MANUAL TRANSMITTAL

10.5.2

Department of the Treasury
Internal Revenue Service

JANUARY 24, 2020

EFFECTIVE DATE

(01-24-2020)

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) Updated display properties of internal links to address security considerations.

(2) Revision of IRM 10.5.2.2.5.1, to clarify processes and procedures already in place in the program.

(3) Removed references to obsolete forms.

(4) Editorial changes to update references to match current legislative and agency guidance.

(5) If the section's modification date changed, but the section is not listed, then that section had minor edits, clarifications, name changes, updated links, or additional examples.

EFFECT ON OTHER DOCUMENTS

IRM 10.5.2, dated November 19, 2018, is superseded. 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.

Peter Wade
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 Responsibilities
10.5.2.1.4 Terms, Acronyms and 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 System PCLIAs
10.5.2.2.4.1 Qualifying Questionnaire (QQ) for PCLIA
10.5.2.2.4.2 PCLIA Updates
10.5.2.2.4.3 Major Change Determination (MCD) for PCLIA
10.5.2.2.4.3.1 System Owner Concurrence and Approval
10.5.2.2.4.4 Milestone Exit Review (MER)
10.5.2.2.4.5 PCLIAs on IRS.gov
10.5.2.2.4.6 Expired and Retired PCLIAs
10.5.2.2.4.6.1 Expired PCLIAs
10.5.2.2.4.6.2 Retired PCLIAs
10.5.2.2.4.7 Reconciliation with As-Built Architecture (ABA)
10.5.2.2.5 Adaptive PCLIAs
10.5.2.2.5.1 Survey PCLIA
10.5.2.2.5.1.1 Survey PCLIA Requirements
10.5.2.2.5.1.2 Surveys Accessed by Links in an Email
10.5.2.2.5.1.3 Internal Surveys
10.5.2.2.5.1.4 External Surveys
10.5.2.2.5.2 Shared Storage PIAs
10.5.2.2.5.2.1 Determining SharePoint PIA Requirement
10.5.2.2.5.3 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

10.5.2.1
(01-24-2020)
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 PII is Personally Identifiable Information], Privacy and Civil Liberties Impact Assessments (PCLIAs), 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 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, *National Security Information*, for additional procedures for protecting classified information.

(4) **Policy Owner.** The Office of Privacy Policy and Knowledge Management (PPKM) 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) **Contact Information.** For questions about PCA or this IRM section, email the PCA office at *Privacy (privacy@irs.gov).

10.5.2.1.1
(01-24-2020)
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.

(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) information of the IRS, 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 (such as Enterprise Life Cycle (ELC), 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 (PCLIAs) [formerly known as Privacy Impact Assessments (PIAs)] for systems, shared storage locations, surveys and social media platforms.
- 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 and Information Protection, Privacy Policy*, has precedence if conflicting information is present, unless the subordinate IRM is more restrictive or otherwise noted.

(6) In an effort to reference the origin of a privacy requirement (National Institute of Standards and Technology (NIST), Treasury, etc.), a requirement may have its origin referenced in parentheses 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 the Policy reference. Refer to the Authority section of IRM 10.5.1.1.6 for applicable authorities.

10.5.2.1.3
(01-24-2020)
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, 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 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
(11-19-2018)
Terms, Acronyms and Related Resources

(1) See IRM 10.5.1 for additional references related to terms, acronyms and related resources not specifically defined in this IRM.

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 PCLIAs 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 PCLIAs 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
(01-24-2020)
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.
- Privacy Act of 1974, as Amended 5 U.S.C § 552a: *https://www.justice.gov/opcl/privacy-act-1974*
- SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
  Appendix J, Privacy Control Catalog.
- Amendments (specifically First and Fourth) to the U.S. Constitution: *https://www.senate.gov/civics/constitution_item/constitution.htm*
- IRM 1.15, *Records and Information Management*, and *Records and Information Management (RIM) site*.

