS reviewed its Privacy Program Plan to ensure consistency with the Department plan.
- The National Institute of Standards and Technology (NIST) published updated security and privacy controls in September 2020[3]. A new control is PM-18 *Privacy Program Plan;* IRS reviewed to ensure this Plan addresses the new requirements of this control.

III. Overview of IRS Privacy Program

The Chief Privacy Officer (CPO) is responsible for privacy protection for the IRS. The IRS CPO serves as the Director of Privacy, Governmental Liaison and Disclosure (PGLD). Under the IRS CPO is the Director, Privacy Policy and Compliance (PPC), who manages the core privacy compliance responsibilities for IRS as described by this plan. The basis for the IRS Privacy Program Plan is the strategy outlined in the PGLD Business Plan with the following commitments:

[1] OMB A-130 Appendix II page 4
[2] Ibid
[3] NIST Special Publication 800-53 Revision 5 *Security and Privacy Controls for Information Systems and Organizations*

A. Strategic Goals, Objectives, and Initiatives

PGLD supports the IRS Strategic Foundation goal to:

Invest in our workforce and the foundational capabilities necessary to achieve our mission and deliver high performance for taxpayers and stakeholders.

PGLD Mission:

To preserve and enhance public confidence by advocating for the proper protection, retention and disclosure of taxpayer information.

The Key PGLD Strategic Initiatives are:

- Foster a culture that protects privacy, promotes transparency, and properly maintains federal records.
- Conduct robust compliance and oversight programs to ensure adherence with federal privacy and disclosure laws and policies in all IRS activities.
- Provide outreach, education, training and reports promoting Privacy, Records and Disclosure priorities.
- Develop and maintain the best Privacy, Records, Disclosure and Governmental Information Specialist professionals in the federal government.

The Privacy Policy and Compliance Mission:

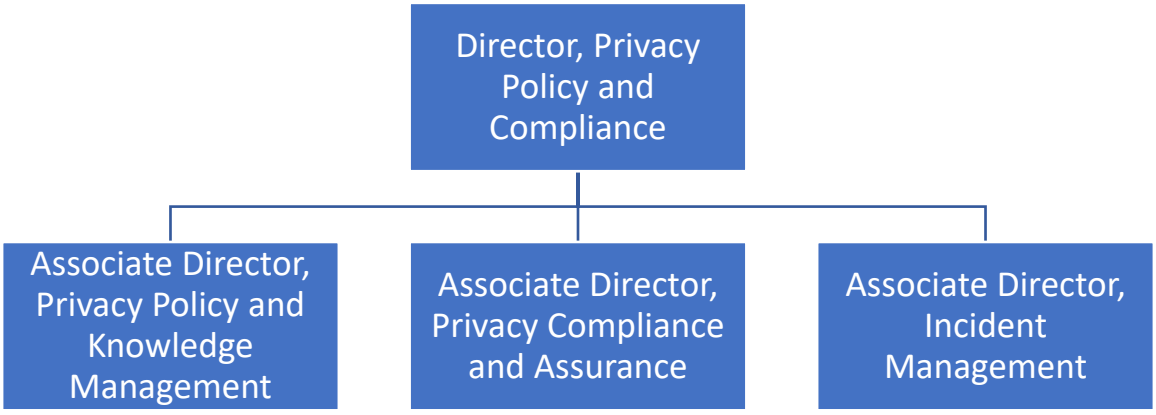
To promote and integrate privacy into business practices, behaviors, and technology solutions

B. IRS Privacy Program

The Privacy Program is overseen and managed by the PGLD Office of Privacy Policy and Compliance; PPC develops, implements, monitors, and reports on the Service-wide privacy initiatives on behalf of PGLD and the Treasury SAOP to promote and integrate privacy policies into business practices, behaviors and technology solutions. The ability for IRS to ensure the privacy and security of taxpayers' information significantly contributes to voluntary compliance with the nation's tax laws;

PPC is comprised of three groups:

