Internal Revenue Service

Privacy Program Plan

December 31, 2023

06/11/2025 - Interim update for administrative corrections and changes only.

Table of Contents

Internal Revenue Service

Privacy Program Plan

1.0 Introduction:

1.1 Purpose

Office of Management and Budget (OMB) Circular A-130 "Managing Information as a Strategic Resource" in the appendix[1] entitled "Responsibilities for Managing Personally Identifiable Information," 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.

Further, Circular 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 roles 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.
- any other information determined necessary by the agency's privacy requirements.

1.2 Background

This Privacy Program Plan, as described by the National Institute of Standards and Technology (NIST) security and privacy control 800-53 Rev. 5[2], PM-18 describes how the Internal Revenue Service (IRS) implements OMB Circular A-130[3] guidance, for effectively managing PII as a strategic resource. This plan serves as a companion to the "Privacy, Governmental Liaison and Disclosure (PGLD) Program Letter" which covers the goals and initiatives for PGLD. The basis for the IRS Privacy Program Plan is the initiatives outlined in the PGLD Program Letter and supported by related commitments, as well as the IRS responsibilities for implementing the Treasury Privacy Program as a bureau of the Department of the Treasury.

2.0 IRS Privacy Program Infrastructure and Organization

2.1 IRS Commissioner

The IRS Commissioner, as a Treasury Department Bureau Head, is responsible for establishing internal controls to ensure the effectiveness of the IRS privacy program and conformity with Treasury-wide privacy requirements. The IRS Commissioner assigned the Director, Privacy Policy and Compliance

---

[1] *A-130 Appendix II page 4*
[2] *NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations*
[3] *OMB Circular A-130 "Managing Information as a Strategic Resource"*

(PPC), the role of IRS Bureau Privacy and Civil Liberties Officer (BPCLO) to serve as the Privacy and Civil Liberties (PCL) point of contact (POC).[4]

2.2 IRS Chief Privacy Officer

The Department of the Treasury's Senior Agency Official for Privacy has delegated the responsibility for privacy protection at the IRS to the IRS Chief Privacy Officer (CPO). The IRS CPO serves as the Chief of PGLD.

2.2.1 IRS Chief Privacy Officer – Roles and Responsibilities

- Implements and manages the IRS Privacy Program and ensures compliance with the Privacy Act of 1974, the E-Government Act of 2002, Federal Information Security Modernization Act (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 Lifecycle (ELC).
- Ensures appropriate privacy controls are integrated into the IRS enterprise architecture (EA) and capital planning and investment control processes.
- 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.
- Ensures the IRS meets reporting requirements mandated by Congress, OMB, and Treasury regarding IRS activities that involve PII or otherwise impact privacy.
- 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.

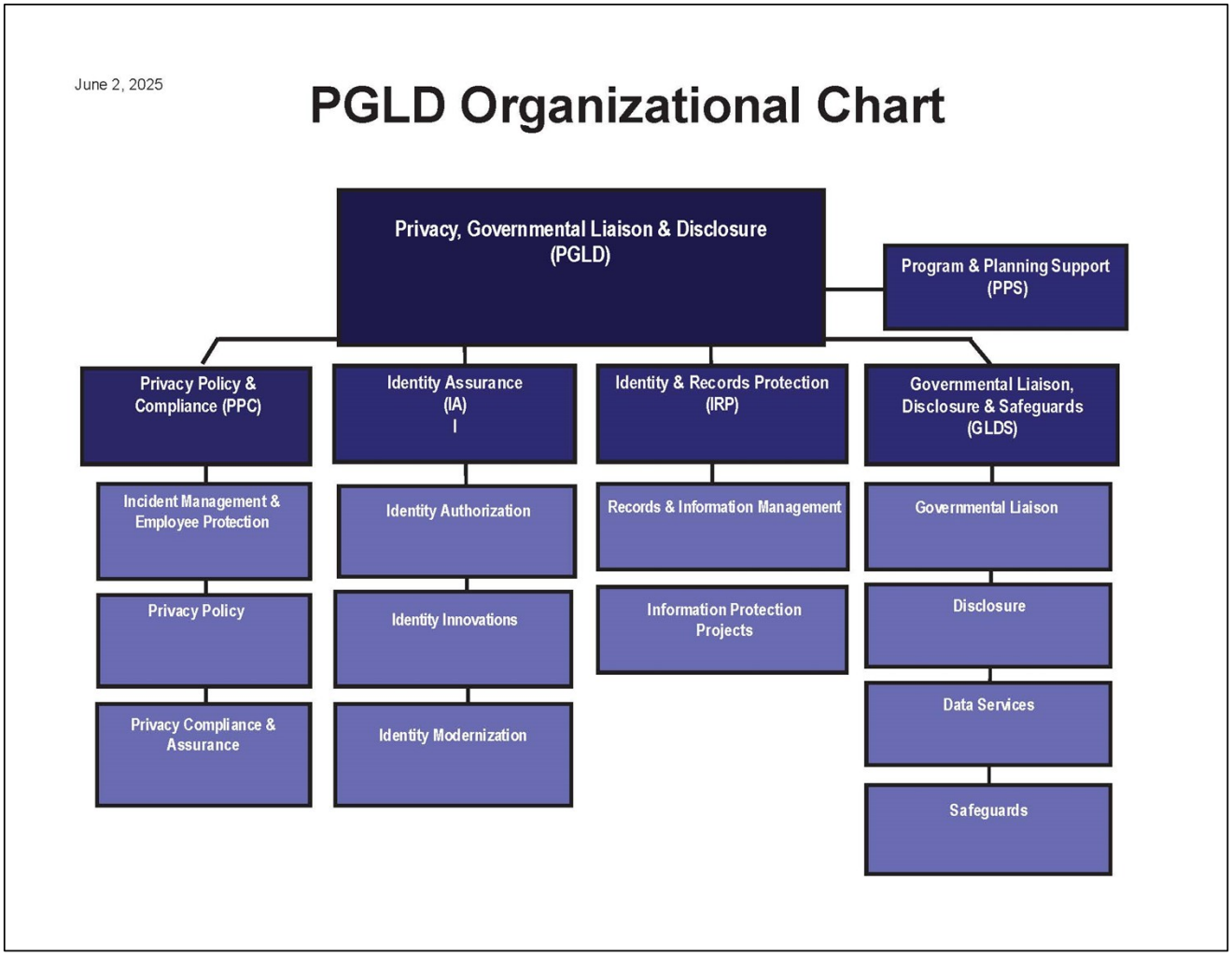
2.2.2 Privacy Governmental Liaison and Disclosure (PGLD)

PGLD supports the IRS Strategic Goals of putting the interests of our taxpayers first in everything we do. Principally, PGLD's focus on protecting the privacy of our taxpayers and the security of their data puts one of the most important interests of our taxpayers first.

[4] *US Department of the Treasury Privacy Program Plan (Version 1.0) @ Page 13*

PGLD Mission:

To preserve privacy and enhance public trust through proper authentication, access, disclosure, retention and protection of all data and records.