10.5.2.2.2
(01-24-2020)
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) To certify that systems going through an Enterprise Life Cycle (ELC) Milestone or Release have not had any major changes to the PII contained in the system, use Form 14474, *Systems Milestone Exit Release* (also see the section Milestone Exit Review (MER) in this IRM (IRM 10.5.2.2.4.4)).

(4) For more information refer to *the ELC site*.

(5) A Privacy PCLIA is a decision tool used to identify and mitigate privacy risks that notifies the public: *https://home.treasury.gov/footer/privacy-act/privacy-and-civil-liberties-impact-assessments*.

- 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 *PCLIA site*.

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.

10.5.2.2.2.2
(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
(01-24-2020)
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 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, and final signing of PIAs/PCLIAs/Privacy Threshold Assessments (PTAs) 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 and related metrics.
- Provide guidance toward the completion of PCLIAs and assist in strengthening the PCLIA process for IRS stakeholders (workflow, monitoring, reporting, processing, etc.)

(4) The **Privacy Review Manager** must review all PIAs/PCLIAs/PTAs for completeness, including the Privacy analyst findings and case notes prior to forwarding to the Associate Director of Privacy Compliance 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 at an acceptable level of risk. As the approver, the SO attests that the PCLIA correctly documents substantial facts about the system, site, or survey. The SO must ensure the PCLIA process begins in the early stages of the development of a system and complete it as part of the system's required ELC review. Additionally, the SO must implement PCLIA findings or mitigations, as necessary. The System Owner may designate someone to approve the PCLIA.

(6) **System Developer**, **Survey 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 the Privacy Impact Assessment Management System (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), to ensure consistency with the PCLIA
- Consider privacy at every stage of the project 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 the Privacy Impact Assessment Management System (known as 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 *PCLIA website* for more information on PIAMS, SORs and SORNs, the related procedures, and the underlying legal requirements.

10.5.2.2.4
(01-24-2020)
System PCLIAs

(1) Submission of the PCLIA to PCA for approval is required by the end of Milestone 2 of the Enterprise Life Cycle. However, the process should begin as early as Milestone 0. 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.

(2) Submit PCLIAs at least 60 days prior to the date needed for milestones, releases, or to begin production and use of the PII contained in the system.

Note: A timely submission and response to Privacy Review feedback is critical to meet deliverable timeframes.

(3) Projects must follow the *Enterprise Architecture (EA) IRS Privacy Requirements*, which are based on mandated NIST privacy controls.

10.5.2.2.4.1
(01-24-2020)
Qualifying Questionnaire (QQ) for PCLIA

(1) The IRS follows TD 25-07, which allows for a Privacy Threshold Analysis, which is "... an abbreviated assessment used to determine whether a PIA is required under Section 208 of the E-Government Act of 2002."

(2) To determine if a full PCLIA is needed, the IRS utilizes the IRS Qualifying Questionnaire (QQ) as a Privacy Threshold Analysis on PIAMS.

(3) The business owner must complete the QQ to determine if a system requires a PCLIA. For more information, refer to the *PCLIA site*.

(4) New projects or systems may use the QQ when owners are not sure if a system 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.

(5) 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 Analysis can be used to identify and document any additional privacy compliance requirements.

(6) If a determination is made that no PCLIA is needed, PGLD returns a signed QQ to the submitter.

10.5.2.2.4.2
(12-17-2015)
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 PII being collected.
- 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-gov 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-gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or e-gov 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.

10.5.2.2.4.3
(01-24-2020)
Major Change Determination (MCD) for PCLIA

(1) If unsure whether to update a PCLIA, business owners and system developers may submit a Major Change Determination Questionnaire and Documentation of Termination/Retirement of IT Systems via PIAMS.

(2) The purpose of a Major Change Determination (MCD) is to assess, through a series of questions, a system's privacy requirements to determine if a major

change has occurred and a new PCLIA is therefore required. If PCA determines that a major change has not occurred since the last PIA or PCLIA was approved, and that the last PIA or PCLIA approval date is within three years, then PCA will provide a Memorandum that a new PCLIA is not required. This memorandum does not extend the expiration date of the existing PCLIA.

