



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.5.2

SEPTEMBER 15, 2025

EFFECTIVE DATE

(09-15-2025)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.5.2, *Privacy and Information Protection, Privacy Compliance and Assurance (PCA) Program*.

BACKGROUND

- (1) IRM 10.5.2 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Privacy and Information Protection.

MATERIAL CHANGES

- (1) Changed Director of Privacy Policy and Compliance (PPC) to John K Hardman
- (2) 10.5.2.1, Program Scope and Objectives:
 - (5) Under Program Owner Updated link to Privacy Knowledge Management site.
 - (6) Added Primary Stakeholders - All business units are stakeholders for privacy.
 - (7) Updated contact information to Privacy Review's mailbox.
- (3) 10.5.2.1.1, Background:
 - (2) Replaced ELC with OneSDLC.
 - (3) Added contractor systems, M365, Robotic Process Automation (RPA), and Artificial Intelligence (AI) to PCLIA requirement. Removed shared storage from PCLIA requirement.
 - (4) Updated Privacy, Governmental Liaison and Disclosure (PGLD) url.
- (4) 10.5.2.1.3, Roles and Responsibilities: Updated title to conform with management and internal control standards.
- (5) 10.5.2.1.4, Program Management and Review: (10.5.2.1.4 formerly Terms, Acronyms and Related Resources) New section that identifies program reports that provide a general description of how the program is managed and how effectiveness and objectives are measured. This is a required element of management and internal control.
- (6) 10.5.2.1.5, Program Controls: New section that identifies reports used to document the program controls developed to oversee the program. This is a required element of management and internal controls.
- (7) 10.5.2.1.6, Terms and Acronyms: Added section to replace 10.5.2.1.4 Terms, Acronyms and Related Resources. Added link to new Exhibit 10.5.2-1 Glossary and Acronyms to conform with management and internal control standards. This update was made to reflect frequently used new terms in this IRM and remove terms not used in IRM 10.5.2.
- (8) 10.5.2.1.7, Related Resources: Added section with link to 10.5.1 to conform with management and internal control standards.
- (9) 10.5.2.2.1, Authority for PCLIA:
 - Added OMB M-10-23.
 - Replaced NIST SP 800-53 Rev. 4 with NIST SP 800-53 Rev. 5.

- (10) 10.5.2.2.2, PCLIA's Relevance to Privacy Compliance:
- (3) Replaced Enterprise Life Cycle (ELC) process with OneSDLC process.
 - (4) Replaced link to ELC with OneSDLC.
 - (7) Replaced link to PCLIA site with Privacy Impact Assessment Management System (PIAMS) User Guide site.
- (11) 10.5.2.2.3, PCLIA Roles and Responsibilities:
- (3) and (4) Replaced the term PTAs with PCLTA to conform with Treasury Directive (TD) 25-07, Privacy and Civil Liberties Impact Assessment (PCLIA) definition.
 - (5) Added contractor system, M365, RPA, AI, survey, and social media sites. In the third sentence replaced system with project to include all that require a PCLIA. Replaced ELC with OneSDLC.
 - (6) Added contractor system developer, M365 developer, RPA developer, AI developer, and social media site administrator.
 - (7) Added RPA Process Definition Document (PDD) as documentation to be submitted by an RPA owner. In the note replaced PCLIA website with PIAMS User Guide and added Records Retention.
- (12) 10.5.2.2.4, Privacy and Civil Liberties Threshold Assessment (PCLTA): Added new section to replace 10.5.2.2.4.1 Qualifying Questionnaire (QQ) for PCLIA and 10.5.2.2.4.3, Major Change Determination (MCD) for PCLIA. PCLTA is used to conform with TD 25-07 standards.
- (13) 10.5.2.2.5, PCLIA Updates: (Formerly 10.5.2.2.4.2) Moved to new section to align with the logical order of the PCLIA process and review. Added SBU Data and FTI.
- (14) 10.5.2.2.6, PCLIA's on IRS.gov: (Formerly 10.5.2.2.4.5) Moved to new section to align with the logical order of the PCLIA process and review. Removed the note: Do not post SharePoint PIAs on the irs.gov website, because SharePoint PIAs are obsolete.
- (15) 10.5.2.2.7, Expired PCLIA's: (Formerly 10.5.2.2.4.6 Expired and Retired PCLIA's) Moved to new section to align with the logical order of the PCLIA process and review.
- Added M365, RPA, AI, survey, and social media site
 - Replaced reference to MCD with PCLTA
 - Added a note to address one year and three expiration dates for surveys.
- (16) Removed 10.5.2.2.4.3.1, System Owner Concurrence and Approval because it's stated in 10.5.2.2.3 PCLIA Roles and Responsibilities.
- (17) 10.5.2.2.8, Retired PCLIA's (Formerly 10.5.2.2.4.6 Expired and Retired PCLIA's) Moved to new section to align with the logical order of the PCLIA process and review. Replaced reference to MCD with PCLTA.
- (18) 10.5.2.2.9, System PCLIA's (formerly 10.5.2.2.4) Moved to a new section to align with the logical order of the PCLIA process and review. Explains policy requirements for System PCLIA's; removed references to ELC and its process; added the Clinger-Cohen Act of 1996 description of Information Technology; updated PCLIA processing timeframe; added required supporting documents; and added links to other sections in 10.5.2 that explain PCLIA requirements.
- (19) 10.5.2.2.9.1, One Solution Delivery Lifecycle (OneSDLC) Readiness and Execution State: Added new section to replace 10.5.2.2.4.4 Milestone Exit Review (part of the ELC process). OneSDLC replaced Enterprise Life Cycle (ELC).

-
- (20) 10.5.2.2.9.2, Reconciliation with As-Built Architecture (ABA): (Formerly 10.5.2.2.4.7) Moved to new section to align with the logical order of the PCLIA process and review. Replaced MCD and QQ with PCLTA.
- (21) 10.5.2.2.10, Contractor System PCLIA: New section explains policy requirements for Contractor System PCLIA's.
- (22) 10.5.2.2.11, M365 PCLIA's: New section explains policy requirements for M365 PCLIA's.
- (23) 10.5.2.2.12, Robotic Process Automation (RPA) PCLIA's: New section explains policy requirements for RPA PCLIA's.
- (24) 10.5.2.2.13, Artificial Intelligence (AI) PCLIA's: New section explains policy requirements for AI PCLIA's.
- (25) 10.5.2.2.14, Adaptive PCLIA's (formerly 10.5.2.2.5): Removed SharePoint PCLIA and changed from three adaptive PCLIA's to two.
- (26) 10.5.2.2.14.1, Survey PCLIA (formerly 10.5.2.2.5.1).
- Updated note with correct IRM reference for surveys conducted via links sent by email.
 - Updated note with correct IRM reference for Recordkeeping and Accounting for Disclosures.
 - Updated note with correct link to Enterprise Architecture site.
- (27) 10.5.2.2.14.1.1, Survey PCLIA Requirements (formerly 10.5.2.2.5.1.1): Updated note changed Privacy mailbox to Privacy Review mailbox.
- (28) 10.5.2.2.14.1.2, Surveys Accessed by Links in an Email (formerly 10.5.2.2.5.1.2).
- (29) 10.5.2.2.14.1.3, Internal Surveys (formerly 10.5.2.2.5.1.3)
- (1) Updated link to Surveys Accessed by Links in an Email; removed Centra and SharePoint and added Teams Forms.
 - (2) Removed paragraph because a SharePoint PIA is no longer required.
 - (3) Updated link to Research Survey Group.
 - (4) Updated the table to spell out the words that TEMPO represent, removed SABA and added Integrated Virtual Learning Platform and Zoom.
- (30) 10.5.2.2.14.1.4, External Surveys (formerly 10.5.2.2.5.1.4)
- (1) Updated link for Surveys Accessed by Links in an Email. Updated link to Paper Reduction Act Clearances.
 - (2) Updated link to Research Survey Group site.
 - (3) Changed from Privacy mailbox to Privacy Review mailbox.
- (31) 10.5.2.2.14.2, Privacy Compliance in Collaborative Environments (formerly 10.5.2.2.5.2, Shared Storage PIAs) The SharePoint and Shared Storage PIA requirement is replaced by Information Technology Enterprise Operations (EOps) process for requesting a SharePoint or Teams Site.
- (32) Removed 10.5.2.2.5.1, Determining SharePoint PIA Requirement because there is no longer a PIA requirement for SharePoint and Shared Storage.
- (33) 10.5.2.2.14.3, Social Media PCLIA (formerly 10.5.2.2.5.3): There isn't a Social Media PCLIA site and it was replaced with a link to Communications & Liaison site.
- (34) 10.5.2.4, Business PII Risk Assessment (BPRA): Removed SharePoint and added contractor systems, M365, RPA and AI.

- (35) 10.5.2.4.1, Authority for BPRAs: Editorial changes and added authorities.
- (36) 10.5.2.4.3, BPRA Roles and Responsibilities: Revised roles and responsibilities of the BPRA team.
- (37) 10.5.2.4.4, BPRA Program Requirements: Changed the email from Privacy to Privacy Review and updated BPRA site address.
- (38) 10.5.2.5.1, Authority for Treasury PII Holdings Report: Changed NIST SP 800-53 Rev 4 to Rev. 5
- (39) 10.5.2-1: Added an exhibit of frequently used glossary and acronyms pertinent to this program. This is an element of the Internal Controls section and 10.5.2.1.6, Terms and Acronyms links to this exhibit.

EFFECT ON OTHER DOCUMENTS

This version supersedes IRM 10.5.2, Privacy Compliance and Assurance (PCA) Program, dated January 20, 2020. This IRM incorporates Interim Guidance Memorandum PGLD-10-0724-0018, Shared Storage Privacy Impact Assessments, dated July 11, 2024. This IRM also supports other IRMs in the 10.5 series.

AUDIENCE

IRM 10.5.2 must be distributed to all personnel responsible for preserving and enhancing public confidence by advocating for the protection and proper use of identity information. This policy applies to all employees, contractors, and vendors of the IRS.