The Key PGLD Strategic Goals, Objectives, and Initiatives:

- Preserving and enhancing public confidence by advocating for the protection and proper use of sensitive information.
- Preventing identity theft and unauthorized disclosures by ensuring proper access and authentication.
- Protecting sensitive information and privacy of taxpayers and employees.
- Mitigating data losses and reducing vulnerabilities for identity theft, thereby, promoting identity protection.

- Ensuring IRS records, including those containing PII, are managed appropriately.
- Partnering with federal, state, and local governmental agencies to promote privacy and protect federal tax information (FTI).
- Working with all IRS operations to ensure only authorized disclosures and data sharing.

2.3 PGLD's Deputy Chief Privacy Officer

In 2022, Treasury approved the establishment of a **Deputy Chief Privacy Officer** who reports directly to the Chief Privacy Officer, and shares responsibility for:

- Establishing the IRS strategic direction regarding the protection, retention, authentication, minimization, and disclosure of taxpayer information.
- Directing a core staff of privacy, records, identity assurance, and security subject matter experts, both on the policy front and in information systems.
- Promoting consistent and compliant implementation of privacy policies, records retention and disclosure statutes, and NIST requirements for authentication and electronic signatures.
- Reporting on IRS activities to promote privacy protection and information security.
- Leading privacy policy development and providing expert advice on privacy, disclosure, records management, authentication, execution of the Freedom of Information Act (FOIA), data protection, and data sharing efforts across IRS and with external government partners.
- Assessing and supporting plans to mitigate organizational risks from potential breaches or unauthorized disclosures of IRS records.
- Partnering with federal, state, and local agencies to obtain data that supports tax administration and efforts to reduce tax refund identity theft.
- Interpreting and administering Internal Revenue Code (IRC) Section 6103 to ensure the confidentiality of tax records and the privacy and integrity of tax administration systems.
- Providing statutory oversight of IRS security and confidentiality requirements for federal, state, and local agencies receiving tax return information.
- Enhancing PGLD expertise and field presence through knowledge management practices that expand the privacy, records, disclosure and IA, knowledge, and professional expertise of all PGLD employees.

Specifically, the Deputy Chief Privacy Officer, is responsible for:

- Sharing participation on, and oversight of, over 50 governance boards where PGLD serves as a voting member or subject matter advisor.
- Representing PGLD and IRS interests involving cross-agency data sharing (now involving more than 16 million data elements) to ensure the data sharing is allowable, properly accounted, and reported to Congress when required.
- Serving as the Executive POC for Servicewide and Government-wide projects and Executive Orders that require PGLD expertise and oversight such as the Federal Contractor Tax Check System, Controlled Unclassified Information (CUI) coordination, Digitalization, and supporting the Security Summit and Identity Theft Tax Refund Fraud Information Sharing and Analysis Center.
- Keeping abreast of recent privacy, records, disclosure, and authentication developments, including legislative changes, including recent court decisions, and

departmental guidance issued by NIST, National Archives and Records Administration, and OMB.

- Examining legislative and other initiatives proposed by Congress, other agencies, and the public to formulate PGLD/IRS positions and, when appropriate, identifying the need for new legislation to strengthen and support the Service's policies that address privacy, records, authentication, and disclosure issues.
- Providing program level oversight of strategic goals and initiatives and ensuring PGLD internal controls are operating as intended to address concerns or deficiencies as they are identified.
- Establishing effective working relationships and communications to understand IRS operational priorities so PGLD can provide tactical assistance and effective advice that will mitigate risks and promote operational excellence.
- Monitoring PGLD recommended/agreed risk mitigations with Servicewide impact to ensure mitigations are in place and operating as intended.
- Motivating and developing PGLD employees by supporting employee engagement, promoting opportunities for veteran appointments, and implementing quality excellence and ethics programs.

2.4 PGLD's Director of Privacy Policy and Compliance (PPC)

The Director, PPC within PGLD manages the core privacy policy and compliance responsibilities for the IRS as described by this plan.

2.4.1 PPC Director's role as Bureau Privacy and Civil Liberties Officer **(**BPCLO)

- The PGLD Director of PPC is designated to serve as the BPCLO under the provisions of TD 25-07. Accordingly, designating the PPC Director as the BPCLO aligns with Treasury requirements and formalizes the approvals and authorities already in place. Under this provision, PGLD ensures the IRS complies with the provisions of the E-Government Act by administering programs that collect, review and store Privacy and Civil Liberties Impact Assessments (PCLIAs).

2.4.2 PPC Director's Oversight of the PCLIA Program

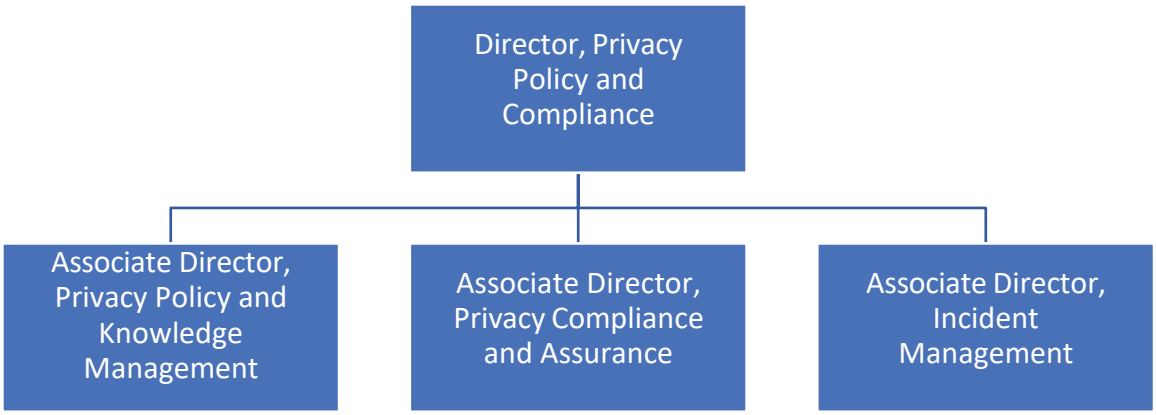
- The Director of PPC oversees the PCLIA program under the delegated authority of the Chief Privacy Officer and has designated the Associate Director of Privacy Compliance and Assurance (PCA) as the reviewer for all IRS PCLIAs.

2.4.3 PPC's Operational Structure - PPC is comprised of three subfunctions:

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

2.4.4 The Privacy Policy and Compliance (PPC) Mission:

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



2.4.5 PPC's Major Operational Responsibilities within the three subfunctions are:

- **Privacy Policy:**
  - Providing Servicewide privacy policy guidance for all issues throughout the data privacy lifecycle, from receipt to disposal, including compliance with FISMA, Sensitive But Unclassified (SBU) data protection[5], email containing PII, and need to know general policy.
  - Overseeing the implementation of requirements from OMB, the Treasury SAOP, FISMA and any new legislation and guidance pertaining to all aspects of Privacy and Data Protection.
  - Leading and participating on collaborative groups such as the IRS Privacy Council[6,] Privacy Advisory Group, and PGLD Policy Working Group.