(3) If PCA determines a major change has occurred, or the 3-year time frame is nearing, then a new PCLIA must be conducted. See the section PCLIA Updates in this IRM (IRM 10.5.2.2.4.2).

(4) Additionally, the MCD is used to inform Privacy Review when terminating or retiring any system with an approved PCLIA.

10.5.2.2.4.3.1
(01-24-2020)
System Owner Concurrence and Approval

(1) The System Owner (SO) must concur and approve that all responses and information provided in the Privacy MCD are accurate, valid, and complete before it can be submitted to PCA for review. By providing concurrence and approval, the SO confirms that they understand the questions and content of the Questionnaire and assume full responsibility for the accuracy, validity, and completeness of all responses.

(2) For more information, refer to the *PCLIA site*.

10.5.2.2.4.4
(01-24-2020)
Milestone Exit Review (MER)

(1) PCA issues a Privacy Exit Memo at the end of a Milestone Exit Review (MER), which is an ELC-mandatory project review performed by IRS executives when a project has reached a lifecycle milestone. The purpose of the MER is to assess the viability of continuing the project, identifying any risks and issues, verifying any changes to cost, scope, schedule, and business results. Generally, the MER does not begin until the project's governance organization receives a formal recommendation from the reviewing organization that the Milestone Readiness Review (MRR) was successfully completed. SOs are required to complete an MER for each milestone exit.

(2) The MER form is intended for a project that has already submitted a full PCLIA for review and approval at an earlier milestone and now is traversing a subsequent milestone. However, it can only be used if no changes have occurred to the system affecting privacy or affecting responses to the previously approved PCLIA. If that is the case, this form bypasses the need to resubmit the PCLIA for review.

Note: The MER form is NOT a PCLIA requirement from PCA. It is provided as a convenience for the project and the ELC process in the event evidence is needed of a current/valid PCLIA at the MER.

10.5.2.2.4.5
(01-24-2020)
PCLIAs on IRS.gov

(1) The IRS posts PCLIAs with PII on members of the public on a website available to the public at IRS.gov, in compliance with the E-Government Act of 2002: [Treasury, *http://www.treasury.gov/privacy/PIAs/Pages/default.aspx*] *https://www.irs.gov/privacy-disclosure/privacy-impact-assessments-pia*

(2) The E-Government Act 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 PCLIAs 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 PCA.
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.

Note: Do not post SharePoint PIAs on the IRS.gov website.

(5) The e-Gov Act 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.

10.5.2.2.4.6
(11-19-2018)
Expired and Retired PCLIAs

(1) The lifecycle of an approved PCLIA is three years. A PCLIA expires three years after the approval date, meaning that a new PCLIA is due every three (3) years for existing systems, even if the system has not changed.

(2) When a system retires, its PCLIA is retired.

10.5.2.2.4.6.1
(11-19-2018)
Expired PCLIAs

(1) When a significant change occurs to a system, the system's PCLIA must be updated to reflect how the changes may affect the information.

(2) An MCD form can be completed to determine if a new PCLIA is needed. For more information, see the section Major Change Determination (MCD) for PCLIA in this IRM (IRM 10.5.2.2.4.3).

(3) If an updated or amended PCLIA is approved prior to the 3-year expiration date, the previous PCLIA becomes expired as it has been replaced with a newer version.

(4) While it is the responsibility of the SO and the SME to update a PCLIA before the PCLIA expires, PCA will contact the SO 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 and SME must be mindful of the timeframes 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.

10.5.2.2.4.6.2
(12-17-2015)
Retired PCLIAs

(1) An MCD form is required for systems that have been retired. PCA will work with the As-Built Architecture (ABA) to identify retired systems. For more information, see the section Reconciliation with As-Built Architecture (ABA) in this IRM (IRM 10.5.2.2.4.7). The retired PCLIA will be stored in PIAMS for the appropriate retention period.