John K Hardman
Acting Director, Privacy Policy and Compliance (PPC)
Privacy, Governmental Liaison and Disclosure

10.5.2

Privacy Compliance and Assurance (PCA) Program

Table of Contents

10.5.2.1 Program Scope and Objectives

10.5.2.1.1 Background

10.5.2.1.2 Authority

10.5.2.1.3 Roles and Responsibilities

10.5.2.1.4 Program Management and Review

10.5.2.1.5 Program Controls

10.5.2.1.6 Terms and Acronyms

10.5.2.1.7 Related Resources

10.5.2.2 Privacy and Civil Liberties Impact Assessment (PCLIA)

10.5.2.2.1 Authority for PCLIA

10.5.2.2.2 PCLIA's Relevance to Privacy Compliance

10.5.2.2.2.1 Civil Liberties

10.5.2.2.2.2 General PCLIA Requirements

10.5.2.2.3 PCLIA Roles and Responsibilities

10.5.2.2.4 Privacy and Civil Liberties Threshold Assessment (PCLTA)

10.5.2.2.5 PCLIA Updates

10.5.2.2.6 PCLIA's on IRS.gov

10.5.2.2.7 Expired PCLIA's

10.5.2.2.8 Retired PCLIA's

10.5.2.2.9 System PCLIA's

10.5.2.2.9.1 One Solution Delivery Lifecycle (OneSDLC) Readiness and Execution State

10.5.2.2.9.2 Reconciliation with As-Built Architecture (ABA)

10.5.2.2.10 Contractor System PCLIA's

10.5.2.2.11 M365 PCLIA's

10.5.2.2.12 Robotic Process Automation (RPA) PCLIA's

10.5.2.2.13 Artificial Intelligence (AI) PCLIA's

10.5.2.2.14 Adaptive PCLIA's

10.5.2.2.14.1 Survey PCLIA

10.5.2.2.14.1.1 Survey PCLIA Requirements

10.5.2.2.14.1.2 Surveys Accessed by Links in an Email

10.5.2.2.14.1.3 Internal Surveys

10.5.2.2.14.1.4 External Surveys

10.5.2.2.14.2 Privacy Compliance in Collaborative Environments (formerly Shared Storage PIA's)

10.5.2.2.14.3 Social Media PCLIA

10.5.2.3 Reporting

-
- 10.5.2.3.1 FISMA Reporting
 - 10.5.2.3.2 Section 803 Reporting
 - 10.5.2.4 Business PII Risk Assessment (BPRA)
 - 10.5.2.4.1 Authority for BPRAs
 - 10.5.2.4.2 BPRA Relevance to Privacy Compliance
 - 10.5.2.4.3 BPRA Roles and Responsibilities
 - 10.5.2.4.4 BPRA Program Requirements
 - 10.5.2.5 Treasury PII Holdings Report
 - 10.5.2.5.1 Authority for Treasury PII Holdings Report
 - 10.5.2.5.2 Treasury PII Holdings Report Roles and Responsibilities
 - 10.5.2.5.3 Treasury PII Holdings Report Program Requirements

Exhibits

- 10.5.2-1 Glossary and Acronyms

10.5.2.1
(09-15-2025)
**Program Scope and
Objectives**

- (1) This IRM establishes the privacy framework for privacy compliance and assurance programs and activities, including privacy risk assessments (such as Business PII Risk Assessments (BPRAs) [where is personally identifiable information (PII)], Privacy and Civil Liberties Impact Assessments (PCLIA), and Service-wide risk assessments), as well as various privacy reporting requirements.
- (2) **Purpose:** This IRM lays the foundation:
 - a. To protect the privacy of sensitive but unclassified (SBU) information of employees and taxpayers, including personally identifiable information (PII), such as tax return, financial, and employment information.
 - b. To collect, maintain, use, access, disposition, and disseminate SBU only as authorized by law and as necessary to fulfill agency responsibilities.
 - c. To implement and maintain a strong privacy program, which enables the IRS to provide effective online services.
- (3) **Audience:** The provisions in this manual apply to:
 - All offices and business, operating, and functional units within the IRS.
 - Individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, with any access to SBU information.

Note: This IRM covers all sensitive data used, operated by and on behalf of the IRS no matter what stage of the Information Technology (IT) lifecycle it is in (i.e., production, pre-production, or post-production systems). For SBU Data (including PII and tax information) that is also considered classified information, refer to IRM 10.9.1, Classified National Security Information, for additional procedures for protecting classified information.

- (4) **Policy Owner:** Privacy Compliance and Assurance (PCA) is under Privacy Policy and Compliance (PPC), within Privacy, Governmental Liaison and Disclosure (PGLD).
- (5) **Program Owner.** The Office of Privacy Compliance and Assurance (PCA) is under Privacy Policy and Compliance (PPC), within Privacy, Governmental Liaison and Disclosure (PGLD). PCA:
 - Promotes the protection of individual privacy and integrates privacy into business practices, behaviors, and technology solutions.
 - Creates, promotes, and supports privacy programs and privacy awareness Servicewide.
 - Builds privacy into IRS information collection systems using the PCLIA process.
 - Ensures IRS programs and projects gather only the taxpayer and employee data necessary to accomplish the Service's business objectives through the PCLIA and BPRA processes.
 - Protects privacy beyond the legal requirements of the Privacy Act to integrate privacy strategies into all business processes.
 - See the *Privacy Knowledge Management site* for more information.
- (6) **Primary Stakeholders.** All business units are stakeholders for privacy.
- (7) **Contact Information.** For questions about PCA or this IRM section, email the PCA office at **Privacy Review*.

10.5.2.1.1
(09-15-2025)
Background

- (1) Privacy requirements derived from IRS Privacy Principles form the basis of privacy protection within the IRS.

Note: For more information on the IRS Privacy Principles, refer to the Key Privacy Concepts section of IRM 10.5.1, Privacy Policy.

- (2) IRS policy:

- Establishes and manages privacy practices within all its offices to create a culture of privacy. This manual provides uniform policies and guidance to be used by each office.
- Protects SBU Data (including PII and tax information) at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that information.
- Allows the use, access, and disclosure of information in accordance with applicable laws, policies, federal regulations, Office of Management and Budget (OMB) Circulars, Treasury Directives (TDs), National Institute of Standards and Technology (NIST) Publications, other regulatory guidance, and best practice methodologies.
- Uses IRS-approved methodologies (One Solution Delivery Life Cycle (OneSDLC) and Enterprise Architecture (EA)) to document and improve IRS privacy compliance processes, and service efficiency and effectiveness.

- (3) This IRM covers Privacy Compliance and Assurance (PCA) programs, including, but not limited to:

- Privacy and Civil Liberties Impact Assessments (PCLIAAs) [formerly known as Privacy Impact Assessments (PIAs)] for Information Technology (IT) which includes but not limited to systems, contractor systems, Microsoft 365 (M365), robotic process automation (RPA), artificial intelligence, surveys, and social media.
- Business PII Risk Assessments (BPRA) and Limited Scope Risk Assessments (LSRAs).

- (4) Subordinate procedural guidance, such as Standard Operating Procedures (SOP) and Desk Procedures, must be used for detailed guidance and instructions for implementing and complying with the requirements within this IRM. For further information, refer to the *Privacy, Governmental Liaison and Disclosure (PGLD) site*.

- (5) IRM 10.5.1, Privacy Policy, has precedence if conflicting information is present, unless the subordinate IRM is more restrictive or otherwise noted.

- (6) The origin of privacy requirement (National Institute of Standards and Technology (NIST), Treasury, etc.) will be referenced in parenthesis at the end of the requirement.

- (7) It is acceptable to employ practices that are more restrictive than those defined in this IRM.

10.5.2.1.2
(11-19-2018)
Authority

- (1) This IRM mirrors authority from Policy reference. Refer to the Authority section of IRM 10.5.1.1.6, Privacy Policy for applicable authorities.

10.5.2.1.3
(09-15-2025)

**Roles and
Responsibilities**

- (1) The Director, Privacy Policy and Compliance (PPC) is the executive responsible for the PCA program.
- (2) The Associate Director, Privacy Compliance and Assurance (PCA), is the program manager for the PCA program.
- (3) Authorizing Officials (AOs), as defined in IRM 10.8.2, IT Security Roles and Responsibilities are required to develop and maintain additional operational documentation (e.g., action and implementation plans, standard operating procedures), necessary for implementation of the privacy controls delineated in the IRM 10.5, Privacy and Information Protection series. Therefore, implementation of privacy policy is the responsibility of the owning AO to include documentation and procedures for how their information systems are managed, administered, and monitored.
- (4) For the purpose of this IRM, the following roles for IRS personnel apply:
 - Employees
 - Consultants
 - Detailees
 - Temporary employees
 - Interns
 - IRS contractors and subcontractors

Note: Authorized or Unauthorized personnel refers to all IRS personnel being authorized or unauthorized to perform a particular action.

10.5.2.1.4
(09-15-2025)

**Program Management
and Review**

- (1) **Program Reports**
 1. PCA in PGLD manages the PCLIA and BPRA programs through the following reviews and reports:
 - a. All approved PCLIAs are segmented into monthly approved PCLIA reports and are provided in the PGLD PCA Quarterly Operation reviews.
 - b. Specifies types of personally identifiable information (PII) and federal tax information (FTI) used in systems, contract systems, M365, Robotic Process Automation (RPA), Artificial Intelligence (AI), surveys and social media are documented in PCLIAs.
 - c. Expired and replaced PCLIAs to ensure business units are compliant with submitting updated PCLIAs.
 - d. The BPRA Chief prepares and reports quarterly operation review data on important BPRA activities such as status/accomplishments, planned, pending and completed BPRAs, upcoming training, program changes, etc. The operation review data is forwarded to business executives and other impacted management.

10.5.2.1.5
(09-15-2025)

Program Controls

- (1) Business Entitlement Access Request System (BEARS) is used to grant access to the Privacy Impact Management System (PIAMS) based on the user's role.
- (2) The requirements within this policy follow privacy controls within NIST SP 800-53 Rev 5.

10.5.2.1.6
(09-15-2025)

Terms and Acronyms

- (1) See Exhibit 10.5.2-1 Glossary and Acronyms

10.5.2.1.7
(09-15-2025)

Related Resources

- (1) See IRM 10.5.1, Privacy Policy for Related Resources.

10.5.2.2
(01-24-2020)

Privacy and Civil Liberties Impact Assessment (PCLIA)

- (1) The IRS recognizes the importance of protecting the privacy of taxpayers and employees. The statutorily required vehicle for addressing privacy issues in a system is the Privacy Impact Assessment (PIA). The IRS Privacy and Civil Liberties Impact Assessment (PCLIA) includes questions that relate directly to the First Amendment and the protection of individual civil liberties.
- (2) Title II Section 208 of the E-Government Act of 2002 requires agencies to conduct PCLIA's before:
 - Developing or procuring information technology (IT) systems or projects that collect, maintain or disseminate information in identifiable form (such as PII) from or about members of the public, or
 - Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for ten (10) or more persons.
- (3) The Clinger-Cohen Act of 1996 describes IT as any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
- (4) A PCLIA is a process analyzing how SBU Data (including PII and tax information) are used, collected, received, displayed, stored, maintained, protected, shared, managed, and disposed. Because the analysis may result in a publicly available report, a PCLIA also refers to the document that covers the assessment.
- (5) The PCLIA process applies to IRS IT systems, applications, projects, and databases – including those in pilot status, technology demonstration, testing or experimental phases, and early stages of development.
- (6) IRS policy requires PCLIA's on internal systems and systems with information about IRS personnel, at the recommendation of the Office of Management and Budget, outlined in OMB Memo (M) 03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, and OMB M 14-04, FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.

10.5.2.2.1
(09-15-2025)

Authority for PCLIA

- (1) For authoritative sources, refer to:
- E-Government Act of 2002, Section 208.
 - Internal Revenue Code (IRC), 26 U.S.C. 6103
 - OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
 - OMB M-10-23, OMB Guidance for Agency Use of Third-Party Websites and Applications.
 - Privacy Act of 1974, as Amended 5 U.S.C 552a:
Office of Privacy and Civil Liberties.

- NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations, September 2020.
- Amendments (specifically First and Fourth) to the U.S. Constitution: *United States Senate*.
- IRM 1.15, Records and Information Management, and *Records and Information Management (RIM) site*.

10.5.2.2.2
(09-15-2025)
PCLIA's Relevance to Privacy Compliance

- (1) The purpose of a PCLIA is to demonstrate that program managers, system owners, and developers have incorporated privacy and civil liberties protections throughout the entire lifecycle of a system. This ensures privacy and civil liberties protections are built into the system from the beginning, when it is less costly and more effective to include them.
- (2) The PCLIA process should be initiated as early in the system lifecycle as possible (e.g., the planning stage) so that technical solutions can be incorporated into system design as necessary to remediate privacy and civil liberties concerns identified during the PCLIA process.
- (3) System Owners must self-certify with OneSDLC that a PCLTA or PCLIA was approved by The Office of Privacy Review. (Also see the OneSDLC section IRM 10.5.2.2.9.1, OneSolution Delivery Lifecycle (OneSDLC) Readiness and Execution State).
- (4) For more information refer to *OneSDLC* site.
- (5) A Privacy PCLIA is a decision tool used to identify and mitigate privacy risks that notifies the public: *U.S. Department of the Treasury*.
 - What PII the IRS is collecting.
 - Why the PII is being collected.
 - How the PII will be used, collected, received, displayed, stored, maintained, protected, shared, managed, and disposed.
- (6) A PCLIA should accomplish these goals:
 - Ensure conformance with applicable legal, regulatory, and policy requirements for privacy.
 - Determine privacy risks and effects.
 - Evaluate protections and alternative processes to mitigate potential privacy risks.
 - Provide assurance to the public about the protection of privacy and constitutional rights.
- (7) For more information about the PCLIA process (including how to determine if a PCLIA is required), refer to the *Privacy Impact Assessment Management System (PIAMS) User Guide*.

10.5.2.2.2.1
(01-24-2020)
Civil Liberties

- (1) The PCLIA includes consideration of how systems affect a person's civil liberties as part of the assessment's protection of the individual's privacy and constitutional rights.
- (2) The Privacy Act prohibits federal agencies from maintaining records on how any individual exercises First Amendment rights unless certain exceptions apply. These rights include religious and political beliefs, freedom of speech and of the press, and freedom of assembly and petition.

5 U.S.C 552a(e)(7)(The Privacy Act) provides in part that federal executive agencies must “maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.”

- (3) While systems do not collect this information exclusively, the broad scope of tax return information means many returns will include information related to First Amendment rights, such as charitable contributions or income/deductions. For such activities, IRS systems cannot exclusively collect information about how an individual exercises First Amendment rights.
- (4) The PCLIA acknowledges information stored in or collected by a system that can identify, locate, and monitor individuals or groups of people, or if the system information is used for data mining and thereby could be seen as infringing upon a person’s civil liberties.
- (5) Other Amendments relative to the civil liberties concerns within IRS systems:
 - Fourth Amendment – Protects against unreasonable search and seizure.
The Fourth Amendment provides that “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
 - Fifth Amendment – Protects an individual from self-incrimination.
The Fifth Amendment provides that “No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.”
 - Fourteenth Amendment – Citizenship rights and equal protection.
The Fourteenth Amendment obligates states not to deny “the equal protection of the laws.”

Note: Both the Fifth and Fourteenth Amendments contain a “due process clause” providing protection against arbitrary federal government actions. In designing procedures and policies cited in the PCLIA, IRS officials must ensure that the IRS enforcement actions, such as placing liens; comply with the Internal Revenue Code (IRC); and provide due process for the taxpayer.

- (6) The PCLIA includes civil liberties questions per Treasury’s PCLIA Template and Guidance. The purpose for these questions is to:
 - Identify civil liberties risks in systems that maintain PII;
 - Ensure compliance with legal, regulatory, and policy requirements;
 - Analyze civil liberties risks;

- Identify remedies, protections, and alternative or additional privacy controls necessary to mitigate those risks; and
- Provide notice to the public of privacy and civil liberties practices.

10.5.2.2.2
(11-19-2018)
**General PCLIA
Requirements**

- (1) The PCLIA must meet guidelines for IRS publications, such as the Plain Writing Act of 2010.
- (2) The following is a list of some guidelines to consider in meeting these requirements:
 - *Remember the audience (i.e., the public) and use plain English.* The PCLIA should be written in a manner that allows the public to understand the activities being described.
 - *Use short sentences.* Sentences should generally be kept under 20 words. The more words in a sentence, the more likely that a member of the public will not understand what is being said.
 - *Do not write from the perspective of a person who is familiar with the program.* Avoid technical jargon and terminology that is known only to personnel inside your business unit.
 - *The amount of detail.* The PCLIA should be written with sufficient detail to permit Privacy Review (PR) to analyze the privacy risks and mitigation steps. There should also be enough detail to allow the public to understand your program, its risks, and the measures you have taken to mitigate those risks.
 - *Explain/Define Acronyms.* Spell out each acronym the first time it is used in the document.
 - *Proofread your document before submitting it.* **This document is meant to be published on the IRS public-facing web site.** Any PCLIA submitted for review should be free of spelling and grammatical errors. As a best practice, the document should be reviewed by someone who is unfamiliar with the system or project before it is submitted for review.

10.5.2.2.3
(09-15-2025)
**PCLIA Roles and
Responsibilities**

- (1) Protecting privacy and civil liberties is the responsibility of every IRS employee. However, specific responsibilities apply to individuals who prepare, maintain, and approve the various PCLIAs. Refer to IRM 10.8.2, IT Security Roles and Responsibilities for how these roles apply to information technology development and security.
- (2) The IRS **Senior Agency Official for Privacy** (SAOP) has oversight responsibility for accounting to Treasury, OMB, and other regulatory agencies regarding the IRS' implementation of information privacy protections, including full compliance with federal laws, regulations and policies relating to information protection, as established by the Division H, Title V, section 522 of the Consolidated Appropriations Act of 2005.
- (3) The **Privacy Review Analyst** (PRA) must:
 - Provide end-to-end support from tracking, reviewing, providing feedback, securing supporting documentation to corroborate answers, addressing privacy risks and final signing of PCLIA/PCLTAs submitted by IRS business units as required by the Privacy Act & E-Government Act of 2002.

- Review available system documentation, related IRMs, job aids and System of Records Notices (SORNs) prior to forwarding PCLIA for approval.
 - Develop analysis and reports to identify and document ongoing PCLIA related completion rates, patterns, trends, risks, targeted training needs, remediation opportunities, related metrics, and elevate heightened privacy risks to leadership, when warranted.
 - Provide guidance toward the completion of PCLIA and assist in strengthening the PCLIA process for IRS stakeholders (workflow, monitoring, reporting, processing, etc.)
- (4) The **Privacy Review Manager** must review all PIAs/PCLIA/PCLTAs for completeness, including the Privacy analyst findings and case notes prior to forwarding to the Associate Director of Privacy Compliance and Assurance for approval memo or report signature. The Privacy Review Manager also provides guidance and final determination regarding approving a PCLIA with risk noted.
- (5) The **Business Owner, Survey Owner, Site Owner or System Owner (SO)** or accrediting official, must be a senior management/executive official government employee with the authority to formally assume responsibility for operating a system, contractor system, M365, RPA, AI, survey, and social Media site at an acceptable level of risk. As the approver, the SO attests that the PCLIA correctly documents substantial facts about the system, contractor system, M365, RPA, AI, survey, and social media site. The SO must ensure the PCLIA process begins in the early stages of the development of a project and complete it as part of the system's required OneSDLC review. Additionally, the SO must mitigate privacy findings or complete a Risk Acceptance Findings Tool (RAFT), as necessary. The System Owner may designate someone to approve the PCLIA.
- (6) **System Developer, Contractor System Developer, M365 Developer, RPA Developer, AI Developer, Survey Administrator, Social Media Site Administrator, Project Manager, and Subject Matter Expert (SME)** are terms applied to the individuals who carry out the development and implementation of the project. They must answer the PCLIA questions and those posed by Privacy Analysts. In PIAMS, the Project Manager approves the PCLIA for submission to Privacy Review.
- (7) The **PCLIA Preparer** may be anyone designated by the SO, including the SO, who completes the applicable form and works with the Privacy Analyst to identify and address any risks. This role includes responsibility to:
- Work with various team members, such as the SO and SME team, to research a project's privacy and civil liberties protections.
 - Review other privacy and security documentation relevant to the system, such as System Security Plan (SSP) or Robotic Process Automation (RPA) Process Definition Document (PDD) to ensure consistency with the PCLIA.
 - Consider privacy at every stage of the product lifecycle: planning, design, development, and testing.
 - Begin preparation of the PCLIA as early as possible, and continually revisit it to ensure the information contained is still accurate.
 - Complete the form in PIAMS.

- Identify if the PCLIA applies to a system that is a System of Records (SOR); then, if needed, list the System of Records Notice (SORN) or create a SORN.

Note: Refer to the *PIAMS User Guide* for more information on PIAMS, SORs, SORNs, and Records Retention, the related procedures, and the underlying legal requirements.

10.5.2.2.4
(09-15-2025)
**Privacy and Civil
Liberties Threshold
Assessment (PCLTA)**

- (1) A Privacy and Civil Liberties Threshold Assessment (PCLTA) is a written risk assessment a Business Owner, System Owner, Contractor System Owner, M365 Project Owner, RPA Project Owner, AI Project Owner, Survey Owner, and Social Media Site Owner is required to complete when:
 - A new Information Technology (IT) and Survey will contain SBU Data (including PII and tax information) about the public, taxpayers, or IRS employees. Generally, answering yes to any of the questions requires the completion of a full PCLIA.
 - If entering into an Information Sharing Agreement with a contractor or vendor that involves custody of or access to IRS-held PII, a Privacy Threshold Assessment can be used to identify and document any additional privacy compliance requirements.
 - To document a Reviewing Official's determination that a PCLIA is not required.
 - Considering an enhancement or modification (major change) of existing information technology or changes to a survey (e.g., to determine if the modification will result in SBU Data, PII, or FTI being added or created). For information about major changes see PCLIA Updates see IRM 10.5.2.2.5, PCLIA Updates.

Note: A PCLTA is not required for Social Media sites, because a PCLIA must be completed whenever an agency's use of a third-party website or application makes PII available to the agency. For more information about PCLIA requirements for Social Media sites, see OMB M-10-23 Guidance for Agency Use of Third-Party Websites and Applications.

10.5.2.2.5
(09-15-2025)
PCLIA Updates

- (1) Generally, agencies must update or file new PCLIAs when a system change creates new privacy risks. The IRS requires PCLIA updates every three years, or sooner for new privacy risks.
- (2) Major changes requiring PCLIA updates include:
 - Changes/additions to the SBU Data, PII, and FTI being collected.
 - Changes to the use of SBU Data, PII, and FTI.
 - The business unit's or system's use of data changes.
 - Conversions - when converting paper-based records to electronic systems.
 - Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form.
 - Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such

additions could create a more open environment and avenues for exposure of data that previously did not exist.

- Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases, or otherwise significantly manipulated.
- New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public (refer to the Electronic Risk Assessment section in this IRM).
- Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PCLIA requirement).
- New Interagency Uses - when federal agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government Act of 2002 initiatives; in such cases, the lead agency should prepare the PCLIA.
- Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:

For example, agencies that participate in E-Government Act of 2002 initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Government Act of 2002 requirements. In most cases, the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.

10.5.2.2.6 (09-15-2025) PCLIA on IRS.gov

- (1) The IRS posts PCLIA with PII on members of the public in compliance with the E-Government Act of 2002:
 - *Privacy Act*
 - *Privacy Impact Assessment (PIA)*
- (2) The E-Government Act of 2002 allows agencies to make decisions to determine what information in a government system should be redacted, or if for compelling security or privacy reasons, a PCLIA should not be posted. SOs (business owners and systems developers) will be instructed to remove certain information within PCLIA that could cause harm to systems or processes or is not in the best interest of the agency to have published, such as:
 - a. References to version numbers, release numbers, specifications (but name of specifications is allowed).
 - b. References to specific security technology, including brand names. Even though a contract is public information, associating the name of the company with a particular IRS system may make the document too sensitive to post. Recognize customer concerns and err on the side of redaction and/or non-disclosure.
 - c. References to SmartCard technologies.
 - d. References to allowable tolerances.

- e. Proper nouns of persons (PII).
- f. Names of IRS locations, servers, and other information regarding or describing IRS processes.

Note: In most instances, this type of information should not be included in a PCLIA. Privacy Analysts are responsible to inform business owners not to include information that does not add value to the privacy review or to suggest edits that remove the information prior to approval of the PCLIA.

- (3) SOs will be notified when a PCLIA is approved and if the PCLIA is designated to post to IRS.gov. The SO will have 10 business days to provide redaction recommendations from the PCLIA prior to posting and return to PCA.
- (4) PCA must:
 - a. Ask the Business Units to mark any portion of the PCLIA that might cause harm to the IRS or any party if disclosed to the public and return to The Office of Privacy Review.
 - b. Send approved PCLIAs to the Office of Disclosure for redaction of items that cannot be made public. Redactions withhold information that, if released might harm systems, compromise law enforcement efforts, or jeopardize competitive business interests.
 - c. Coordinate the posting of redacted PCLIAs with the PGLD Posting Analyst on the IRS.gov website.
- (5) The E-Government Act of 2002 requires redactions, as allowed by FOIA. The Disclosure Analyst must use available FOIA exemptions to redact information from the PCLIA.
- (6) If a business owner believes that their PCLIA is exempt in its entirety from being posted to IRS.gov, the business owner will be directed to provide the authority for not posting and work with the Office of Disclosure to resolve the matter. Office of Disclosure may require a ruling from the Office of Chief Counsel. However, if the information is discloseable per FOIA, PCA will be required to post the PCLIA to IRS.gov, and will work with the business owner and Disclosure to determine if a summary of the PCLIA would be allowed.

10.5.2.2.7 (09-15-2025) Expired PCLIAs

- (1) An expired PCLIA must be updated to reflect how changes may affect the sensitive information in a system, contractor system, M365, RPA, AI, survey, or social media.
- (2) A PCLTA questionnaire is used to determine if a new PCLIA is needed. For more information, see the section PCLTA in this IRM (IRM 10.5.2.2.4, Privacy and Civil Liberties Threshold Assessment (PCLTA)).
- (3) If an updated or amended PCLIA is approved prior to the 3-year expiration date, the previous PCLIA is superseded as it has been replaced with a newer version.
- (4) It is the responsibility of the SO, project owner and the SME to update a PCLIA before the PCLIA expires. PCA will contact the SO, project owner and the SME 90 days prior to the expiration date giving notification that a new PCLIA is due. Two more attempts will be made at 60 days (second notice) and 30 days (third and final notice) prior to PCLIA expiration.

- (5) Because the PCLIA process could take up to 30 business days (preparation, review, and approval), the SO, project owner and SME must be mindful of the time frames needed to complete the PCLIA and remain compliant with the E-Government Act of 2002. The new approved PCLIA will replace the expired PCLIA, restarting the 3-year cycle.

Note: Surveys can have a 1-year expiration date and 3-year expiration date. For more information about surveys see IRM 10.5.2.2.14.1, Survey PCLIA

10.5.2.2.8
(09-15-2025)
Retired PCLIA

- (1) A PCLTA questionnaire is required for systems, contractor systems, M365, RPA, AI, surveys, and social media sites that have been retired. For systems The Office of Privacy Review will work with the As-Built Architecture (ABA) to identify retired systems. For more information, see IRM 10.5.2.2.9.2 Reconciliation with As-Built Architecture (ABA). The retired PCLIA will be stored in PIAMS for the appropriate retention period.

10.5.2.2.9
(09-15-2025)
System PCLIA

- (1) A system is included in the definition of Information Technology (IT). The Clinger-Cohen Act of 1996 describes IT as any equipment, software or inter-connected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
- (2) A System PCLIA is a process analyzing how SBU Data (including PII and tax information) are used, collected, received, displayed, stored, maintained, protected, shared, managed, and disposed.
- (3) A PCLIA should be submitted to The Office of Privacy Review in the Initial Production Deployment process of OneSDLC. The PCLIA helps identify privacy or civil liberties issues early on, thereby facilitating the development of technical solutions necessary to remediate and/or mitigate any potential privacy and civil liberties concerns.
- (4) Submit a System PCLIA at least 30 business days prior to the date needed for releases or to begin production and use of the PII contained in the system.
- (5) Include supporting documents with the System PCLIA to corroborate your answers. For information about the supporting documents see the *PIAMS User Guide*. Projects must follow the Enterprise Architecture (EA) IRS Privacy Requirements in IRM 2.15.1, Enterprise Architecture (EA) Overview which are based on mandated NIST SP privacy controls.
- (6) For more information about PCLIA requirements and the PCLIA process (including how to determine if a new or updated PCLIA is required), refer to the following IRM references:
 - IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - IRM 10.5.2.2.1, Authority for PCLIA
 - IRM 10.5.2.2.2, PCLIA Relevance to Privacy Compliance
 - IRM 10.5.2.2.2.1, Civil Liberties
 - IRM 10.5.2.2.4, Privacy and Civil Liberties Threshold Assessment (PCLTA)
 - IRM 10.5.2.2.5, PCLIA Updates
 - IRM 10.5.2.2.6, PCLIA on IRS.gov
 - IRM 10.5.2.2.7, Expired PCLIA
 - IRM 10.5.2.2.8, Retired PCLIA

10.5.2.2.9.1
(09-15-2025)
**One Solution Delivery
Lifecycle (OneSDLC)
Readiness and
Execution State**

- (1) In the Readiness state the Product Manager and Deployment Authorizing Official (DAO) must certify that a PCLTA or PCLIA was completed with other compliance requirements by using the Initial Production Deployment Artifact Checklist. The Product Team works with the process owners to complete all requirements.
- (2) The Execution state includes the Prior-to-Production (P2P) Compliance Process and Product Review process. The PCLTA and PCLIA are part of the compliance requirements.

The OneSDLC Prior-to-Production process requires the Product Manager and DAO to certify that a PCLTA or PCLIA was completed with other compliance requirements by using the Prior-to-Production Checklist. The Product Team works with the process owners to complete all requirements. The Product Team receives deployment approval from the Product Manager and DAO for each production deployment and saves the completed checklist to their document repository for each deployment.

The OneSDLC Product Review Process requires the Product Manager to certify that a PCLTA or PCLIA was completed with other compliance requirements by using the Product Review Artifact Checklist. The Product Review Process is held at the end of each 6-month Product Cycle and is a required event to share outcomes and gather feedback from the product's governing body on work completed in the ending Product Cycle and to project work for the next product cycle. Prior to the Product Review, product teams work with process owners to complete/update all requirements. The Product Manager certifies all requirements are completed/updated by signing the Product Review Artifact Checklist.

- (3) For more information about OneSDLC refer to IRM 2.31.1, One Solution Delivery Life Cycle Guidance and *OneSDLC site*.

10.5.2.2.9.2
(09-15-2025)
**Reconciliation with
As-Built Architecture
(ABA)**

- (1) IRS Enterprise Architecture Division's *ABA website* presents an enterprise view of the IRS' current Information Technology and Business environments.
- (2) The reasons why PCA might contact a business owner about the ABA are:
 - a. A system is added to the ABA that contains PII and a PCLIA cannot be found. Once contacted by PCA, the owner must begin completing a PCLIA in PIAMS.
 - b. A system with a PCLIA is retired in the ABA. If PCA does not have any record of the retirement, the business owner will be asked to fill out a PCLTA questionnaire indicating the system is retired.
 - c. A system currently on the ABA that should have a PCLIA or PCLTA will be contacted by PCA to determine if one is needed or which questionnaire should be filled out by the business owner.
- (3) If a system needs to update their entry within the ABA or have their system added to the ABA, consult the *As-Built Architecture* for information on what forms to use and where to send the information.
- (4) PCA adds PCLIA information to systems on the ABA.

10.5.2.2.10
(09-15-2025)
**Contractor System
PCLIA**s

- (1) A system owned by a contractor with IRS data has the same PCLIA requirements as an IRS owned system.
- (2) For information about System PCLIA's see IRM 10.5.2.2.9, System PCLIA's.
- (3) For more information about PCLIA requirements and the PCLIA process (including how to determine if a new or updated PCLIA is required), refer to the following IRM references:
 - IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - IRM 10.5.2.2.1, Authority for PCLIA
 - IRM 10.5.2.2.2, PCLIA Relevance to Privacy Compliance
 - IRM 10.5.2.2.2.1, Civil Liberties
 - IRM 10.5.2.2.4, Privacy and Civil Liberties Threshold Assessment (PCLTA)
 - IRM 10.5.2.2.5, PCLIA Updates
 - IRM 10.5.2.2.6, PCLIA's on IRS.gov
 - IRM 10.5.2.2.7, Expired PCLIA's
 - IRM 10.5.2.2.8, Retired PCLIA's

10.5.2.2.11
(09-15-2025)
M365 PCLIAs

- (1) Dedicated environments and visualization tools are information technology and an M365 PCLIA is used to analyze privacy risk in dedicated environments and the use of visualization tools.
- (2) An M365 PCLIA is a process analyzing how SBU Data (including PII and tax information) are used, collected, received, displayed, stored, maintained, protected, shared, managed, and disposed.
- (3) Submit a M365 PCLIA at least 30 business days prior to the date needed for milestones, releases, or to begin production and use of the PII contained in the system.
- (4) Include supporting documents with the M365 PCLIA. For information about the supporting documents see the *PIAMS User Guide*.
- (5) For more information about PCLIA requirements and the PCLIA process (including how to determine if a new or updated PCLIA is required), refer to the following IRM references:
 - IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - IRM 10.5.2.2.1, Authority for PCLIA
 - IRM 10.5.2.2.2, PCLIA Relevance to Privacy Compliance
 - IRM 10.5.2.2.2.1, Civil Liberties
 - IRM 10.5.2.2.4, Privacy and Civil Liberties Threshold Assessment (PCLTA)
 - IRM 10.5.2.2.5, PCLIA Updates
 - IRM 10.5.2.2.6, PCLIA's on IRS.gov
 - IRM 10.5.2.2.7, Expired PCLIA's
 - IRM 10.5.2.2.8, Retired PCLIA's