- **Privacy Compliance and Assurance (PCA):**
  - Reviewing and approving PCLIAs for computer systems, social media, SBU data use requests, clean desk waivers, and employee and taxpayer surveys.[7]
  - Privacy Control Management.
    - Overseeing implementation of the NIST 800-53 Rev. 5, Privacy specific and Joint with Cyber Controls. (*See Attached Appendices B1and B2*)
    - Performing risk assessments on all information system controls and initiating steps to mitigate the risks to individuals from the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personal information by IRS.
    - The Privacy Controls Assessment Team (PCAT) improve IRS Privacy and Security compliance by performing assessments of NIST 800-53 Rev. 5 Controls during the annual FISMA risk assessments performed on IRS information systems interacting with PII.
    - PPC also oversees the risk assessment of the implemented enterprise-wide privacy common controls applicable to information systems and any other system that collects PII which could span multiple business units.
  - Conducting Business PII Risk Assessments (BPRA).[8]

- **Incident Management and Employee Protection (IM/EP):**

---

[5] *See IRM 10.5.1.2.2, Sensitive but Unclassified (SBU) Data*
[6] *See IRM 10.5.1.7.1, IRS Privacy Council*
[7] *See IRM 10.5.1.7.2, Privacy and Civil Liberties Impact Assessment (PCLIA)*
[8] *See IRM 10.5.1.7.3, Business PII Risk Assessment (BPRA)*

- Implementing requirements from OMB, the Treasury SAOP, FISMA and other legislation and guidance pertaining to Incident Management, Breaches, etc.
- Managing IRS incidents involving the loss, theft, or unauthorized disclosure of SBU data, including PII and Tax information through the loss or theft of 1) IRS IT assets, 2) BYOD assets, and 3) Physical and electronic documents, which contain such SBU data, including PII and tax information.
- Tracking potentially dangerous taxpayers and those taxpayers who should be approached with caution.
- Managing the approval and use of authorized pseudonyms.[9]

2.5 Other Roles and Responsibilities Essential to IRS's Privacy Program

2.5.1 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.

2.5.2 Chief Information Officer and Chief Information Security Officer

- Collaborates with the CPO on ensuring appropriate security and privacy protection related to IRS PII.

2.5.3 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.

2.5.4 All IRS Employees are responsible to:

- Keep informed of privacy policies and procedure.
- Ask for guidance and clarification from their supervisors when necessary.
- Access IRMs and PGLD Knowledge Management Base and Library as necessary.

3.0 Privacy Program Controls and Requirements

The (NIST Special Publication (SP) 800-53 Rev. 5, provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors.

When NIST issued SP 800-53 Rev. 5 in 2020, IRS Privacy and Security policy owners identified the new Privacy and joint with Security Privacy and Security controls to be implemented as IRS Organization Common Controls (OCCs). These OCCs (*attached as Appendices B1 and B2*) are the primary mechanisms for ensuring the consistent Treasury-wide and IRS-wide implementation of privacy requirements.

[9] *See IRM 10.5.1.7.16, Pseudonym.*

3.1 Privacy and Security Controls

NIST SP 800-53 Rev. 5 describes three types of controls impacting Privacy.

1. Security Controls are the safeguards or countermeasures employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage information security risk.
2. Privacy Controls are the administrative, operational, technical, management and physical safeguards employed within a system or an organization to
   - manage privacy risks.
   - ensure compliance with applicable privacy requirements.
   - maintain the integrity, confidentiality, and security of PII.
   - to minimize PII maintained in federal information systems to only what is relevant and necessary.
3. Security and Privacy Controls are selected and implemented to satisfy security and privacy requirements levied on a system or organization. Security and privacy requirements are derived from applicable laws, executive orders, directives, regulations, policies, standards, and mission needs to ensure the confidentiality, integrity, and availability of information processed, stored, or transmitted and to manage risks to individual privacy.

3.2 Common Controls

Common controls are controls that provide security/privacy capabilities for multiple information systems. These controls are referred to as "inherited controls" when applied to support a specific information system. When a common control is applied to a particular information system, that common control is deemed "inherited" for that system. The control itself is developed, implemented, assessed, authorized, and monitored by programs or officials other than those responsible for the information system.

Common privacy controls are not managed by information system owners but are managed at a higher level because they affect multiple systems. That means, in most cases, an agency program or official other than the information system owner manages them. Moreover, privacy controls designated as information system-specific may be the primary responsibility of information system owners and their respective authorizing officials. In all cases, the management of privacy controls are subject to the coordination and oversight of the SAOP (Assistant Secretary for Management (ASM)) / Treasury Chief Privacy and Civil Liberties Officer (CPCLO), and. PPC Director / BPCLO in IRS.

The IRS performs privacy and security risk assessments to help management decide which controls to use to mitigate network risk to an acceptable level. The IRS continuously monitors and periodically reviews these controls to ensure they are effectively implemented.

4.0 Privacy Program Plan Execution

4.1 Privacy Program Governance Requirements

4.1.1 Fostering Collaboration

PPC promotes collaboration with many stakeholders and partners for effective privacy governance and implements privacy program governance requirements through the following, along with its IRS and

PGLD partners by:

- Allocating sufficient resources and staffing
  - CPO serves on the IRS Senior Executive Team and advocates for sufficient resources.
- Monitoring Federal laws, regulations, and policies for privacy related changes
- Attending many of the major privacy conferences, including the Federal Privacy Summit and International Association of Privacy Professionals (IAPP) conferences.
- Participating on and contributing to the Federal Privacy Council and several of its sub-committees in reviewing pending privacy legislation, regulations, best practices, privacy emerging issues, and court decisions for updates, precedents and policy or program changes.
- Assessing and tracking action items identified through monitoring, consistent with the Risk Management Framework.
- Having the PCAT Assess Privacy Control Risks annually for IRS compliance with FISMA, OMB Circular A-130 and NIST SP 800-53.
- Developing and implementing Servicewide privacy policies and procedures for systems, programs, and operations by:
  - Updating and managing the privacy sections of the Internal Revenue Manual (IRM), the compendium of IRS policies and procedures, and
  - Issuing 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.

4.1.2 Fostering Compliance

PPC, in coordination with IRS and PGLD partners, implements privacy program governance to promote privacy compliance by:

- Improving contractor oversight in collaboration with Cybersecurity, Personnel Security, and Procurement.
- Reviewing Memoranda of Understanding (MOUs) between IRS business units and other Federal and state agencies for Privacy Compliance Requirements.
- Providing Privacy guidance with respect to the implementation legislative mandates and executive directives.
- Collaborating with IRS Cybersecurity to conduct FISMA privacy risk assessments on complex IRS information systems.
- Fostering IRS-wide compliance through privacy policies, procedures, and continuous monitoring.
- Developing and providing guidance to assist system developers and owners in incorporating privacy protection throughout the lifecycle of systems and programs to:
  - Embed privacy requirements into the existing IRS ELC, waterfall method, which ensures all system requirements are assessed and approved.
  - Work with ELC's replacement One Solution Delivery Life Cycle (OneSDLC), agile method, so stakeholders are educated on the privacy requirements to ensure a privacy by design mindset.
  - Require justification and approval for any use of PII for system testing.
- Conducting PCLIAs, and publishing PCLIAs when appropriate
- Ensuring privacy policies are posted on IRS websites and other digital services by
  - Maintaining online privacy policy. [Note: To comply with OMB requirements, IRS restructured its internet privacy program page].
  - Posting instructions on how to submit privacy requests, complaints, and comments on IRS.gov.
  - Consulting with Online Services developers to ensure compliance with posting of privacy

policies.