10.5.2.2.4.7
(01-24-2020)
Reconciliation with As-Built Architecture (ABA)

(1) IRS Enterprise Architecture Division's *ABA web site* 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 the 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 an MCD form indicating the system is retired.
c. A system currently on the ABA that should have a PCLIA or QQ will be contacted by the PCA to determine if one is needed or which form 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 *ABA FAQ* for information on what forms to use and where to send the information.

10.5.2.2.5
(12-17-2015)
Adaptive PCLIAs

(1) IRS developed unique PCLIAs, 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 PCLIAs may be developed in the future to proactively focus on privacy concerns identi-

fied with other uses of non-conventional data or collaborative environments. Currently, the IRS utilizes three adaptive PCLIAs to cover SharePoint, 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.

10.5.2.2.5.1
(01-24-2020)
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 10.5.2.2.5.1.2, Surveys Accessed 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.

(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: *https://www.gpo.gov/fdsys/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf*

(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 11.3.19 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.

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*.

10.5.2.2.5.1.1
(01-24-2020)
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 updates 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 (privacy@irs.gov)

(6) Survey PCLIAs will expire as follows:

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

10.5.2.2.5.1.2
(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, and in IRM 10.8.1, 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.

10.5.2.2.5.1.3
(01-24-2020)
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 10.5.2.2.5.1.2.
- A third-party website is utilized.
- The survey is administered or analyzed by a contractor or vendor.
- Employee satisfaction surveys utilizing Survey Manager, Centra or SharePoint.
- Recurring events/meetings/town halls which are planned using Survey Manager or Centra.
- SharePoint surveys.

(2) If conducting a Survey (with PII) on a SharePoint site, along with the Survey PCLIA, you may be required to complete a SharePoint PIA. Please contact the *Privacy (privacy@irs.gov) mailbox for guidance.

(3) 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*.

(4) 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 (privacy@irs.gov).

IF	AND	THEN
Course evaluation: Level 1-4	Using TEMPO, or Integrated Talent Management (ITM)	No Survey PCLIA required.
ITM course evaluation	Using ITM	
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	
Webinar	Using Saba and not recorded	

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.

10.5.2.2.5.1.4
(01-24-2020)
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 10.5.2.2.5.1.2.
- 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 *IRS Generic Clearance Administered by SOI*

(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 Privacy that a PCLIA is not required. Contact *Privacy (privacy@irs.gov) 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.

10.5.2.2.5.2
(01-24-2020)
Shared Storage PIAs

(1) This section applies to information in shared storage locations, such as SharePoint and shared drives.

Note: The Shared Storage Privacy Impact Assessment is a PIA instead of a PCLIA because it relies on the Civil Liberties protections of the system through which IRS received the information. For this reason, Civil Liberties are not addressed at a level of specificity to include that designation in this process.

(2) For shared storage locations, use the adaptive SharePoint PIA, which focuses on access to and use of SBU Data (including PII and tax information):

- This template allows the Business Unit to define the information shared on the site and safeguards put in place to secure the data.
- By using this template, only the questions relevant to shared storage will be asked.
- A SharePoint PIA is required any time a shared storage location contains SBU data.
- Overarching SharePoint PIAs covering multiple shared storage uses may be allowed as long as those collections all serve the same operational purpose and contain similar types and uses of SBU data. However, a previously approved SharePoint PIA may not be edited to add new sites.
- Refer to the *PCLIA Knowledge Management site* for SharePoint PIA procedural details.
- Visit *SharePoint Central* for more information on the site collection creation process.

Note: This PIA policy does not apply to limited SBU data that IRS proactively makes available to all employees on resource sites (including, but not limited to, Discovery, Outlook Address Book, or SharePoint site contributors), such as names, profile, and contact information about employees.

(3) Complete a SharePoint PIA in the *Privacy Impact Assessment Management System* (PIAMS).

(4) Shared storage locations must not serve as the sole method for a business process to handle its casework. If the work includes taxpayer information, the business unit must:

- Explain the need to collect and use the data.
- Restrict IRC § 6103 data on SharePoint to cases where no other reasonable avenue exists to share the information with those assigned the case.
- Not use shared storage areas as substitutes for an existing system.

