EFFECTIVE DATE

(11-14-2023)

PURPOSE

(1) This transmits revised IRM 10.5.6, Privacy and Information Protection, Privacy Act.

MATERIAL CHANGES

(1) IRM 10.5.6.1, Program Scope and Objectives, removed duplicate language, clarified plain language and cross-references, clarified audience to match language in IRM 10.5.1.

(2) IRM 10.5.6.1.1, Background, clarified plain language.

(3) IRM 10.5.6.1.2, Authority, changed title, corrected Taxpayer Bill of Rights (TBOR) reference, clarified plain language and cross-references.

(4) IRM 10.5.6.1.3, Roles and Responsibilities, changed title, clarified plain language and cross-references.

(5) IRM 10.5.6.1.4, Program Management and Review, added section to follow IRM 1.11.2, Address Management and Internal Controls.

(6) IRM 10.5.6.1.5, Program Controls, added section to follow IRM 1.11.2, Internal Revenue Manual (IRM) Process.

(7) IRM 10.5.6.1.6, Terms and Acronyms, added section to follow IRM 1.11.2, Internal Revenue Manual (IRM) Process.

(8) IRM 10.5.6.1.7, Related Resources, added section to follow IRM 1.11.2, Internal Revenue Manual (IRM) Process.

(9) IRM 10.5.6.2, Privacy Act General Provisions, changed title, added clarifying examples, clarified plain language and cross references.

(10) IRM 10.5.6.2.1, Requirements of the Privacy Act, added full list of requirements from the law, added clarifying examples, clarified plain language and cross references.

(11) IRM 10.5.6.2.2, Conditions of Disclosure Under the Privacy Act, moved from IRM 10.5.6.8, Personnel Records, added clarifying examples, clarified plain language and cross-references.

(12) IRM 10.5.6.2.3, Privacy Act Consent to Disclosure, new section added to clarify provision of the law under existing policy and add reference to new optional form.

(13) IRM 10.5.6.2.4, Health or Safety Disclosure, new section added to clarify provision of the law under existing policy.

(14) IRM 10.5.6.2.5, Disclosure Under Court Order, moved from IRM 10.5.6.8, Personnel Records, added clarifying examples, clarified plain language and cross-references.

(15) IRM 10.5.6.2.6, Exemption from Disclosure Under the Privacy Act, moved from IRM 10.5.6.8, Personnel Records, added clarifying examples, clarified plain language and cross-references.

(16) IRM 10.5.6.2.7, IRS Privacy Principles, moved down, added clarifying examples, clarified plain language and cross-references.

(17) IRM 10.5.6.2.8, Privacy Act Training, moved down, added clarifying examples of what higher level training might include, clarified plain language and cross-references.

(18) IRM 10.5.6.2.9, OMB Privacy Act Guidance, moved down, added clarifying examples, clarified plain language and cross-references.

(19) IRM 10.5.6.2.9.1, Privacy Act Contract Requirements, moved down, added more language from OMB requirements, added clarifying examples and cautions, clarified plain language and cross-references.

(20) IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs), changed title, added clarifying examples, clarified plain language and cross-references.

(21) IRM 10.5.6.3.1, SORN Responsibilities, changed title, clarified plain language and cross-references.

(22) IRM 10.5.6.3.2, When to Publish a SORN, changed title, clarified plain language and cross-references.

(23) IRM 10.5.6.3.3, Records Not Subject to SORN Requirements, moved up, changed title, clarified plain language and cross-references.

(24) IRM 10.5.6.3.4, Scope of a SOR, changed title, clarified plain language and cross-references.

(25) IRM 10.5.6.3.5, Content of a SORN, changed title, clarified plain language and cross-references.

(26) IRM 10.5.6.3.6, Notice to Establish an Exempt SOR, changed title, added clarifying examples, clarified plain language and cross-references.

(27) IRM 10.5.6.3.7, New Notices of SORs, clarified plain language and cross-references.

(28) IRM 10.5.6.3.11, Deleting a SORN, changed title, clarified plain language and cross-references.

(29) IRM 10.5.6.3.12, SORN Reports, changed title, deleted subsections and consolidated them here, clarified plain language and cross-references.

(30) IRM 10.5.6.3.12.1, Reporting Systems of Records to OMB and Congress, moved, clarified plain language and cross-references.