- Providing 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.
  - Preparing quarterly scorecards on breaches for IRS partners to reduce and mitigate data losses.
  - Creating an annual report on breaches and vulnerabilities for mitigation.

4.1.3 Managing PII Requirements

PPC, in collaboration with PGLD and IRS Privacy Partners manage PII requirements by:

- System Monitoring: Implementing procedures for Cybersecurity to review systems with PII to ensure they have appropriate security, in compliance with Privacy Controls.
- Social Security Number (SSN) Elimination: Eliminating unnecessary collections and displays of SSNs through PGLD's SSN Elimination and Reduction Program to ensure SSN usage is minimized on IRS' letters, forms, and CP Notices and in Systems by working closely with SMEs in IRS Correspondence Processing and Collaborating with PPC to update the PCLIA process to document on form 14132 systems that use SSNs.
- Records Management: Using records management techniques to reduce volumes of PII. The Records and Information Management (RIM) office oversees IRS's implementation of records management to reduce volumes of PII by:
  - Collaborating with PGLD's other functions to ensure PII is properly protected in records, and that PII is disposed of properly.
  - Developing guidance for records management functionality in electronic systems.
  - Providing guidance and overseeing activities related to the creation, maintenance and use, and disposition (final retention) of records to ensure IRS records are available only where and when they are needed. to whom they are needed; and for only as long as they are needed, to conduct business, adequately document IRS activities, and protect the interests of the federal government.
  - Reassessing and revising Records Retention Schedules to reduce the retention schedule whenever a shorter time frame better reflects how long IRS needs the records are needed.
- Access and Amendment: Managing Access, Amendment and Disclosure of Individual Privacy and FTI by:
  - Supporting the implementation of Privacy Act and IRC requirements for access, amendment, and disclosure through the implementation and assessment of specific related controls, and by monitoring compliance with those controls.
  - managing requests for access and amendment of Privacy Act records.
  - ensuring disclosures of individual tax return information conform with IRC Section 6103 confidentiality requirements and disclosures are limited to what is authorized and required.
  - ensuring data-sharing with third parties complies with the Computer Matching Act, and
  - enforcing the tax information safeguarding requirements

4.1.4 Privacy Risk Management

PPC, along with its IRS and PGLD partners, implements privacy risk management requirements in IRS information systems by:

- Preparing the IRS for changes within the privacy risk management framework through cross functional communication updates in the recurring, stakeholder meetings and privacy training.
- Categorizing integral elements in the IRS EA to ensure privacy requirements are addressed by participating in cross functional working groups.

- Selecting and tailoring privacy controls for systems or projects to reduce risk to an acceptable level based on the privacy risk assessment.
- Implementing privacy organizational level controls to perform key privacy functions for all of IRS.
- Assessing complex IRS information systems to determine if the controls are implemented properly.
- Facilitating the authorization of privacy level controls based on an acceptable level of privacy risk as determined by the IRS Enterprise Risk Management Framework.
- Monitoring the systems and controls on an ongoing basis by performing assessments at inception, during significant system changes, and annually.
- Performing deep dive assessments during business PII risk assessments (BPRA) on how PII is handled when recurring assessment issues are identified (within scope) or when a business function makes a qualifying referral to PPC.
- Assessing the implementation of the privacy risk management requirements on contractors and cloud service providers to implement a risk management framework consistent with OMB guidance.
- Contributing to the recurring and multi-agency, Federal Privacy Council, to discuss privacy risk management and develop best privacy practices across the federal government.
- Performing privacy risk assessments through continuous monitoring on complex IRS information systems and organization level controls to identify privacy risks.
- Note: When a privacy risk is identified, the responsible party will generally either:
  - Mitigate the risk and monitor and document the mitigation through the Plan of Action and Milestone (POA&M) process in which regular updates are required until the mitigation is implemented, or,
  - Accept the risk by entering the Risk-Based-Decision process.
- Ensuring privacy policies are posted on IRS websites and other digital services where appropriate. For example:
  - Maintaining an online privacy policy. (Note: To comply with OMB requirements, IRS restructured its internet privacy program page.)
  - Posting instructions on how to submit privacy complaints and comments on IRS.gov, and
  - Consulting with online services developers to ensure compliance with posting of privacy policies.
- Providing performance metrics and reports as required, or as needed to reduce risks.
  - Reporting metrics to Treasury for inclusion in the FISMA and 803 reports.
  - Creating an annual report on breaches, including trend analysis and vulnerabilities or mitigation.

4.1.5 Budget and Acquisition

PPC, along with its IRS and PGLD partners ensures budget consideration for Servicewide privacy programs through budget requests and membership on the Senior Executive Team.

- IRS Chief Privacy Officer:
  - Follows PGLD's previously developed criteria for including privacy costs into budget requests based on OMB Circular A-130, and
  - Advocates for privacy risk mitigation cost inclusion in budget requests.
- PGLD reviews new legislation, NIST directives, and OMB guidance for Privacy program impacts and adjusts budget and staffing requests accordingly.

4.2 Privacy Awareness and Training

PPC, along with its PGLD and IRS partners, implements role-based privacy training requirements by:

4.2.1 Role-Based Training:

- Supporting the development of role-based training for delivery to all IRS employees and contractors and providing role-based foundational and advanced privacy training for appropriate employees such as managers, IT specialists, IT system developers, EA and Data Strategy Officers, and Cybersecurity personnel.
- Implementing workforce management strategies and initiatives to increase the privacy competency of Privacy staff.
- Supporting developments and maintenance of appropriate mandatory Servicewide privacy training for employees and updates with new policies and requirements each year.
- Providing privacy training for systems and adaptive PCLIA preparers.
- Supporting Contractor Security Management in their responsibility to ensure appropriate role-based privacy training is completed for Contractors during onboarding and then annually.

4.2.2 Workforce Management Strategies and Initiatives

PPC implements workforce management requirements of Privacy Staff through the following:

- Implements competency requirements for privacy staff and managers.
- Ensures privacy staff have appropriate training and skills.
- Establishes privacy rules of behavior and consequences for violations.
- Requires certified agreement to the Privacy Rules of Behavior for access to IRS systems.
- Establishes consequences for violations in the Guide to Penalty Determinations.

4.3 Incident Response and Breach Management

PPC implements breach management requirements, along with its IRS and PGLD partners, by:

- Maintaining breach management policies and competencies.
- Establishing roles and responsibilities for effective management of breaches.
- Testing breach procedures in a variety of scenarios including desktop exercises.
- Implementing and verifying corrective actions.
- Administering the breach reporting requirements as required.