10.5.2.2.12
(09-15-2025)
**Robotic Process
Automation (RPA)
PCLIA**

- (1) Robotic Process Automation (RPA) is a software technology that makes it easy to build, deploy, and manage software robots that emulate human actions interacting with digital systems and software. Software robots can do things like understand what's on a screen, complete the right keystrokes, navigate systems, identify and extract data, and perform a wide range of defined actions. RPAs can have an AI or machine learning component.
- (2) There are two types of RPAs used by the IRS.
 - a. Attended RPAs requires human input and oversight to function.
 - b. Unattended RPAs run automation that operates on a Virtual Machine (VM) utilizing designated Non-Person Entity (NPE) access credentials. Unattended RPAs function as the name indicates, pre-programmed to carry out the automation's specific programming actions. Human-in-the-Loop auditing ensures proper adherence to policy.
- (3) An RPA PCLIA is a process analyzing how SBU Data (including PII and tax information) are used, collected, received, displayed, stored, maintained, protected, shared, managed, and disposed.
- (4) Submit an RPA PCLIA at least 30 business days prior to the date of deployment, releases, and use of the PII by the RPA.
- (5) Include supporting documents with the RPA PCLIA. For information about the supporting documents see the *PIAMS User Guide*.
- (6) An RPA PCLIA may be completed to cover multiple RPAs if their uses are for the same business unit and system and use the same SBU Data, PII, and FTI.
- (7) For more information about PCLIA requirements and the PCLIA process (including how to determine if a new or updated PCLIA is required), refer to the following IRM references:
 - IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - IRM 10.5.2.2.1, Authority for PCLIA
 - IRM 10.5.2.2.2, PCLIA Relevance to Privacy Compliance
 - IRM 10.5.2.2.2.1, Civil Liberties
 - IRM 10.5.2.2.4, Privacy and Civil Liberties Threshold Assessment (PCLTA)
 - IRM 10.5.2.2.5, PCLIA Updates
 - IRM 10.5.2.2.6, PCLIA on IRS.gov
 - IRM 10.5.2.2.7, Expired PCLIA
 - IRM 10.5.2.2.8, Retired PCLIA

10.5.2.2.13
(09-15-2025)
**Artificial Intelligence (AI)
PCLIA**

- (1) Artificial Intelligence is information technology.
- (2) Examples of AI or associated technology include, but are not limited to:
 - Generative AI
 - Predictive AI
 - Machine Learning (ML)
 - Large Language Models (LLM)
 - Voicebots and chatbots

Note: AI capabilities often appear as part of many other tools, applications, or commercial off the shelf (COTS) products, without expressly being identified as an AI.

- (3) For an overarching IRS AI policy and definition, refer to the *internal Enterprise AI site*.
- (4) An AI PCLIA is a process analyzing how SBU Data (including PII and tax information) is used, collected, received, displayed, stored, maintained, protected, shared, managed, and disposed of by AI.
- (5) Submit an AI PCLIA at least 30 business days prior to the date of deployment, releases, and use of the PII by AI.
- (6) Include supporting documents with the AI PCLIA. For information about the supporting documents see the *PIAMS User Guide*.
- (7) For more information about PCLIA requirements and the PCLIA process (including how to determine if a new or updated PCLIA is required), refer to the following IRM references:
 - IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
 - IRM 10.5.2.2.1, Authority for PCLIA
 - IRM 10.5.2.2.2, PCLIA Relevance to Privacy Compliance
 - IRM 10.5.2.2.2.1, Civil Liberties
 - IRM 10.5.2.2.4, Privacy and Civil Liberties Threshold Assessment (PCLTA)
 - IRM 10.5.2.2.5, PCLIA Updates
 - IRM 10.5.2.2.6, PCLIA on IRS.gov
 - IRM 10.5.2.2.7, Expired PCLIA
 - IRM 10.5.2.2.8, Retired PCLIA
- (8) For privacy policy on AI, refer to IRM 10.5.1.6.22, Artificial Intelligence (AI), and its subsections.

10.5.2.2.14
(09-15-2025)
Adaptive PCLIA

- (1) IRS developed unique PCLIA, referred to as “adaptive,” to address the specific issues and privacy concerns for non-conventional data and collaborative environments that were not addressed in the general PCLIA used for systems. Doing this complies with OMB M-03-22 and M-10-23, as well as the Title II Section 208 of the E-Government Act of 2002. Other adaptive PCLIA may be developed in the future to proactively focus on privacy concerns identified with other uses of non-conventional data or collaborative environments. Currently, the IRS utilizes two adaptive PCLIA to cover surveys and social media sites.
- (2) A System PCLIA that addresses all issues included in an adaptive PCLIA usually overrides the need for the adaptive PCLIA.

10.5.2.2.14.1
(09-15-2025)
Survey PCLIA

- (1) Surveys of the public or employees require a Survey Privacy and Civil Liberties Impact Assessment (PCLIA), as mandated by the E-Government Act of 2002, when:
 - a. Developing or procuring information technology (IT) systems or projects that collect, maintain or disseminate information in identifiable form (such as PII) from or about members of the public, or
 - b. Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for ten (10) or more persons.

Note: These requirements also apply to information collections maintained by contractors and subcontractors for federal agency contracts.

- (2) An important and useful tool for the IRS, surveys are any measurement procedure that involves asking standardized questions of a selected group of respondents representing a particular population. Surveys provide a critical source of data and insights which measure a variety of employee and customer opinions.

Note: For the purposes of this IRM the term “survey” applies to any data collection method, including but not limited to surveys, focus groups, interviews, pilot studies, and field tests.

- (3) Surveys have a variety of purposes and can be conducted in many ways. There are two types of surveys conducted by the IRS.
- a. Internal surveys which are used to solicit input from agency personnel. For survey PCLIA requirements, see the Internal Surveys section of this IRM.
 - b. External surveys which are used to solicit input from taxpayers, tax practitioners, or vendors. For survey PCLIA requirements, see the External Surveys section of this IRM.
- (4) There are four methods of survey data collection that are commonly used:
- a. Face-to-face surveys, interviews, and Focus Groups (Focus Groups)
 - b. Telephone surveys, interviews, and Focus Groups
 - c. Self-administered paper and pencil surveys
 - d. Self-administered computer surveys (typically online or link sent via email)

Note: For surveys conducted via links sent by email, see IRM 10.5.2.2.14.1.2, Surveys Access by Links in an Email.

- (5) Privacy issues arise with surveys because they commonly collect personally identifiable information (PII) and sensitive but unclassified (SBU) data. PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. For more information and a complete description of IRS policy on SBU Data (including PII and tax information), refer to the Key Privacy Definitions section of IRM 10.5.1, Privacy Policy.
- (6) Because surveys may be anonymous or non-anonymous, notification to participants of the level of anonymity must be clear. Data collected for statistical purposes under pledges of confidentiality or similar promises is governed by the 2002 Confidential Information Protection and Statistical Efficiency Act (CIPSEA). CIPSEA makes intentional use of results for other purposes a felony unless certain exceptions for disclosures for qualifying law enforcement purposes apply or additional informed consent is obtained from respondents. See: *Statute-116*.
- (7) Survey Administrators are not required to maintain anonymity in their data collection systems if they:
- a. have appropriate clearance to obtain PII (contractors must be covered by proper Privacy and Security clauses)
 - b. do not associate PII with individual responses
 - c. do not provide any PII in their response to the requesting business unit
 - d. do not utilize responses for any other purpose or survey.

Note: This anonymity exemption applies to the systems used to collect, aggregate and analyze data. Survey Administrators must notify participants if they may be associated with their responses (not anonymous) after the data collection and analysis.

- (8) When choosing a vendor as a Survey Administrator, the Survey Owner must actively engage Procurement during the selection process to ensure that sufficient privacy and security safeguards are in the contract.

Note: Refer to IRM 11.3.37, Recordkeeping and Accounting for Disclosures to determine applicable requirements for Privacy Act accounting of non-tax disclosures.

- (9) Employees must not conduct internal or external Surveys or Focus Groups as part of their external professional or educational studies. All collections of data must directly relate to an IRS business need and use. Surveys that utilize IRS contacts or resources purely for personal gain are prohibited.
- (10) IRS regulations do not allow use of Cloud Computing or Open-Source software to conduct surveys unless an exception is obtained by submitting a change request through IRS Enterprise Architecture (EA). Information is also available in IRM 10.8.24, Cloud Computing Security Policy.
 - a. Web-based survey tools offered by any companies, whether free or subscription, are examples of cloud computing tools.
 - b. Free tools that do not require the transmission of data because they are based on downloading executable files, browser plug-ins, or applets are not considered cloud computing tools, but do fall under regulations for Open-Source software.
 - c. The list of approved products and a link for change requests are located on the *Enterprise Architecture site*.

10.5.2.2.14.1.1
(09-15-2025)
**Survey PCLIA
Requirements**

- (1) The Survey PCLIA process examines and evaluates the risks and ramifications of using, collecting, maintaining and disseminating information in identifiable form about members of the public and agency employees. The IRS has both legal requirements and a responsibility to protect information collected from survey respondents regardless of the data collection method.
- (2) The requesting organization must comply with privacy and security requirements and, as outlined in this IRM, must complete a Survey PCLIA in the *Privacy Impact Assessment Management System (PIAMS)*. For more information, refer to the Reference Guides available in the Help section of PIAMS.
- (3) At least 30 business days prior to the beginning of the survey, submit the following items with the Survey PCLIA (as applicable):
 - a. Final Survey questions
 - b. Moderators guides and scripts
 - c. Any documents related to the information collection, such as letters, emails, and postcards
 - d. Supporting Statement for any survey requiring Office of Management and Budget (OMB) approval
 - e. Copy of applicable vendor contracts.

Note: Privacy analysts may need additional documentation not included in this list to complete their assessment.

- (4) A new PCLIA is required when an unexpired survey has new privacy risks. Changes that require a Survey PCLIA update include:
 - a. New uses of survey results not previously included in the General Business Purpose of the PCLIA.
 - b. Changes/additions to the PII being collected.
 - c. Conversions - when converting paper-based records to electronic systems.
 - d. Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form.
 - e. Disclosure of results to additional sources.
 - f. Changes to survey collection method, instrument, or participant selection process.
 - g. Changes in vendor or vendor responsibilities.
- (5) An Overarching Survey PCLIA may be completed that covers multiple surveys or recurring survey collections, if those collections all serve the same operational purpose and contain similar types and uses of SBU Data (including PII and tax information).