- Incident Management and Employee Protection (IM/EP)
- Privacy Compliance and Assurance (PCA)
- Privacy Policy and Knowledge Management (PPKM)



Below are some of PPC's operational responsibilities:

- Reviewing and approving Privacy and Civil Liberties Impact Assessments (PCLIA)[4] for computer systems, SharePoint sites containing PII, social media, and employee and taxpayer surveys
- Conducting business PII risk assessments (BPRA)[5]
- Implementing requirements from OMB, the Treasury SAOP, privacy related aspects of the Federal Information Security Management Act (FISMA) and other legislation and guidance impacting privacy
- Providing Service-wide privacy policy guidance for all issues throughout the data privacy lifecycle, including eAuthentication[6], email containing PII, compliance with FISMA and general protections for sensitive information
- Leading the IRS Privacy Council[7], Privacy Advisory Group, and PGLD Policy Working Group
- Managing incidents involving the loss or theft of an IRS asset, or loss, theft or disclosure of personally identifiable information (PII)
- Tracking potentially dangerous taxpayers and those taxpayers who should be approached with caution.
- Managing the approval and use of authorized pseudonyms.[8]

[4] See IRM 10.5.1.7.2 *Privacy and Civil Liberties Impact Assessment*
[5] See IRM 10.5.1.7.3 *Business PII Risk Assessment*
[6] See IRM 10.5.1.7.9 *Electronic Risk Assessment*
[7] See IRM 10.5.1.7.1 *Privacy Council*
[8] See IRM 10.7.1.13 *Pseudonym*

1. Privacy Control Management
   PPC oversees the implementation of the National Institute of Standards and Technology (NIST) Privacy Controls, and directly administers the Program Management Privacy Controls. These controls mitigate the risks to individuals from the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personal information by IRS.

2. Privacy Program Governance Requirements
   PPC implements privacy program governance requirements through the following, along with its IRS and PGLD partners:

   - Allocate sufficient resources and staffing
     - CPO serves on the IRS Senior Executive Team and advocates for sufficient resources
     - PPC establishes collaboration among the many stakeholders for effective privacy governance

   - Monitor for privacy changes to Federal laws, regulations, and policies
     - Attends many of the privacy conferences, including the Federal Privacy Summit and those of the International Association of Privacy Professionals (IAPP)
     - Participates on and contributes to the Federal Privacy Council and several of its sub-committees to develop policy and guidance that improves peoples' protection of privacy
     - Reviews pending privacy legislation, regulations, best practices, privacy emerging issues, and court decisions for updates, precedents and policy or program changes
     - Assesses and tracks action items identified through monitoring, using a Privacy Issues Framework
     - Reassesses at least annually for IRS compliance with OMB Circular A-130, and resolve any lapses

   - Develop and implement Service-wide privacy policies and procedures for systems, programs, and operations
     - Updates and manages the privacy sections of the Internal Revenue Manual (IRM), the compendium of IRS policies and procedures
     - Issues Interim Guidance Memoranda (IGM) on emerging privacy issues such as the use of digital assistants while working, personal email by employees, and the access requirements for shared drives. A recent IGM issued was on privacy risk management for authentication via non-electronic transactions such as in-person or over the telephone.

   - Foster IRS-wide compliance with privacy policies and procedures
     - Conducts privacy outreach and maintains the Disclosure and Privacy Knowledge Base, an online virtual library for sharing privacy resources.