5.0 Privacy Control Requirements

5.1 Privacy Control Requirements

The Privacy Act, Section 208 of the E-Government Act, and OMB policies impose collection, maintenance, use, and disposal requirements for executive branch agencies that maintain PII. Privacy controls are based on the Fair Information Practice Principles (FIPPs) embodied in the Privacy Act. The FIPPs provide the foundation and guiding principles for Treasury's privacy program controls through the implementation of the NIST 800-53 Rev. 5 Privacy Controls.

The FIPPs are designed to build public trust and help agencies avoid tangible and intangible costs resulting from privacy incidents. The Privacy Control Families are derived from the FIPPs, each

family consists of one or more privacy controls, and each control imposes one or more requirements. All privacy families, including their controls and requirements, are implemented at the agency, bureau, program, or information system level.

5.2 Privacy and Civil Liberties Threshold Analysis or Qualifying Questionnaire

Some systems and projects do not require a PCLIA, either because they do not process PII or because an OMB M-03-22 exemption applies. If there is uncertainty about whether a PCLIA is required, the system owner must use the Departmental Privacy and Civil Liberties Threshold Analysis (PCLTA) template (or a bureau-specific alternative) to assist in making this determination. The IRS uses a Qualifying Questionnaire (QQ) as a bureau-specific alternative to satisfy this requirement, along with Major Change Determinations (MCDs) to determine if a new PCLIA is needed to replace or amend an existing PCLIA.

The IRS BPCLO assesses the IRS's information systems and determines whether a PCLIA is required. A QQ also documents the BPCLO's reasons for determining that a PCLIA was or was not required. A QQ or MCD must be reviewed and updated as necessary where an IT system or information collection modification creates new privacy risks or to reflect changed information collection authorities, business processes, or other factors affecting the collection and handling of PII.

5.3 Privacy and Civil Liberties Impact Assessments

The IRS Conducts PCLIAs on all systems, projects, applications, or databases that contain PII and publishes them when appropriate to:

- (i) analyze how information is handled.
- (ii) ensure handling conforms with applicable legal, regulatory, and policy requirements regarding privacy.
- (iii) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system. and
- (iv) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The goal in conducting the PCLIA is to identify and mitigate privacy risks. The PCLIA ensures the business implement privacy protections and records and information management protections that are consistent with applicable laws, policies, and regulations.

The PCLIA also provides the public with notice at the system level regarding the PII Treasury is collecting, why the PII is being collected, and how the PII will be collected, used, accessed, shared, safeguarded, and stored.

The PPC Director, as the BPCLO, acts as the reviewing official for IRS PCLIAs and provides the certification needed from the function that has the unique knowledge of the information, the systems and the IRS mission that is necessary to conduct a thorough assessment. If the PCLIA is a Treasury-wide or multi-bureau PCLIA, the Deputy Assistant Secretary for Privacy Transparency and Records (DASPTR) acts as the reviewing official to approve PCLIAs that cover Treasury-wide and multi-bureau system PCLIAs.

The IRS improves upon the PCLIA development process by

- Engaging stakeholders with guidance on compliance with privacy principles by incorporating privacy by design into the into the OneSDLC process.
- Developing a malleable environment to allow for flexibility in work processes by improving upon the web-based Privacy Impact Assessment Management Systems (PIAMS) to incorporate new privacy requirements.

5.4 System of Records Notice (SORN)

The SORN is the vehicle by which the IRS notifies individuals when the organization maintains information about them in a system of records, what categories of records are maintained about them, the category of individuals covered by the system, how the information is shared externally by Treasury (routine uses), and how long the information is retained.

The Privacy Act defines a "system of records" as "a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier."

When the IRS maintains information about an individual in a system of records and retrieves the information by a personal identifier, and that system of records is not already covered by a Government Wide SORN or a Treasury Wide SORN, the IRS must update an existing SORN or develop and publish a new SORN in the *Federal Register.*

PPC oversees IRS's development and publication of IRS SORNs. The drafting of the SORNs and the required OMB and statutory documentation is the responsibility of the IRS privacy stakeholder (Business Unit or function) who operates the system of records.

If exemptions from certain Privacy Act provisions are claimed for a system of records for law enforcement or national security reasons, the bureau or office proposing the exemption also drafts a Notice of Proposed Rulemaking ("NPRM") (and the Final Rule, as needed) for publication in the *Federal Register*.

All SORNs receive a stringent legal review before they are sent to the DASPTR for approval and transmission to OMB, and Office of Information and Regulatory Affairs (OMB/OIRA.)

OMB Circular A-108, *Federal Agencies Responsibilities for Review, Reporting, and Publication under the Privacy Act.* requires that all federal agencies submit their SORNs to Office of Information and Regulatory Affairs (OIRA) for comment and approval before the SORN is published in the *Federal Register*. Circular A-108 also requires that agencies send notice to Congress 30 days before publication in the Federal Register. After receiving approval from OMB (and in the absence of comment from Congress), The IRS publishes its SORNs in the *Federal Register* before the system becomes operational.

If no comments are received from the public, the SORN becomes final without the publication of a final rule. If comments are received, the ASM/CPCLO will review them with the program manager and legal counsel before the final rule is published. An updated SORN (to address public comments) can be republished along with the final rule. After the SORN publication requirements are completed, the system of records becomes operational.

Agencies are required to establish and maintain an agency-wide privacy continuous monitoring (PCM) program. The PCM program replaced the former requirement that agencies conduct Privacy Act reviews of their SORNs on an annual basis. Information systems that maintain

systems of records are required to monitor the effectiveness of their privacy controls on an ongoing basis, document changes to the information system, and determine whether the applicable SORN(s) remains accurate or requires updating.

If a system of records is no longer needed, Treasury begins the process to remove it from its inventory. The ASM/CPCLO, through PTR, works with the program managers to determine if a system of records should be retired. If the ASM/CPCLO determines that rescission is appropriate, the relevant bureau drafts a Notice of Rescindment of a Privacy Act SOR.

The rescindment notice summarizes what information system is being retired, what the system was originally designed to collect, and why it is being retired. The notice must also provide an account of what will happen to the records that were previously maintained in the system. The ASM/CPCLO and legal counsel approve the rescindment notice before it is submitted to OMB and before publication in the *Federal Register*.

5.5 Privacy Act Statements

Privacy Act which requires an agency asking individuals to supply information that will become part of a system of records, to provide a Privacy Act Statement (PAS) on the form used to collect the information or on a separate form that can be retained by the individual. The IRS utilizes an Umbrella Privacy Act Statement to cover tax administration contacts, in addition to providing the PAS at the point of collection regardless of whether the information is collected on paper or an electronic form, on a website, on a mobile application, over the telephone, or through some other medium.

The PAS is drafted and reviewed by various privacy stakeholders. PPC and the IRS Office of General Counsel review the PAS before it is added to a form or other method of delivery to the individual from whom the IRS or Treasury collects information.

To ensure individuals have enough information to decide whether to share their information with the IRS, the PAS ensures individuals have the following information about the request:

(1) the authority (whether granted by statute or EO) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary.
(2) the principal purpose(s) for which the information is intended to be used.
(3) the published routine uses to which the information is subject.
(4) the effects on the individual, if any, of not providing all or any part of the requested. information (for example the loss or denial of a privilege, benefit, or entitlement sought if the individual does not furnish the requested information).
(5) an appropriate citation (and, if practicable, a link) to the relevant SORN(s).