Note: To ensure an Overarching Survey PCLIA is the appropriate action, please contact **Privacy Review*.

- (6) Survey PCLIA's will expire as follows:

- One-time surveys 1 year after the Privacy approval date.
- Recurring surveys 3 years after the Privacy approval date.

10.5.2.2.14.1.2
(01-24-2020)

Surveys Accessed by Links in an Email

- (1) Surveys that include a link (i.e., hyperlink, URL or other web address reference) within an email (or article) must follow specific rules:
 - a. The link must be to a secure website.
 - b. Clearly notify the participant of who will have access to responses (i.e., role of survey administrators).
 - c. If a promise of privacy or confidentiality is provided to the participant, then only the administrator of the survey should have access to the responses. Only aggregated responses should be provided to the business unit, or the requestor.
 - d. Embedded links must not represent themselves as belonging to the IRS, if they direct responses to another location.
 - e. When conducting surveys for IRS employees, emails containing links should be sent by an internal email address. Employees should be provided an internal email address to verify the validity of the survey. Email addresses outside the IRS firewall should not be used.
- (2) These rules also apply to links sent to IRS employees for internal website surveys such as SharePoint, Survey Manager or vendor supported sites.
- (3) Emails which include links must comply with email policy in IRM 10.5.1, Privacy Policy and in IRM 10.8.1, Security Policy as applicable.

- (4) The IRS must have a business need to send a survey by email, instead of by other methods such as telephone or mail. Organizations should use other survey methods (such as telephone or mail) if feasible.

10.5.2.2.14.1.3
(09-15-2025)
Internal Surveys

- (1) A survey PCLIA is required for internal surveys in any of the following conditions:
- The survey uses SBU Data (including PII and tax information) to either select participants, or within the survey questions.
 - Any non-anonymous survey.
 - Any survey sent by email. Refer to Surveys Accessed by Links in an Email, IRM 10.5.2.2.14.1.2, Surveys Accessed by Links in an Email.
 - A third-party website is utilized.
 - The survey is administered or analyzed by a contractor or vendor.
 - Employee satisfaction surveys utilizing Survey Manager or Teams Forms.
 - Recurring events/meetings/town halls which are planned using Survey Manager.
 - SharePoint surveys.
- (2) If surveying Bargaining Unit (BU) IRS employees, or conducting a Focus Group which will include BU employees, NTEU notification may be required. Refer to *Research Survey Group*.
- (3) There are several occasions where an Internal Survey does not require a PCLIA. The chart below illustrates these occasions. For assistance in determining the need for a Survey PCLIA, contact **Privacy Review*.

IF	AND	THEN
Course evaluation: Level 1-4	Using Training Evaluation & Measurement for Performance Optimization (TEMPO), or Integrated Talent Management (ITM)	No Survey PCLIA required.
ITM course evaluation	Using ITM	No Survey PCLIA required.
Polling questions (while in an electronic meeting, with no expectation of anonymity)	Spur-of-the-moment questions to ensure understanding, not pre-planned or recorded	No Survey PCLIA required.
Webinar	Using Integrated Virtual Learning Platform (IVLP) or Zoom and not recorded	No Survey PCLIA required.

Reminder: When creating an internal survey using fill-in response(s) that might allow someone to input SBU Data (including PII and tax information), advise the participant not to include any identifiable information within the response.

10.5.2.2.14.1.4
(09-15-2025)
External Surveys

- (1) A survey PCLIA is required for any external survey when:
- SBU Data (including PII and tax information) is utilized to either select participants, or within the survey questions, moderators guide, or interview questions.
 - Any non-anonymous survey.

- Any mode of survey is sent by email. Refer to Surveys Accessed by Links in an Email, IRM 10.5.2.2.14.1.2, Surveys Accessed by Links in an Email.
- A third-party website is utilized.
- The survey is administered or analyzed by a contractor or vendor.

Note: All survey and focus group information collection requests submitted for review under one of the IRS Office of Management and Budget (OMB) Generic Clearances require the inclusion of a completed Survey PCLIA. See *Paper Reduction Act Clearances*

- (2) The Paperwork Reduction Act (PRA) - Requires OMB to approve each collection of information by a Federal agency that involve requesting identical information from 10 or more members of the public before it can be implemented. For further information regarding OMB, Statistics of Income (SOI), and Taxpayer Forms and Publication (TF&P) requirements, visit the *Research Survey Group site*.

Permissible Use of Results – The 2002 Confidential Information Protection and Statistical Efficiency Act (CIPSEA) governs the use of the results of data collection efforts taken for statistical purposes under pledges of confidentiality or similar promises. CIPSEA makes intentional use of results for other purposes a felony unless certain exceptions for disclosures for qualifying law enforcement purposes apply or additional informed consent is obtained from respondents.

- (3) External survey collections that do not meet PCLIA requirements, but require SOI or OMB approval, must have approval from The Office of Privacy Review that a PCLIA is not required. Contact **Privacy Review* to document this determination.
- (4) Email addresses used for contacting external survey participants must be collected with consent for that purpose. IRS and vendors may not use email addresses for any purpose not included at the time of collection without further consent. The notice requesting consent must:
- Explain the purpose is to request survey responses
 - Describe any penalty or redress for failure to respond (even if the statement is that there is no penalty)
 - Expected time frame to receive the request
 - Include reference to published IRS Privacy Policy, such as found on irs.gov, or provide specific Privacy Policy for the survey
 - An individual confirms consent to the stated purpose(s) when he or she provides an email address in response to a request for survey.

Note: Email addresses provided with consent (see above) do not require encryption. However, IRC 6103 protections apply to mentions of the existence of a return, specific IRS actions or communications and may not be included in unencrypted communications.

- (5) Organizations sending surveys to external participants must:
- a. Post a notice on irs.gov describing the survey in a manner that participants may understand the nature, purpose, and method of administering the survey.
 - b. Provide information for contact representatives responding to questions regarding the survey to verify its legitimacy.

- (6) For surveys that use the IRS Logo or seal, see IRM 1.17.1, Overview of Publishing Authorities, Roles and Responsibilities, and Organizational Structure .

10.5.2.2.14.2

(09-15-2025)

Privacy Compliance in Collaborative Environments (formerly Shared Storage PIAs)

- (1) This section applies to information in IRS collaborative environments, such as Microsoft SharePoint and Teams applications, and other IRS collaborative environments.

- (2) Most IRS collaborative environments no longer require separate PIAs or Privacy and Civil Liberties Impact Assessments (PCLIAAs) beyond those for their underlying systems. SharePoint and Shared Storage PIA is no longer used.

Caution: You are always responsible for the information you share in collaborative environments, the same as you are in a conversation or email.

- (3) The SharePoint PIA requirement is replaced by Information Technology Enterprise Operations (EOps) process for requesting a SharePoint or Teams site. Document through that process how the site complies with privacy requirements, including whether the site maintains SBU data (including PII or tax information) and how you limit access to those with a need to know.

Note: This process will include recertification on a regular basis as determined by the EOps team. For more information about EOps privacy requirements, refer to *SharePoint Online Central*

- (4) The EOps request process will ask if you use the environment for a complex processing system that uses custom code and connects to other systems. If so, it might become a system that requires a separate system PCLIA. Contact **Privacy Review* to ask if you need a system PCLIA. For more information on system PCLIAAs, refer to IRM 10.5.2.2.9, System PCLIAAs.

- (5) Microsoft 365 US Government Community Cloud (M365) includes OneDrive functionality and the ability to host single-use Teams meetings that allow the sharing of documents and data. These instances do not go through the IT EOps SharePoint Site or Teams request process because you are responsible for the data you share in collaborative environments. Before sharing documents and data from OneDrive or during a Teams meeting, make sure you understand how the system works to limit who gets to see it. For more information on Collaborative Technology and Systems, refer to that section of IRM 10.8.1, Security Policy.

10.5.2.2.14.3

(01-24-2020)

Social Media PCLIA

- (1) IRS Third-Party and Social Media sites must have an approved Social Media PCLIA. The adaptive Social Media PCLIA specifically addresses issues relating to third-party and social media use on the internet. These issues include how the IRS will interact with the public and what PII, if any, will be collected. The Social Media PCLIA asks about the type of third-party or social media site being developed, whether the public can respond or interact with comments or questions, how any PII will be used, with whom it will be shared, and how it will be stored. It addresses any risks unique to the social networking environment as well as tracking of visitors to the sites. It also ensures the site contains the required privacy notice and links to IRS.gov and its privacy policy.

- (2) In addition to completing a PCLIA, new Social Media platforms must be approved by the IRS Social Media Branch. Refer to IRM 1.1.11.2.2, Chief, Communications and Liaison.

- (3) For information about other requirements for Social Media sites, see the *Communications & Liaison* site.
- (4) Refer to OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, and OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies, for information about the requirements.

10.5.2.3
(12-17-2015)
Reporting

- (1) The IRS is required to provide specific reports to Treasury.

10.5.2.3.1
(12-09-2016)
FISMA Reporting

- (1) The Federal Information Security Modernization Act (FISMA) requires agencies to conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical controls). As such, agencies are required to certify and accredit each system prior to it being placed in the production environment, as well as every three years or when a significant change has occurred. The Privacy and Civil Liberties Impact Assessment (PCLIA) is one of these artifacts.
- (2) Information Technology Cybersecurity owns the Enterprise FISMA Dashboard, an Enterprise level report that provides system-by-system and Business Unit level views of the state of FISMA compliance for the current FISMA year. System level data includes the current status of FISMA artifacts to include the PCLIA, along with multiple other areas. The primary data source for the Dashboard is the Treasury FISMA Inventory Management System (TFIMS), which is supplemented by additional sources as necessary. The Dashboard is used by senior management to proactively manage the progress of key FISMA metrics.
- (3) The FISMA cycle begins on July 1 of each year, and ends on June 30 of the following year.
- (4) PCA is responsible for uploading current FISMA PCLIA's to TFIMS. PCA contacts system owners and SMEs of the requirement to prepare a new PCLIA 90 days prior to PCLIA expiration.
- (5) Once PCLIA's are approved by PCA, expired PCLIA's are archived and current PCLIA's uploaded. The FISMA goal for PCLIA's is 90% compliance.

10.5.2.3.2
(12-17-2015)
Section 803 Reporting

- (1) Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (*Public Law 110-53*), Treasury requires each bureau, including IRS, to provide a privacy and civil liberties report on recent activities on a periodic basis.
- (2) These reports may be requested bi-annually and generally include the following information:
 - Information on the numbers and types of reviews and activities undertaken (e.g., BPRAs, PCLIA's, etc.).
 - The type of advice provided and the response given to such advice.

- The number and nature of the complaints received for alleged privacy and civil rights violations, along with a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities.

In addition, the IRS includes a short narrative highlighting relevant privacy programs and initiatives.

- (3) The reports from each Treasury bureau are rolled into one Agency report and published on the Treasury public web site:
Public Law 110-53-Implementing Recommendations of the 9/11 Commission Act of 2007.