Example: If multiple people in different locations are assigned an account that is on Integrated Data Retrieval System (IDRS), do not post IDRS information on SharePoint. Each person can access IDRS to view the account. However, in some cases taxpayers provide paper documentation needed by multiple employees assigned to the case that cannot be scanned into another system for access. With proper access controls and safeguards, it may be acceptable to scan and post on SharePoint, in these limited situations.

(5) If IRC § 6103, Privacy Act, Title 18, Bank Secrecy Act, or other SBU Data (including PII and tax information) must be placed on a shared storage location, use access controls on the document(s) to limit access properly. Access must be limited to those who have a need to access the documents (need to know) while working the accounts.

(6) Business units must designate a management official at each major program area level responsible for multiple shared storage locations as long as those shared resources all serve the same operational purpose and contain similar types and uses of SBU Data (including PII and tax information).

(7) Shared storage locations must have strong access controls based on least privilege and need-to-know principles as designated in IRM 10.8.1 (related to Collaborative Technology and Systems) and the IRS Privacy Principles.

(8) For SharePoint sites, use of SharePoint built-in permission group options. For all shared storage locations, access controls must:

- Document approval by a manager, including the approval date.
- Document any restrictions, such as “read only” or “between these dates.”
- Review periodically, as defined in the Account Management section of IRM 10.8.1 to keep them current.
  See also the Collaborative Technology and Systems section of IRM 10.8.1.

(9) For more information on SharePoint PIAs, the related procedures, and the underlying legal requirements, refer to the *Privacy and Civil Liberties Impact Assessment site*.

10.5.2.2.5.2.1
(01-24-2020)
Determining SharePoint PIA Requirement

(1) Not all shared storage locations require a PIA. The need for a SharePoint PIA is based on the sensitivity of the data being shared. The Information Owner is responsible for the security of the data at rest or in flight through the shared storage location and makes or approves the final determination.

(2) If the shared location will not include any form of SBU Data (including PII and tax information), then a PIA is not required.

Note: This PIA policy does not apply to limited SBU data that IRS proactively makes available to all employees on resource sites (including, but not limited to, Discovery, Outlook Address Book, or SharePoint site contributors), such as names and contact information about employees.

(3) An Overarching SharePoint PIA is a PIA that covers multiple sites or site collections as long as those collections all serve the same operational purpose and contain similar types and uses of SBU data.

(4) Follow the If-Then chart to determine requirements based on the specific data and sharing needs.

If	**Then**
If no SBU Data (including PII and tax information) is shared	No PIA is required. Use existing safeguards (i.e., SharePoint Permission Groups) to maintain the security of information shared on the site. ***Note:*** This reference does not change the nature of the information made available through SharePoint. Employees must follow existing Business Unit policies concerning the security of information, whether it is stored on SharePoint or any other media.
Information is generally available to all employees with access to the IRS Intranet, (i.e., Employee/ Program contact information (Discovery Directory) General IRS policy, such as IRMs (SERP) All Employee communications (IRWeb) Team procedures/meeting minutes. ***Note:*** SharePoint is not intended to be a duplicate repository for published guidance. To the extent possible, utilize links rather than copies of existing resources.	No PIA is required, as long as site permissions align access to the level of the information (i.e., team level user groups for team level communications). This information is safeguarded sufficiently through a combination of the standard access OL-5081 process granting employee access to the IRS Intranet (Baseline Standard Access or similar equivalent) and the SharePoint Site Administrator's use of standard User Group permissions tied to Active Directory.
Custom application development or hosting that includes SBU Data (including PII and tax information)	Follow Enterprise Life Cycle (ELC) path. An ELC coach will help determine the exact requirements for your tool/application. • For applications with PII, a PIA is required. Include explanation of how to implement and monitor an audit trail for data stored or accessed through SharePoint Custom Applications. • Complete IRS SharePoint Privacy Impact Assessment (PIA) via PIAMS, after determining the exact nature of the ELC path.