5.6 Computer Matching Agreements

PPC ensures data-sharing with third parties complies with Congress's 1988 Computer Matching and Privacy Protection Act (CMPPA) if there is a Computer Matching Program as part of the data-sharing arrangement as follows:

- During the PCLIA review process and the reviews of all data sharing MOUs, privacy specialists analyze the systems, projects, agreements or other data sharing arrangements to determine if there exists any comparison of two or more automated computerized federal or non-federal system of records for the purpose of "establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirement by applicants for,

recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under a Federal benefit program or recouping payments or delinquent debts under such Federal benefits programs." (5 U.S.C. § 552a(a)(8)).

- If such a "Matching Program" exists, PPC analysts assist the owner in developing a Computer Matching Notice in accordance with the requirements of OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, that discusses the content of a "*matching notice*" as follows:

  - *A matching notice identifies the agencies involved, the purpose(s) of the matching program, the authority for conducting the matching program, the records and individuals involved, and additional details about the matching program.*

- The Data Integrity Board (DIB) established by Treasury through Treasury Directive 25-6, The Data Integrity Board, ensures CMAs include the required procedural and other protections necessary to manage the recipient agency's use of information and procedures regarding notifications to individual, information verification, record retention, and safeguarding.

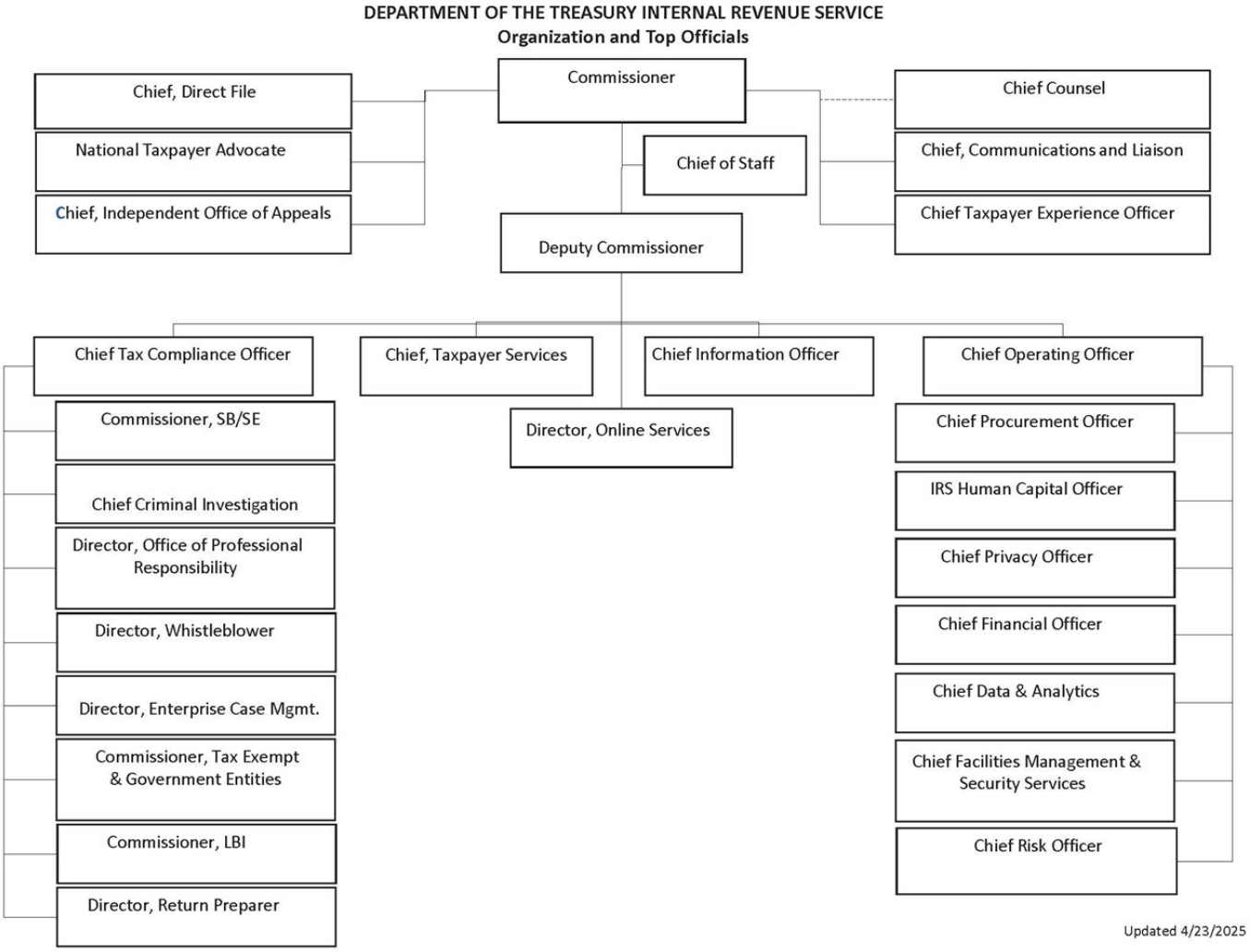
- The requirement for agencies to publish a matching notice in the Federal Register allows the Federal Government to foster transparency and accountability with respect to agencies' matching programs.

5.7 Contractors and Third-Party Requirements

PPC, along with its PGLD and IRS functional partners, implements contractor and third-party privacy and data security requirements to ensure contracts and agreements include privacy requirements by:

- Developing guidance for the privacy oversight of contractors.
- Collaborating with Cybersecurity to improve auditing of IRS systems to detect unauthorized accesses, including unauthorized access of contractors.
- Collaborating with Procurement and the Security offices on new training for Contracting Officer's Representatives (COR) regarding their contractor oversight and COR training responsibilities.
- Revising the PCLIA process to require implementation of contractor specific requirements with respect to all systems and projects involving contractor access to IRS Systems and Data.

Appendix A: Internal Revenue Service Organization Chart[10]



Appendix B1: IRS Privacy Controls
NIST SP 800-53 Revision 5 (May 2023)

Implementation, risk assessment and monitoring of these IRS Privacy controls protect the operations and assets of individuals, employees, citizens, other organizations, and the country from threats and risks stemming from cyberattacks, human error, foreign intelligence and most importantly, privacy vulnerabilities.