10.5.2.4
(12-17-2015)
**Business PII Risk
Assessment (BPRA)**

- (1) A Business PII Risk Assessment (BPRA) assesses the privacy risk in an IRS process. Similar to an IT security risk assessment that addresses the impact of risks to the IRS, the BPRA addresses the privacy risk. Note that the BPRA focus is on processes, while the PCLIA focus is on systems, contractor systems, M365, RPA, AI, , surveys, and social media.

10.5.2.4.1
(09-15-2025)
Authority for BPRAs

- (1) *The Privacy Act of 1974 (5 U.S.C. 552a(e)(10))* requires each agency to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.
- (2) OMB M-17-12 sets forth the policy for Federal agencies to prepare for and respond to a breach of personally identifiable information (PII). It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. This Memorandum is intended to promote consistency in the way agencies prepare for and respond to a breach by requiring common standards and processes.
- (3) OMB M-16-24 establishes the Senior Agency Official for Privacy (SAOP) role to ensure the agency complies with applicable privacy requirements in law, regulation, and policy.
- (4) OMB M-06-15 states the agency's Senior Official for Privacy should conduct a review of the policies and processes and take corrective action as appropriate to ensure the agency has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, PII. This review shall address all administrative, technical, and physical means used by the agency to control such information, including but not limited to procedures and restrictions on the use or removal of personally identifiable information beyond agency premises or control.
- (5) OMB M-05-08 – Senior Agency Official for Privacy (SAOP) designation: Agencies have the authority to conduct periodic reviews (e.g., as part of their annual FISMA reviews) to promptly identify deficiencies, weaknesses, or risks. When compliance issues are identified, agencies must take appropriate steps to remedy them.
- (6) OMB Circular A-130 policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT

resources, and supporting infrastructure and services. The appendices to this Circular also include responsibilities for protecting Federal information resources and managing personally identifiable information (PII).

- (7) OMB Circular A-108 – agency responsibilities for implementing the review, reporting, and publication requirements of the Privacy Act of 1974 (“the Privacy Act”), and related OMB policy.
- (8) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 AU-3, AU-6, CA-7 – To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments).
- (9) IRM 10.5.1 - outlines additional authorities and roles and responsibilities for executives, managers, and employees regarding BPRAs.
- (10) IRM 10.5.2.4 outlines the BPRA PII Risk Assessment process, authority, privacy compliance and roles and responsibilities.
- (11) For more information about authorities and resources, refer to the *BPRA site*.

10.5.2.4.2 (12-17-2015) **BPRA Relevance to Privacy Compliance**

- (1) Privacy Compliance and Assurance (PCA) conducts BPRAs on IRS processes to determine how IRS handles and safeguards PII throughout a specific process.
- (2) BPRAs are not normally conducted during the data lifecycle stages of design, but are conducted after deployment or in the operations and maintenance stages of existing processes.
- (3) The criteria are designed to identify diverse processes enabling the BPRA team to obtain a broader view of how IRS protects PII across the IRS landscape.

10.5.2.4.3 (09-15-2025) **BPRA Roles and Responsibilities**

- (1) PGLD Executive responsibilities include:
 - a. Approve annual BPRA Program Plan.
 - b. Issue memorandum of engagement to the Business Process Executives (BPE).
 - c. Inform Business Process Executives (BPE).
 - d. Provide financial and human resources needs.
 - e. Provide Disclosure, Privacy, Records and Identity Assurance resources (co-leads required for PGLD (Consolidated Reviews)).
 - f. Provide Disclosure resources for sampling during the consolidated review and other engagements.
 - g. Review, provide input, and guidance regarding the BPRA program.
 - h. Make decisions on key issues regarding the BPRA program.
- (2) PGLD Associate Director, PCA responsibilities include:
 - a. Provide oversight of the planning, development, and implementation of the BPRA program.
 - b. Review, provide input and guidance regarding the BPRA program.
 - c. Support Chief, Privacy Risk as needed.
 - d. Ensure memorandum of engagement is sent to the BPE.

- (3) PGLD Chief, Privacy Risk responsibilities include:
- a. Manage the planning, development, and implementation of the BPRA program.
 - b. Support the opening and closing of the BPRA workshops.
 - c. Review and provide input and guidance.
 - d. Support BPRA team as needed.
 - e. Approve documents.
 - f. Liaise between the Associate Director and BPRA team.
 - g. Manage/approve system accesses regarding BPRA program.
 - h. Manage/assign BPRA team training regarding BPRA program.
 - i. Manage/assign BPRA Outreach Initiatives.
 - j. Designate BPRA Coordinator(s).
 - k. Designate BPRA Lead(s) and support team for each BPRA case.
 - l. Support BPRA Case Lead as needed.
 - m. Serve as Subject Matter Expert (SME).
- (4) BPRA Coordinator responsibilities include:
- a. Serve as a BPRA Case Lead.
 - b. Create and maintain the BPRA designation schedule on the BPRA Share-Point site.
 - c. Manage the BPRA Suggestion List.
 - d. Conduct initial research and analysis of incoming suggestions.
 - e. Liaise between the Chief, Privacy Risk and team (status updates/ accomplishments etc.).
 - f. Conduct training for new employees/team members.
 - g. Develop and implement outreach initiatives.
 - h. Serve as SME.
- (5) PGLD BPRA Case Lead responsibilities include:
- a. Liaise with the business unit Point of Contact (POC).
 - b. Conduct research and analysis on assigned BPRA.
 - c. Coordinate and facilitate the BPRA Workshop.
 - d. Conduct analysis of BPRA findings.
 - e. Conduct briefings.
 - f. Prepare talking points (bullets) for management, for briefings.
 - g. Manage (receive/create/store) BPRA documentation (SharePoint & e-Trak).
 - h. Create and manage Work Breakdown Structure (WBS) and update the Privacy Risk Chief or BPRA Coordinator, as appropriate.
 - i. Follow-up with the Vulnerability Owner to ensure the mitigation strategy was implemented.
 - j. Serve as SME.
- (6) PGLD BPRA Support Analysts (Internal PGLD) responsibilities include:
- a. Review documentation.
 - b. Participate in workshops.
 - c. Take notes.
 - d. Support the BPRA Case Lead.
 - e. Serve as SME.
- (7) Business Process Stakeholders responsibilities include:

- a. Business Process Executive (BPE):
 - Identifies the POC, which meets the qualifications established by the BPRA team.
 - Participate in BPRA executive briefings.
 - b. Business Process POC:
 - Liaison with the BPRA Lead.
 - Provide background documentation and other research, as requested.
 - Coordinate and participate in all aspects of the workshop.
 - Identify subject matter experts (SMEs).
 - Participate in briefings.
 - Collaborate with Office of Privacy BPRA team to identify mitigation strategies.
 - c. Business Process Subject Matter Experts (SME).
 - Participate and provide expertise.
 - Collaborate with BPRA team to identify mitigation strategies.
- (8) PGLD Enterprise Risk Management (ERM) Liaison responsibilities include:
- a. Receive copies of applicable Memorandums of Engagement.
 - b. Receive invitations to applicable executive briefings.
 - c. Receive copies of applicable quarterly reports.
 - d. Liaison and coordinate with BPE and Vulnerability Owner, when applicable.
- (9) Vulnerability Owner responsibilities include:
- a. Assessing and rationalizing assigned vulnerabilities during the BPRA process. Actions may include accepting, mitigating, transferring, and/or providing justification for vulnerabilities:
 - Accept, mitigate, transfer.
 - Provide justification.
 - b. Complete, *Form 14675*, Decision Making Framework Risk Acceptance Form and Tool (RAFT).
 - c. Respond to vulnerabilities to the BPRA process within established timeframes.
- (10) Authorizing Official (AO) or approving official (who may be different from the Vulnerability Owner) responsibilities include:
- a. Formally assume responsibility for operating the business process at an acceptable level of risk.
 - b. Assume accountability for the privacy risks associated with the business process.
 - c. Sign the RAFT.
- (11) For more information on BPRAs and the related procedures, refer to the *BPRA site*.

10.5.2.4.4
(09-15-2025)
**BPRA Program
Requirements**

- (1) PCA conducts BPRAs on processes, as opposed to systems. PCA assesses privacy risks in systems through PCLIA and SORN review.
- (2) The BPRA team must apply criteria to identify processes for potential BPRAs in the upcoming year.
- (3) The BPRA categories and what they entail are:

- a. Proactive BPRAs: Process analysis to identify potential vulnerabilities prior to an incident (e.g., breach). These BPRAs often address new processes associated with new systems or with emerging issues or trends.
 - b. Reactive BPRAs: Process analysis when known or probable vulnerabilities exist, in order to make recommendations to mitigate the vulnerabilities.
 - c. Revalidation BPRAs: Reviews of completed BPRAs to determine if additional action is required. These BPRAs might be a follow-up or revalidation of a process on which a BPRA was previously conducted.
- (4) In addition to the BPRAs that PCA plans for annually, circumstances may warrant ad hoc BPRAs. These circumstances include: executive requests, high profile breaches, emerging trends, etc.
 - (5) The BPRA team must review the work components, assign Vulnerability Risk levels to the relevant privacy risks, and identify Vulnerability Owners.
 - (6) The vulnerability owner must respond to assigned vulnerabilities within the time frame associated with the vulnerability's assigned risk level.
 - (7) PCA must report to PGLD and BU executives and other impacted management quarterly regarding the important activities.
 - (8) For more information about the response process or reports, send email to **Privacy Review* or refer to the *BPRA site*.

10.5.2.5
(12-17-2015)
Treasury PII Holdings Report

- (1) The Treasury PII Holdings Report is designed to assist Treasury in maintaining a detailed inventory of its PII holdings.

10.5.2.5.1
(09-15-2025)
Authority for Treasury PII Holdings Report

- (1) E-Government Act of 2002.
- (2) NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020.
- (3) M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
- (4) OMB A-130, Management of Federal Information Resources.
- (5) TD 25-07, Privacy and Civil Liberties Impact Assessment.
- (6) Compliance:
 - a. Sec. 522 of Consolidated Appropriations Act of 2005: Each agency shall prepare a written report on its use of information in an identifiable form . . .
 - b. OMB Memo 17-12, **Preparing for and Responding to a Breach of Personally Identifiable Information**, states: **The SAOP shall... develop and implement new policies to protect the agency's PII holdings.**
 - c. Treasury issued memo from Assistant Secretary of Management (ASM) directing bureaus on compliance Partners: Bureaus CIOs and Senior Privacy Officers.

10.5.2.5.2
(12-17-2015)
**Treasury PII Holdings
Report Roles and
Responsibilities**

- (1) Treasury issues a data call every odd year (i.e., 2013, 2015, etc.). For more information, see the following Treasury PII Holdings Report Program Requirements section (IRM 10.5.2.5.3), Treasury PII Holdings Report Program Requirements.
- (2) Privacy analyst coordinates and submits the PII holding report to Treasury.
- (3) PGLD leadership reviews and approves final submission.
- (4) Business Unit Security Program Management Office (SPMO) reviews prior PII holding report and provides updated or new information.
- (5) Treasury's PII Holdings application was developed by the Office of Privacy, Transparency, and Records (OPTR) with help from the Chief Information Officer (CIO). The application acts as a library of all of the Department of Treasury's PII holdings. It describes the different data elements and uses of all the Treasury systems that hold PII. The application itself does not contain the PII maintained in the systems documented.