If	Then
Any site containing SBU Data (including PII and tax information) that does not meet one of the above descriptions	A PIA is required. • Review previously submitted PIAs by the Business Unit to determine if an existing PCLIA covers the data for the new site. • If not, complete IRS SharePoint Privacy Impact Assessment (PIA) via PIAMS.

10.5.2.2.5.3
(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.

(3) For more information and procedural details about Social Media PCLIAs, refer to the *Social Media PCLIA 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 PCLIAs to TFIMS. PCA contacts system owners and SMEs of the requirement to prepare a new PCLIA 90 days prior to PCLIA expiration.

(5) Once PCLIAs are approved by PCA, expired PCLIAs are archived and current PCLIAs uploaded. The FISMA goal for PCLIAs 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 (*https://www.govinfo.gov/content/pkg/PLAW-110publ53/html/PLAW-110publ53.htm*), 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, PCLIAs, 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:
https://www.gpo.gov/fdsys/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf
https://www.gpo.gov/fdsys/pkg/PLAW-110publ53

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, SharePoint, social media, and surveys.

10.5.2.4.1
(01-24-2020)
Authority for BPRAs

(1) Privacy Act requires each agency to establish appropriate administrative, technical, and physical safeguards to ensure the security and privacy 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. (5 U.S.C. § 552a(e)(9)-(10))

(2) 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.

(3) OMB M-06-15 requires the SAOP to review processes to ensure safeguards of Personally Identifiable Information (PII).

(4) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 AR-4 Privacy Monitoring and Auditing – 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).

(5) 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
(01-24-2020)
BPRA Roles and Responsibilities

(1) PGLD Executive responsibilities include:

a. Conduit to Business Process Executives (BPE).
b. Provide financial and human resources needs.
c. Review, provide input and guidance.
d. Make decisions on key issues.

(2) PGLD Associate Director, PCA responsibilities include:

a. Determine BPRA Lead.
b. Ensure memorandum of engagement is sent to the BPE.
c. Ensure opening and closing at BPRA workshops are conducted.
d. Review, provide input and guidance.
e. Approve documents.

(3) PGLD BPRA Lead responsibilities include:

a. Liaison with the POC.
b. Coordinate the workshop.
c. Conduct briefings.
d. Facilitate BPRA workshop.
e. Maintain Work Breakdown Structure (WBS) and update associate director bi-weekly.
f. Maintain electronic monitoring tool (such as e-trak) for BPRA.

(4) PGLD BPRA Support Analysts (internal PGLD) responsibilities include:

a. Review documentation.
b. Participate in workshop.
c. Support BPRA Lead.

(5) 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.

c. Business Process Subject Matter Experts (SME)
- Participate and provide expertise.

(6) 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.

(7) Vulnerability Owner responsibilities include:

a. Assessment and rationale for assigned vulnerabilities:
- Accept, mitigate, transfer.
- Provide justification.

b. Complete Risk Acceptance Form and Tool (RAFT), Form 14675.
c. Respond to vulnerability within established timeframes.

(8) 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.

(9) For more information on BPRAs and the related procedures, refer to the *BPRA site*.

10.5.2.4.4
(01-24-2020)
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) A BPRA 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 (privacy@irs.gov) 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
(11-19-2018)
Authority for Treasury PII Holdings Report

(1) E-Government Act of 2002.

(2) SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

- Appendix J, Privacy Control Catalog, SE-1 Inventory of Personally Identifiable Information.

(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 Impact Assessment.

(6) Compliance:

a. Sec. 522 of Consolidated Appropriations Act of 2005: "Each agency shall prepare a written report on its use of (PII) . . ."
b. OMB Memo 17-12, **Preparing for and Responding to a Breach of Personally Identifiable Information**, states: **The SAOP shall... [d]evelop 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).

(2) Privacy analyst coordinates and submits the PII holding report to Treasury.

(3) PGLD leadership reviews and approves final submission.

(4) Business Unit 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 PCLIAs 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 PCLIAs (formerly PIAs).
d. Remove any PCLIAs 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.