Privacy, Government Liaison & Disclosure (PGLD) is responsible for assessment of 31 privacy OCC controls, 61 joint OCC controls, and the following system level controls:

- AC-3(14) Access Enforcement | Individual Access
- AT-3(5) Role-based Training | Processing Personally Identifiable Information
- AU-3(3) Content of Audit Records | Limit Personally Identifiable
- CA-2 Control Assessments
- CA-5 Plan of Action and Milestones
- CA-6 Authorization
- CM-4 Impact Analysis
- MP-6 Media Sanitization
- PE-8(3) Visitor Access Records Limit Personally Identifiable Information Elements
- PL-2 System Security and Privacy Plans
- PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research
- PT-4 Consent
- PT-5 Privacy Notice
- PT-5(2) Privacy Notice | Privacy Act Statements
- PT-7(1) Specific Categories of Personally Identifiable Information | Social Security Numbers
- RA-8 Privacy Impact Assessments
- SA-8(33) Security and Privacy Engineering Principles | Minimization
- SA-11 Developer Testing and Evaluation
- SC-7(24) Boundary Protection Personally Identifiable Information
- SI-12 Information Management and Retention
- SI-12(1) Information Management and Retention | Limit Personally Identifiable Information Elements
- SI-12(3) Information Management and Retention | Information Disposal
- SI-18 Personally Identifiable Information Quality Operations
- SI-18(4) Personally Identifiable Information Quality Operations | Individual Requests
- SI-19 De-identification

Appendix B2: Privacy Organizational Common Controls (OCC)

NIST SP 800-53 Revision 5 (May 2023)

These controls are extracted from the full set of Security and Privacy controls for Information systems and organizations and are common to an organization's system security plan across the enterprise. They are the foundation of the plan and constitute protective measures used to meet the confidentiality, integrity, and availability of the organization's information systems. They can range from management constraint, personal security, and physical as well as technical security controls. The following are the controls common for privacy and are to be implemented through the efforts of PGLD.

- AC-3(14) Access Enforcement | Individual Access | Control Type: *Enhancement OCC*
- AT-3(5) Role-based Training | Processing Personally Identifiable Information |Control Type: *Enhancement OCC*
- IR-2(3) Incident Response Training | Breach | Control Type: *Enhancement OCC*
- IR-8(1) Incident Response Plan | Breaches | Control Type: *Enhancement OCC*
- PM-5(1) System Inventory | Inventory of Personally Identifiable Information | Control Type: *Enhancement OCC*
- PM-18 Privacy Program Plan | Control Type: *OCC*
- PM-19 Privacy Program Leadership Role | Control Type: *OCC*
- PM-20 Dissemination of Privacy Program Information | Control Type: *OCC*
- PM-20(1) Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services | Control Type: *Enhancement OCC*
- PM-21 Accounting of Disclosures | Control Type: *OCC*
- PM-22 Personally Identifiable Information Quality Management | Control Type: *OCC*
- PM-24 Data Integrity Board | Control Type: *OCC*
- PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research | Control Type: *OCC*
- PM-26 Complaint Management | Control Type: *OCC*
- PM-27 Privacy Reporting | Control Type: *OCC*
- PT-1 Policy and Procedures | Control Type: *OCC*
- PT-2 Authority to Process Personally Identifiable Information | Control Type: *OCC*
- PT-3 Personally Identifiable Information Processing Purposes | Control Type: *OCC*
- PT-5 Privacy Notice | Control Type: *(Partial) OCC* objectives a, b, c, d, and/or e
- PT-5(2) Privacy Notice | Privacy Act Statements | Control Type: *Enhancement OCC*
- PT-6 System of Records Notice | Type: Control Type: *OCC*
- PT-6(1) System of Records Notice | Routine Uses | Control Type: *Enhancement OCC*
- PT-6(2) System of Records Notice | Exemption Rules | Control Type: *Enhancement OCC*
- PT-7 Specific Categories of Personally Identifiable Information | Control Type: *OCC*
- PT-7(1) Specific Categories of Personally Identifiable Information | Social Security Numbers | Control Type: *Enhancement OCC*
- PT-7(2) Specific Categories of Personally Identifiable Information | First Amendment Information | Control Type: *Enhancement OCC*
- PT-8 Computer Matching Requirements | Control Type: *OCC*
- RA-8 Privacy Impact Assessments | Control Type: *OCC*
- SI-12(1) Information Management and Retention | Control Type: *Enhancement OCC*
- SI-12(2) Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research | Control Type: *Enhancement OCC*

Appendix C: Frequently Used Acronyms and Abbreviations	
BPCLO	Bureau Privacy and Civil Liberties Officer
BPRA	Business PII Risk Assessment
CPO	Chief Privacy Officer
CUI	Controlled Unclassified Information
EA	Enterprise Architecture
ELC	Enterprise Lifecycle
IM/EP	Incident Management/Employee Protection
IT	Information Technology
IRC	Internal Revenue Code
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FTI	Federal Tax Information
IA	Identity Assurance
IAPP	International Association of Privacy Professionals
IGM	Interim Guidance Memoranda
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OneSDLC	One Solution Delivery Life Cycle
OMB	Office of Management and Budget
PCA	Privacy Compliance & Assurance
PCAT	Privacy Controls Assessment Team
PCLIA	Privacy and Civil Liberties Impact Assessment
PGLD	Privacy Governmental Liaison & Disclosure
PCM	Privacy Continuous Monitoring
PIAMS	Privacy Impact Assessment Management System
PII	Personally Identifiable Information
POA&M	Plan Of Action and Milestones
POC	Point of Contact
PPC	Privacy Policy and Compliance
PP	Privacy Policy
Rev.	Revision
RIM	Records and Information Management
SAOP	Senior Agency Official for Privacy
SP	Special Publication
SSN	Social Security Number
UNAX	Unauthorized Access

Appendix D: Summary of Key Federal Privacy Statutes

- **The Privacy Act of 1974, as amended (5 U.S.C. § 552a)**, available at: https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf . The Privacy Act allows U.S. citizens and persons admitted to the U.S. for permanent residence to review personal information that is maintained about them in paper and electronic form by the federal government unless such information is specifically exempted from the access provisions. It allows these individuals to seek amendment of their records and provides for relief in federal court if the government wrongly refuses to amend, unless specifically exempted from this provision. This law requires agencies to publish systems of records notices whenever they collect personally identifiable information (PII) that is retrieved (either manually or electronically) by a unique personal identifier.

- **CMPPA of 1988, P.L. 100-503,** available at: https://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg2507.pdf . The CMPPA amended the Privacy Act to add several new provisions: 5 U.S.C. § 552a (a) (8) - (13), (e) (12), (o), (p), (q), (r), (u) (2006). The CMPPA added procedural requirements that federal agencies must follow when engaging in computer-matching activities. This includes civil liberties protections that require federal agencies to provide individuals an opportunity to receive notice and to refute adverse information before the government denies or terminates rights, benefits, or privileges. The CMPPA require that agencies engaged in matching activities establish Data Integrity Boards to oversee those activities.

- **Clinger-Cohen Act of 1996 also known as the ITMRA, P.L. 104-106**, available at: https://www.treasury.gov/privacy/Documents/Clinger-Cohen_Act_of_1996.pdf . The ITMRA together with the Federal Acquisition Reform Act became known as the Clinger-Cohen Act. ITMRA is designed to improve the way the federal government acquires, uses, and disposes of information technology. The Clinger-Cohen Act supplements the information resources management policies of the executive agencies by ensuring a comprehensive approach to improve the acquisition and management of the agency's information resources.