- Collaborates[9] with a wide variety of partners; current projects include:
  - Improve contractor oversight in collaboration with Cybersecurity, Personnel Security, and Procurement
  - Collaborated with IRS tax collection staff and the Social Security Administration on requirements for the Taxpayer First Act
  - Advise and assist on Memoranda of Understanding between IRS business units and other Federal agencies, including agreements related to relief programs from the COVID-19 pandemic

- Ensure privacy protection incorporated throughout lifecycle of systems and programs
  - Integrates privacy protection requirements into the IRS Enterprise Lifecycle, which ensures all privacy system requirements are tested and approved
  - Includes privacy requirements in the IRS Enterprise Architecture
  - Requires justification and approval for any use of PII for system testing

- Conduct PCLIAs, and publish when appropriate
  - IRS developed the Privacy Impact Assessment (PIA) in 1999, which was adopted by the eGov Act of 2002 as a Federal requirement
  - Deployed the Web-based Privacy Impact Assessment Management System (PIAMS) in 2011
  - Revised and renamed the PIA as the Privacy and Civil Liberties Impact Assessment (PCLIA), as instructed by Treasury
  - Maintain approximately 400 active and approved system PCLIAs
  - Review and approve approximately 500 PCLIAs of all types annually

- Ensure privacy policies are posted on IRS websites and other digital services where appropriate
  - Maintains online privacy policy. Note: To comply with OMB requirements, IRS revamped its internet privacy program page
  - Posts instructions on how to submit privacy complaints and comments on IRS.gov
  - Consults with online services developers to ensure compliance with posting of privacy policies

- Provide performance metrics and reports as required, or as needed to reduce risks
  - Report privacy related metrics to Treasury for inclusion in the FISMA and 803 reports
  - Prepare quarterly scorecards on breaches for IRS partners to reduce and mitigate data losses
  - Create an annual report on breaches, including trend analysis and vulnerabilities for mitigation

[9]Note: the new Privacy Control PM-18 *Privacy Program Plan* requires an explanation of the agency's "coordination among organizational entities responsible for the different aspects of privacy"

3. Manage PII requirements
   PPC manages PII requirements through the following, along with its IRS and PGLD partners:

   - Maintain and regularly review PII holdings for opportunities to reduce risk
     - Submit PII Holdings report upon request of Treasury
     - Implement a procedure for Cybersecurity to review systems with PII to ensure they have appropriate security, in compliance with a Privacy Control
   - Eliminate unnecessary collections and displays of Social Security Numbers (SSN)
     - Collaborate with PGLD's SSN Elimination and Reduction Program to ensure SSN usage is minimized
   - Use records management to reduce volumes of PII
     - Collaborates with PGLD's Records and Information Management (RIM) to ensure that PII is properly protected in records, and that PII is disposed of properly. The RIM office oversees IRS's implementation of records management;
     - Developed the guidance for records management automation in systems, which will aid in reducing the volume of PII
     - Executed records management for its own records, including approved disposal of expired PCLIAs and Incident Management reports. PPC will be executing its File Plans later this calendar year in coordination with PGLD.
   - Manage Privacy Act and Internal Revenue Code requirements for access, amendment, and disclosure
     - Ensure data-sharing with third parties complies with the Computer Matching Act, and enforce the safeguarding requirements of tax information
     - Manage the requests for access and amendment of Privacy Act records.
     - Ensure IRS information conforms to confidentiality requirements and disclosures are limited to what is authorized and required. This program is administered by PGLD Office of Government Liaison, Disclosure and Safeguards, and supported by PPC.

4. Budget and Acquisition
   PPC implements budget and acquisition requirements through the following, along with its IRS and PGLD partners:

   - Ensure the IRS allocates for Service-wide privacy programs
     - The Chief Privacy Officer ensures budget consideration for Service-wide privacy programs through budget requests and membership on the Senior Executive Team
     - PGLD will add in privacy costs once the IRS Chief Finance Officer (CFO) has an approved list of proposals for upcoming budget cycle

   - Advocate for privacy risk mitigation cost inclusion in budget requests
     - PGLD developed and implemented criteria for including privacy costs into budget requests based on OMB Circular A-130

5. Contractor and Third-Party Requirements
   PPC implements contractor and third-party requirements through the following, along with its IRS and PGLD partners:

   - Ensure contracts and agreements include privacy requirements
     - Initiated a contract review program to ensure privacy requirements are included in contracts, in collaboration with Procurement