10.5.2.5.3
(11-19-2018)
**Treasury PII Holdings
Report Program
Requirements**

- (1) Treasury is mandated by Congress to maintain a listing of all systems that contain personally identifiable information (PII). The Treasury data call requests information for some specific areas; however, the information requested may vary from data call to data call:
 - a. Section A: The Privacy Act of 1974 (6 questions)
 - b. Section B: Data Sharing (4 questions)
 - c. Section C: OMB 3/22 (7 questions)
 - d. Section D: Information Security – User Environment (6 questions)
- (2) The IRS must provide responses to Treasury for each applicable system. Most of these answers may be gleaned from the systems PCLIA's with additional support from Disclosure and the Business Unit SPMOs.
- (3) The general program requirements are to:
 - a. Contact the Treasury Holdings Coordinator to gain access to the IRS page of the Treasury Holdings.
 - b. Access the Treasury Holdings website.
 - c. Identify all current PCLIA's (formerly PIA's).
 - d. Remove any PCLIA's for systems or programs that are no longer applicable or active.
 - e. Coordinate with the PCLIA SME or Program Manager to validate or provide responses.
 - f. Provide the Treasury coordinator with the completed PII Holding Report.

This Page Intentionally Left Blank

Exhibit 10.5.2-1 (09-15-2025)

Glossary and Acronyms

Term	Definition or Description
AI	Artificial Intelligence (Interim Guidance RAAS-10-0325-0001, Interim Policy for AI Governance)
AO	Authorizing Official. The AO is a federal employee who is an executive or other senior official with the authority to formally assume responsibility of the operation of an information system and the information contained therein, at an acceptable level of risk. (Refer to IRM 10.8.2.3.1.9, IT Roles and Responsibilities for more information.
ATO	Authorization to Operate. An ATO is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of a Business Product and explicitly accepts the risk to IRS operations. The ATO is signed after a Certification Agent (CA) certifies that the system has met and passed all requirements to become operational. Systems continue to operate under the same ATO following the Information System Continuous Monitoring (ISCM) process.
BEARS	Business Entitlement Access Request System; replaced Online 5081.
civil liberties	The basic rights guaranteed to individuals by law.
CNSI	Classified National Security Information
consent	Consent can be explicit (verbal or by other action) or implied (by continuing or inaction).
controls	From NIST SP 800-53 Rev 5, Section 2.1: Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. Controls are selected and implemented by the organization in order to satisfy the system requirements. Controls can include administrative, technical, and physical aspects.
COR	Contracting Officer Representative
CPO	Chief Privacy Officer
CSP	Cloud Service Provider
DIRA	Digital Identity Risk Assessment
employee information	All employee information covered by the Privacy Act of 1974 (5 USC 552a, as amended). Examples include personnel, payroll, job applications, disciplinary actions, performance appraisals, drug tests, health exams, and evaluation data. Most employee information falls under the SBU data category called PII or Privacy information.
ELC	Enterprise Life Cycle; being replaced by One Solution Delivery Life Cycle (OneSDLC).

Exhibit 10.5.2-1 (Cont. 1) (09-15-2025)

Glossary and Acronyms

Term	Definition or Description
electronic mail message (email)	A record created or received on an electronic mail system including briefing notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message. Email is not encrypted by default and may be exchanged with recipients who are operating in a separate technology environment (domain), outside IRS control.
employees	IRS employees, which includes: <ol style="list-style-type: none"> 1. Employees 2. Seasonal/temporary employees 3. Interns 4. Detailees
EP	Employee Protection, within PGLD's Privacy Policy and Compliance (PPC).
Federal tax information (FTI)	Any return or return information as defined in IRC 6103(b). This includes any information obtained, received, or generated by IRS or any Treasury component with respect to determining liability, potential liability, or amount of liability under the IRC. FTI falls under the SBU data category called tax information or Tax. This IRM uses the term tax information to encompass all types of tax data.
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014.
IRC	Internal Revenue Code
M365	Microsoft 365
MCD	Major Change Determination replaced by PCLTA.
NIST	National Institute of Standards & Technology
OneSDLC	One Solution Delivery Life Cycle; replacing ELC. Note: The term SDLC on it's own usually refers to a system's development. OneSDLC is meant to be more comprehensive solution delivery than traditional system development.
PCA	Privacy Compliance and Assurance
PCLIA	Privacy and Civil Liberties Impact Assessment; replaced PIA for most privacy assessments.
PCLTA	Privacy and Civil Liberties Threshold Assessment; Replacing QQ and MCD.

Exhibit 10.5.2-1 (Cont. 2) (09-15-2025)

Glossary and Acronyms

Term	Definition or Description
personnel	IRS personnel or users, which includes: <ol style="list-style-type: none"> 1. Employees 2. Season/temporary employees 3. Interns 4. Detailees 5. Consultants 6. IRS contractors (including contractors, subcontractors, non-IRS-procured contractors, vendors, and outsourcing providers) Subcategory of data in Privacy category.
PGLD	Privacy, Governmental Liaison and Disclosure.
PIA	Privacy Impact Assessment; replaced by PCLIA at IRS for most privacy assessments.
PIAMS	Privacy Impact Assessment Management System.
PII	<p>Per OMB Circular A-130: Personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.</p> <p>Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency must perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever more information becomes available – in any medium and from any source – that would make it possible to identify an individual.</p> <p>PII as defined here falls under the SBU data category called General Privacy, which is subcategory of the Privacy category. General Privacy refers to personal information, or, in some cases, personally identifiable information as defined in OMB M-17-12, or means of identification as defined in 18 USC 1028(d)(7).</p>
PPC	Privacy Policy and Compliance.
PPKM	Privacy Policy and Knowledge Management, under PGLD's Privacy Policy and Compliance (PPC).
privacy	Privacy at the IRS reflects the combined effort of the IRS, its personnel, and individual taxpayers to protect, control, and exercise rights over the collection, use, retention, dissemination, and disposal of personal information.
Privacy Compliance and Assurance (PCA)	Organization that owns and manages the PCLIA, BPRA, SBU Data Use programs for IRS.

Exhibit 10.5.2-1 (Cont. 3) (09-15-2025)

Glossary and Acronyms

Term	Definition or Description
privacy controls	The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. [NIST SP 800-53]
privacy culture	Where all personnel think about privacy before acting. In such an environment or culture, protecting privacy guides the day-to-day practices and routines of everyone.
privacy and information lifecycle	<p>The series of uses and status of information. It includes the creation, collection, receipt, use, processing, maintenance, access, inspection, display, storage, disclosure, dissemination, or disposal of SBU data (including PII and tax information) regardless of format.</p> <p>Note: Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining. [NIST SP 800-53 PT-2]</p> <p>Information life cycle means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion. [OMB A-130]</p> <p>Also described as designation, safeguarding, marking, sharing (accessing and disseminating), destruction, and decontrol.</p>
privacy principles	The IRS Privacy Principles describe how the IRS protects an individual's right to privacy. Protecting taxpayer privacy and safeguarding confidential tax information is a public trust. To maintain this trust, the IRS and its personnel must follow the privacy principles.
privacy requirements	Mandatory IRS system requirements derived from IRS Privacy Principles and linked to the Privacy Controls, form the basis for privacy protection within the IRS. They mirror the IRS Privacy Principles and provide high-level privacy requirements applicable to the IRS Enterprise Architecture.
QQ	Qualifying Questionnaire (QQ) being replaced by PCLTA.
RAFT	Risk Acceptance Form and Tool.
Record	Anything you create or receive (in hard copy or electronic format) related to your daily work activities. Refer to the Records and Information Management IRM 1.15 series for information.

Exhibit 10.5.2-1 (Cont. 4) (09-15-2025)

Glossary and Acronyms

Term	Definition or Description
requirements	<p>Per NIST SP 800-53, Section 2.1: For federal information security and privacy policies, the term requirement is generally used to refer to information security and privacy obligations imposed on organizations. For example, [OMB A-130] imposes information security and privacy requirements with which federal agencies must comply when managing information resources. The term requirement can also be used in a broader sense to refer to an expression of stakeholder protection needs for a particular system or organization. Stakeholder protection needs and the corresponding security and privacy requirements may be derived from many sources (e.g., laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments).</p>
return	<p>Any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity IRC 6103 (b)(1).</p> <p>Also falls under the SBU data subcategory called Federal Taxpayer Information, which is in the Tax category.</p>
return information	<p>In general, is any information collected or generated by the IRS with regard to any person's liability or possible liability under the IRC. IRC 6103 (b)(2)(A) defines return information as very broad.</p> <p>Also falls under the SBU data subcategory called Federal Taxpayer Information, which is in the Tax category.</p>
RIM	Records and Information Management, under PGLD's Identity and Records Protection (IRP).
RPA	Robotic Process Automation.

Exhibit 10.5.2-1 (Cont. 5) (09-15-2025)

Glossary and Acronyms

Term	Definition or Description
SBU Data	<p>Sensitive but Unclassified Data is any information which, if lost, stolen, misused, or accessed or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs (including IRS operations), or the privacy to which individuals are entitled under the Privacy Act (5 USC 552a). [TD P 15-71]SBU data includes but is not necessarily limited to:</p> <ul style="list-style-type: none"> • federal tax information (FTI), personally identifiable information (PII), protected health information (PHI), certain procurement information, system vulnerabilities, case selection methodologies, system information, enforcement procedures, investigation information. • Live data, which is production data in use. Live means that when changing the data, it changes in production. Authorized personnel may extract the data for testing, development, etc., in which case, it is no longer live. Live data often includes SBU data. <p>For more information about security protections of SBU data, refer to IRM 10.8.1, Security Policy.</p>
SDLC	System development life cycle.
SOR	System of Records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying element assigned to the individual.
SORN	System of Records Notice is Information which is required to be published in the Federal Register by 5 USC 552a(e)(4). Refer to IRM 10.5.6, Privacy Act.
SP	Special Publication (NIST).
Survey	Any data collection method, including but not limited to surveys, focus groups, interviews, pilot studies, and field tests. Refer to IRM 10.5.2.2.14.1, Survey PCLIA for more information.
tax information	<p>Any return or return information as defined in IRC 6103(b). This includes any information obtained, received, or generated by IRS or any Treasury component with respect to determining liability, potential liability, or amount of liability under the IRC.</p> <p>For this IRM, the terms <i>tax data</i> and <i>tax information</i> include <i>return</i> and <i>return information</i> as defined in IRC 6103(b).</p> <p>Tax information falls under the SBU data category called FTI or Tax. This IRM uses the term tax information to encompass all types of tax data. The Tax category includes:</p> <ul style="list-style-type: none"> • Federal Tax Information • Tax Convention • Taxpayer Advocate Information • Written Determinations