- **Computer Fraud and Abuse Act (CFAA) of 1986, P.L. 104-106**, available at: https://www.law.cornell.edu/uscode/text/18/1030. CFAA was enacted by Congress as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984. The law prohibits accessing a computer without authorization, or in excess of authorization.

- **Consolidated Appropriation Act (CCA) of 2005, P. L. 108-447**, available at: https://www.gpo.gov/fdsys/pkg/PLAW-108publ447/pdf/PLAW-108publ447.pdf . Section 522(a) of the CCA requires each agency to have a Chief Privacy Officer (CPO) with the responsibility of protecting privacy and safeguarding data collected from individuals. It also prescribes other roles and responsibilities of the CPO. Additionally, the Chief Privacy Officer must ensure that PII contained in a system of records is handled pursuant to the Privacy Act and adhere to the privacy reporting requirements.

- **Rehabilitation Act of 1998, Section 508,** available at: https://www.section508.gov/manage/laws-and-policies/. In 1998, Congress amended the Rehabilitation Act of 1973 (*29 U.S. C. § 794 (d)*) to require federal agencies to make their Electronic and Information Technology (EIT) accessible to people with disabilities. This law applies to all federal agencies as they develop, procure, maintain, or use information technology. Under Section 508, agencies must give disabled employees and disabled members of the public access to information that is comparable to the access available to employees and members of the public who do not have disabilities.

- **The E-Government Act of 2002, P.L. 107-347**, available at: https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm . The E-

Government Act requires every federal agency to conduct a Privacy Impact Assessment (PIA) on its IT Systems. A PIA is required when designing and developing a new information system or amending an old system that contains personally identifiable information (PII). The purpose of the PIA is to ensure that privacy protections and Privacy Act requirements are considered in developing information systems. The OMB Office of Information and Regulatory Affairs (OIRA) drafted guidelines for conducting PIAs: M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 30, 2003). Treasury has expanded the coverage of its PIA to include civil liberties. Therefore, Treasury refers to them as Privacy and Civil Liberties Impact Assessments (PCLIA).

- **The Paperwork Reduction Act (PRA) of 1995**, available at: https://www.gpo.gov/fdsys/pkg/PLAW-104publ13/html/PLAW-104publ13.htm . Congress enacted the PRA to minimize the paperwork burden that the government imposes on the public and to improve the quality of its information. PRA requires federal agencies to establish an independent review process for information collection. In the PRA, Congress established the OIRA within OMB and required that it provide guidance to and oversight of federal agencies' information collection practices. OMB has used this authority to require the posting of privacy policies on federal agencies' websites and developed restrictions on the use of "cookies" on federal websites. Federal agencies must get OMB approval before undertaking a collection of information directed to 10 or more individuals.

- **The Federal Records Act (FRA) of 1950,** as amended, available at: http://www.archives.gov/about/laws/fed-agencies.html. FRA requires the head of each federal agency to make and preserve records containing proper documentation of its functions, policies, decisions, procedures, and essential transactions to furnish the information necessary to protect the legal and financial rights of the government and of individuals directly affected by the agency's activities. The 2014 Amendments expanded the definition of Federal Records to clearly include electronic records. This is the first change to the definition of a federal record since the enactment of the Act in 1950.This Act requires agencies to establish and maintain an active program for the efficient management of the agency's records. The program must provide for:
    - Effective control over the creation, maintenance, and use of records in the conduct of current business.
    - Cooperation with the archivist at the National Archives and Records Administration (NARA) in applying standard procedures, and techniques designed to improve the management of records; and
    - Promote the maintenance and security of records and facilitate the segregation and disposal of records of temporary value.
- **The Freedom of Information Act (FOIA) of 1996, P.L. 104-231**, available at: https://www.justice.gov/oip/blog/foia-update-freedom-information-act-5-usc-sect-552-amended-public-law-no-104-231-110-stat . FOIA requires that government agencies disclose agency records unless that information is exempt from disclosure. FOIA provides two separate exemptions to protect privacy.
    - Exemption 6 authorizes agencies to withhold information contained in medical files and personnel records "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;" and
    - Exemption 7 (C) protects collected in connection with a law enforcement investigation where disclosure "would constitute an unwarranted invasion of privacy."
- **The Children's Online Privacy Protection Act (COPPA) of 1998, P.L. 105-277,** available at: https://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap91.htm . Federal agencies were not covered by the COPPA statute itself. OMB OIRA, however, extended the COPPA requirements to federal agencies as a matter of federal policy. OMB Memorandum M-03-22,

Guidance for Implementing the Privacy Provision of the E-Government Act of 2002, reinforced COPPA compliance by federal agencies and provided more detailed guidance. COPPA regulates the collection, use, and disclosure of information received from children under the age of 13 via the internet. It applies to any operator of a website who directs its material toward children under 13 and any general website operator who knows that it is collecting information from children under 13. It requires parental notice, consent, and review of information. Sites must post privacy policies and detail the personal information they collect and how they will use it. Website operators who violate COPPA could be liable for civil penalties.

- **The Health Insurance Portability and Accountability Act (HIPAA) of 1996, P.L. 104-191,** available at: https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf . Before HIPAA, health care providers routinely transferred patient medical information for reasons that had nothing to do with medical treatment or reimbursement for treatment. The HIPAA Privacy Rule applies to health information created or maintained by health care providers who participate in certain electronic transactions, health plans, and health care clearinghouses. The HIPAA Privacy Rule requires organizations to notify all patients in writing about the uses of their health information and to whom such information will be disclosed and to give patients full access to their own medical records to ensure the information in the records is only related to health care and not for marketing purposes. To ensure HIPAA compliance, organizations must establish privacy procedures, designate a privacy officer, and train employees in privacy compliance. The HIPAA Privacy Rules applies to government-operated health plans and health care providers.

- **The Federal Information Security Modernization Act (FISMA) of 2002,** 44 U.S.C. § 3541, et seq. is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (P.L. 107–347, 116 Stat. 2899) available at: https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf . FISMA (2014) requires OMB to define the term "major incident"; directs agencies to notify Congress in the event of a "major incident"; and further instructs agencies to submit an annual report regarding major incidents to OMB. The Department of Homeland Security (DHS) is to assist the OMB Director in administering the implementation of agency information and security practices for federal information systems. DHS reports to Congress on an annual basis the effectiveness of Treasury information security policies and practices that include a summary of information security incidents, thresholds for reporting major information security incidents, a summary of the results of federal agency information system risk assessments, and agency compliance with breach notification policies and procedures. The Government Accountability Office (GAO) and Comptroller General provide technical assistance to Treasury if needed.

- FISMA requires government agencies to develop and implement a robust security program to protect and safeguard their information and information systems. The ASM/CPCLO with the CIO, the CISO, the Chief Security Officer, and other officials having privacy related responsibilities play an important role in identifying and mitigating risks to PII lost.

- FISMA reports must include:
    - Threats and threat actors, vulnerabilities, and impacts.
    - Risk assessments of affected systems before, and the status of compliance of the systems at the time of, major incidents.
    - Detection, response, and remediation actions.
    - Total number of major incidents.
    - Description of the number of individuals affected by, and the information exposed by major incidents involving a breach of PII.