(31) IRM 10.5.6.4, Privacy Notices, changed title, clarified plain language and cross-references.

(32) IRM 10.5.6.4.1, Privacy Notice Responsibilities, changed title, clarified plain language and cross-references.

(33) IRM 10.5.6.4.2, Notice to Individuals Asked to Supply Information (Privacy Act Notice), added example of a notice to help understand required elements, clarified plain language and cross-references.

(34) IRM 10.5.6.4.5, Privacy Notices Not Related to Tax Administration, changed title, clarified plain language and cross-references.

(35) IRM 10.5.6.5, Privacy Act Recordkeeping Restrictions (Civil Liberties Protections), changed title, clarified plain language and cross-references.

(36) IRM 10.5.6.5.4, Collecting Information Relating to Individuals from Third Party Sources, deleted subsections and consolidated them here, clarified plain language and cross-references.

(37) IRM 10.5.6.6, Privacy Act Requests for Non-Tax Records, changed title, deleted subsections and consolidated them here, clarified plain language and cross-references.

(38) IRM 10.5.6.6.1, How to Make a Privacy Act Request, added new section by consolidating subsections into one overarching section about all requests.

(39) IRM 10.5.6.6.2, Requests for Notification of and Access to Privacy Act Records, changed title, added clarifying examples and details from the law, clarified plain language and cross-references.

(40) IRM 10.5.6.6.2.1, Verification of Identity, moved, clarified plain language and cross-references.

(41) IRM 10.5.6.6.2.2, Duplication Fee, changed title, moved, clarified plain language and cross-references.

(42) IRM 10.5.6.6.3, Requests for Amendment of Non-Tax Privacy Act Records, changed title, moved, added clarifying details from the law, clarified plain language and cross-references. Added content from deleted subsection, Statutory Exemption for Amendment of Tax Records.

(43) IRM 10.5.6.6.3.1, Review of Refusal to Amend a Record, moved, added clarifying details from the law, clarified plain language and cross-references.

(44) IRM 10.5.6.6.3.2, Statement of Disagreement, moved, added clarifying details from the law, clarified plain language and cross-references.

(45) IRM 10.5.6.6.4, Requests for Disclosure of Privacy Act Records, new section added to clarify provision of the law under existing policy and add reference to new optional form.

(46) IRM 10.5.6.6.5, Privacy Act Complaints, new section added to clarify complaints per OMB guidance.

(47) IRM 10.5.6.6.6, Requests for Privacy Act Accounting of Disclosures, new section added to show all Privacy Act requests here. Moved content to here from deleted subsection Requests for Accountings of Disclosure of Privacy Act Records.

(48) IRM 10.5.6.7, Privacy Act Accounting of Disclosures, changed title, deleted subsections and consolidated them here, clarified plain language and cross-references.

(49) IRM 10.5.6.7.1, Form 5482 Procedure, moved, added clarifying examples, clarified plain language and cross-references.

(50) IRM 10.5.6.8, Personnel Records, changed title, added clarifying examples, clarified plain language and cross-references.

(51) IRM 10.5.6.8.1, Personnel Systems of Records, changed title, moved language from deleted subsection formerly 10.5.6.8.2.1 that had duplicate or unnecessary language or content already in another IRM, added clarifying examples, clarified plain language and cross-references.

(52) IRM 10.5.6.8.2, Requests for Personnel Records, moved, changed title, clarified plain language and cross-references.

(53) IRM 10.5.6.8.3, Access to Records of Deceased Employees, moved from IRM 10.5.6.6, clarified plain language and cross-references.

(54) IRM 10.5.6.8.4, Freedom of Information Act (FOIA) and Personnel Records, moved, deleted duplicate or unnecessary language or content already in another IRM, clarified plain language and cross-references.

(55) IRM 10.5.6.8.4.1, Commercial Solicitation, moved, deleted duplicate or unnecessary language or content already in another IRM, clarified plain language and cross-references.

(56) IRM 10.5.6.8.4.2, Public Information Listing, moved, deleted duplicate or unnecessary language or content already in another IRM, clarified plain language and cross-references.

(57) IRM 10.5.6.8.5. Disclosure Under 5 USC 7114, changed title, moved, deleted duplicate or unnecessary language or content already in another IRM, clarified plain language and cross-references.