   - Implement privacy oversight of contractors
     - Collaborate with Cybersecurity and others to improve auditing of IRS systems to detect unauthorized accesses, including of contractors
     - Assists the PGLD Office of Identity and Records Protection (IRP) UNAX team[17] in the drafting of the Standard Operating Procedures (SOP) for adjudication of contractors that committed UNAX violations; the SOP was subsequently signed for approval by IRP Director and the management of HCO and Agency Wide Shared Services (AWSS) in 2015
     - Collaborates with Procurement and the Security offices on new training for Contracting Officer's Representatives (COR) regarding their contractor oversight responsibilities. Trained approximately 600 CORs

   - Implement privacy requirements on contractor systems and programs
     - Adapted the PCLIA for contractor systems, programs, and services.

   - Ensure breach management procedures include contractor breaches
     - Audit contracts for inclusion of the contract breach clause
     - Work with Procurement to update the clause regarding breaches by contractors based on OMB instructions
     - Trained CORs on reporting of and assisting on contractor breaches.

6. Workforce Management
   PPC implements workforce management requirements through the following, along with its IRS and PGLD partners:

   - Implement competency requirements for privacy staff and managers
   - Ensure privacy staff have appropriate training and skills
     All PPC employees have access to the privacy resources on the IAPP website. Because of the 2020 pandemic, numerous privacy conferences were cancelled, including the National IAPP conference in April. IAPP however has created Webinars covering a variety of relevant subjects, such as privacy impact assessments on Artificial Intelligence systems. The Federal Privacy Council held the annual Federal Privacy Summit virtually in 2020 which many IRS privacy staff attended online. Employees are also eligible to attend local IAPP events and view on-line privacy presentations. More than half of our core privacy employees have at least one IAPP privacy professional certification.

7. Privacy Training
   PPC implements privacy training requirements through the following, along with its IRS and PGLD partners:

   - Maintain appropriate mandatory Service-wide privacy training of employees and contractors[19]
     - Manage the annual privacy training for employees
       - As of June 2020, 69K (95%) of IRS employees were trained so far for FY20
     - Collaborate with Contractor Security Management to ensure appropriate privacy training is done for onboarding and then annually
   - Ensure that training is updated with new policies and requirements
     - Review and update the training every year
   - Provide foundational and advanced privacy training
   - Provide role-based training to appropriate employees and contractors
     - Provide privacy training for managers, IT specialists, IT system developers, Enterprise Architecture and Data Strategy Officers, and Cybersecurity personnel.
     - Provide privacy training for systems and adaptive PCLIA preparers
   - Establish privacy rules of behavior and consequences for violations
     - Require certified agreement to the Privacy Rules of Behavior for access to IRS systems
     - Include employee and manager responsibilities in the IRM
     - In concert with the Human Capital Office, establish consequences for violations in the Guide to Penalty Determinations
     - Investigate unauthorized accesses (through TIGTA), and if verified report to the IRS Employee Conduct and Compliance Office for adjudication

8. Breach Management
   PPC implements breach management requirements through the following, along with its IRS and PGLD partners:

   - Maintain breach management policies and competencies
   - Establish roles and responsibilities for effective management of breaches
     - Data Breach Response Playbook outlines a plan for the IRS to effectively and efficiently react when SBU, including PII and tax information has been potentially lost, stolen, or disclosed and the circumstances require an enhanced response.
     - IRS Breach Response Plan provides a framework for PGLD's IM program, outlines the methodology the IRS will use to categorize breaches and determine the appropriate response based on the OMB guidance, and contains the procedures the IRS will follow for routine breaches.
     - Incident Management Operations guide provides guidance for obtaining systems access to facilitate assignments, working and documenting breaches, creating necessary reports, and required notification procedures.
   - Test breach procedures in a variety of scenarios periodically
     - IM conducts tabletop exercises to practice a coordinated response to a breach to

further refine and validate the Playbook and Response Plan and to identify potential weaknesses. The tabletop is conducted annually or more frequently if needed (following organizational changes, plan updates, issuance of new guidance, etc.).
    - Verify and Implement corrective actions based on gaps discovered during the tabletop exercise.
- Report on breaches as required
    - Supply information for the Annual FISMA report that includes a description of major information security incidents and major incidents that involved a breach.
    - Report breaches to TSCIRC as Treasury requires, including all paper breaches and any breaches that could raise media attention or those that are exceptional in terms of number or importance of the individuals involved.