(58) IRM 10.5.6.8.6, Disclosure Under IRC 6103(l)(4), changed title, moved, deleted duplicate or unnecessary language or content or subsections already in another IRM, clarified plain language and cross-references.

(59) IRM 10.5.6.8.7, Congressional Inquiries on Individuals, moved, combined or deleted duplicate or unnecessary language or content, sections, or subsections already in another IRM, added clarifying examples, clarified plain language and cross-references.

(60) IRM 10.5.6.8.8, Promotion Files, changed title, moved, deleted duplicate or unnecessary language or content or subsections already in another IRM, clarified plain language and cross-references.

(61) IRM 10.5.6.8.8.1, Promotion File Disclosure to Employees, moved, clarified plain language and cross-references.

(62) IRM 10.5.6.8.9, Agency and Negotiated Agreement Grievance Files, changed title, moved, combined or deleted duplicate or unnecessary language or content, sections, or subsections already in another IRM, added clarifying examples, clarified plain language and cross-references.

(63) IRM 10.5.6.8.10, Retirement Records, changed title, moved, combined or deleted duplicate or unnecessary language or content, sections, or subsections already in another IRM, added clarifying examples, clarified plain language and cross-references.

(64) IRM 10.5.6.8.11, Medical Records, moved, consolidated or deleted duplicate or unnecessary language or content, sections, or subsections already in another IRM, added clarifying examples, clarified plain language and cross-references.

(65) IRM 10.5.6.8.12, Official Personnel Folder (OPF), moved, combined or deleted duplicate or unnecessary language or content, sections, or subsections already in another IRM, added clarifying examples, clarified plain language and cross-references.

(66) IRM 10.5.6.8.13, Position Management and Classification and Classification Appeals Files, changed title, moved, combined or deleted duplicate or unnecessary language or content, sections, or subsections already in another IRM, added clarifying examples, clarified plain language and cross-references.

(67) IRM 10.5.6.8.14, Disciplinary Action Files, moved, combined or deleted duplicate or unnecessary language or content, sections, or subsections already in another IRM, added clarifying examples, clarified plain language and cross-references.

(68) IRM 10.5.6.8.15, Adverse Action Files, moved, combined or deleted duplicate or unnecessary language or content, sections, or subsections already in another IRM, added clarifying examples, clarified plain language and cross-references.

(69) IRM 10.5.6.8.16, Equal Employment Opportunity Complaint Files, moved, combined or deleted duplicate or unnecessary language or content, sections, or subsections already in another IRM, added clarifying examples, clarified plain language and cross-references.

(70) IRM 10.5.6.8.17, Supervisory Documentation Files, moved, combined or deleted duplicate or unnecessary language or content, sections, or subsections already in another IRM, added clarifying examples, clarified plain language and cross-references.

(71) IRM 10.5.6.9, Privacy Act Reports, changed title, moved from IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs) to clarify all Privacy Act reports, clarified plain language and cross-references.

(72) IRM 10.5.6.9.1, Privacy Act SORN Reports, changed title, moved from IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs) to clarify kinds of reports, referring to SORN Reports section.

(73) IRM 10.5.6.9.2, Privacy Act Request Report, moved from IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs) to clarify all Privacy Act reports, clarified plain language and cross-references.

(74) IRM 10.5.6.9.3, Annual FISMA Privacy Review and Report, moved from IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs) to clarify all Privacy Act reports, clarified plain language and cross-references.

(75) IRM 10.5.6.9.4, Annual Matching Activity Review and Report, moved from IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs) to clarify all Privacy Act reports, clarified plain language and cross-references. Deleted duplicate content because information is in IRM 11.3.39.

(76) IRM 10.5.6.9.5, Section 803 Reports About Privacy Act Complaints, moved from IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs) to clarify all Privacy Act reports, clarified plain language and cross-references.

(77) Exhibit 10.5.6-1, Agency Review Requirements, changed title, clarified plain language and cross-references.

(78) Exhibit 10.5.6-2, Agency Public Website Posting Requirements, changed title, clarified plain language and cross-references.

(79) Exhibit 10.5.6-3, Reporting Requirements, changed title, clarified plain language and cross-references.

(80) Exhibit 10.5.6-4, Federal Register Publication Requirements, changed title, clarified plain language and cross-references.

(81) Exhibit 10.5.6-5, Terms and Acronyms, changed title from Glossary and Acronyms.