9. Privacy Risk Management
   PPC implements privacy risk management requirements through the following, along with its IRS and PGLD partners:

- Implement a risk management framework consistent with OMB guidance
    - The Federal Privacy Council is establishing the Privacy Risk Management Working Group that includes PPC representation. This group will discuss risk management among multiple agencies and develop best practices.
- Assess regularly for risks based on the privacy controls
    - Managed the initial Service-wide risk assessment from the privacy controls.
    - Contribute to the development of the updated controls
    - Participate in discussions, identification and mitigations of Service-wide privacy risks. Capture these discussions and determinations on a Risk Acceptance Form and Template (RAFT) and generally require CPO approval of mitigation plans and any risks accepted.
- Develop and monitor mitigation projects to minimize privacy risks
    - Conduct Privacy Control Risk Assessments to gauge IRS compliance with the controls and make recommendations to mitigate the risks
    - Between risk assessments implement continuous monitoring as prescribed in NIST SP 800-53R5 to maintain ongoing awareness of developing vulnerabilities

IV. Roles and Responsibilities

Following are roles and responsibilities as they relate to the IRS privacy program.

- IRS Chief Privacy Officer
    - Implements and manages the IRS Privacy Program and ensures compliance with the Privacy Act of 1974, the E-Government Act of 2002, FISMA, OMB guidance, and other Federal requirements
    - Sets the strategic direction for the IRS Privacy Program to include defining privacy risk management, privacy policies, creating awareness, designing effective incident response and data / PII breach notification procedures

    - Develops and promotes IRS privacy policy, guidance, and requirements for all IRS systems in alignment with applicable laws, regulations and standards throughout the System Enterprise Life Cycle (ELC)
    - Ensures privacy controls are integrated into the IRS enterprise architecture and capital planning and investment control processes
    - Ensures the IRS meets reporting requirements mandated by Congress, OMB, and Treasury regarding IRS activities that involve PII or otherwise impact privacy
    - Ensures appropriate privacy controls are implemented on IRS information systems that contain PII, whether owned and operated by or operated on behalf of the Service
    - Reviews and approves privacy compliance documentation
    - Identifies and analyzes breaches and manages the analysis and IRS response
    - Approves external notifications and communications, including, but not limited to congressional notifications, press releases, and notifications to individuals potentially affected by a breach
    - Serves as the principal IRS liaison with organizations outside of IRS for matters relating to privacy
    - Communicates to IRS leadership the significance of privacy risk to Service operations
- Senior Agency Official for Privacy
    - Responsible and accountable for the implementation of privacy compliance requirements at the Department of Treasury
    - Collaborates with IRS and other bureaus to implement privacy requirements
- Chief Information Officer and Chief Information Security Officer
    - Collaborates with the Chief Privacy Officer (CPO) on ensuring appropriate security and privacy protection related to IRS PII[24]
- Chief Procurement Officer
    - Collaborates with CPO to ensure contracts have appropriate clauses and are enforced to protect the privacy of IRS PII
- Senior Management and Executives
    - Ensure existing and new requirements to protect privacy are implemented throughout the IRS
    - Ensure employees know their privacy responsibilities
    - Respond to employee questions regarding privacy protection
- All IRS Employees are responsible to:
    - Keep informed of privacy policies and procedures
    - Ask for guidance and clarification from their supervisors when necessary
    - Access IRMs and PGLD Knowledge Management Base and Library as necessary

Appendix – PGLD Organization Chart