(82) Throughout, if not listed here, clarified plain language and cross-references.

EFFECT ON OTHER DOCUMENTS

This version supersedes IRM 10.5.6, dated January 31, 2020. Also, this IRM supports other IRMs in the IRM 10.5 family.

AUDIENCE

All Operating Divisions and Functions.

Peter Wade
Director, Privacy Policy and Compliance

10.5.6
Privacy Act

Table of Contents

10.5.6.1 Program Scope and Objectives
10.5.6.1.1 Background
10.5.6.1.2 Authority
10.5.6.1.3 Roles and Responsibilities
10.5.6.1.4 Program Management and Review
10.5.6.1.5 Program Controls
10.5.6.1.6 Terms and Acronyms
10.5.6.1.7 Related Resources
10.5.6.2 Privacy Act General Provisions
10.5.6.2.1 Requirements of the Privacy Act
10.5.6.2.2 Conditions of Disclosure Under the Privacy Act
10.5.6.2.3 Privacy Act Consent to Disclosure
10.5.6.2.4 Health or Safety Disclosure
10.5.6.2.5 Disclosure Under Court Order
10.5.6.2.6 Exemption from Access and Amendment Rights Under the Privacy Act
10.5.6.2.7 IRS Privacy Principles
10.5.6.2.8 Privacy Act Training
10.5.6.2.9 OMB Privacy Act Guidance
10.5.6.2.9.1 Privacy Act Contract Requirements
10.5.6.3 Privacy Act System of Records Notices (SORNs)
10.5.6.3.1 SORN Responsibilities
10.5.6.3.2 When to Publish a SORN
10.5.6.3.3 Records Not Subject to SORN Requirements
10.5.6.3.4 Scope of a SOR
10.5.6.3.5 Content of a SORN
10.5.6.3.6 Notice to Establish an Exempt SOR
10.5.6.3.7 New Notices of SORs
10.5.6.3.8 Modified System
10.5.6.3.9 Editorial Changes
10.5.6.3.10 Limited Changes
10.5.6.3.11 Deleting a SORN
10.5.6.3.12 SORN Reports
10.5.6.3.12.1 Reporting Systems of Records to OMB and Congress
10.5.6.4 Privacy Notices
10.5.6.4.1 Privacy Notice Responsibilities

10.5.6.4.2 Notice to Individuals Asked to Supply Information (Privacy Act Notice)
10.5.6.4.3 Notice to Individuals Asked to Disclose Their Social Security Number
10.5.6.4.4 The “Umbrella” Approach for Tax Returns
10.5.6.4.5 Privacy Notices Not Related to Tax Administration
10.5.6.4.6 Online Privacy Policy Notices
10.5.6.4.7 Notifying Individuals that Their Records Were Made Available to a Person Under Compulsory Legal Process
10.5.6.4.7.1 Notification Procedure
10.5.6.5 Privacy Act Recordkeeping Restrictions (Civil Liberties Protections)
10.5.6.5.1 Recordkeeping Restrictions - Responsibilities
10.5.6.5.2 Permissible Records
10.5.6.5.3 Equal Treatment
10.5.6.5.4 Collecting Information Relating to Individuals from Third Party Sources
10.5.6.5.4.1 Inquiries Affected
10.5.6.5.5 Restrictions on the Maintenance of Information About Individuals
10.5.6.5.5.1 Records Affected
10.5.6.5.5.2 Relevant and Necessary Guidelines
10.5.6.5.5.3 Recordkeeping Restrictions Required
10.5.6.5.6 Privacy Act Requirement to Maintain Accurate, Relevant, Timely, and Complete Records
10.5.6.5.6.1 Exempt Systems
10.5.6.5.6.2 Actions Required to Ensure Accurate, Relevant, Timely, and Complete Records
10.5.6.6 Privacy Act Requests for Non-Tax Records
10.5.6.6.1 How to Make a Privacy Act Request
10.5.6.6.2 Requests for Notification of and Access to Privacy Act Records
10.5.6.6.2.1 Verification of Identity
10.5.6.6.2.2 Duplication Fee
10.5.6.6.3 Requests for Amendment of Non-Tax Privacy Act Records
10.5.6.6.3.1 Review of Refusal to Amend a Record
10.5.6.6.3.2 Statement of Disagreement
10.5.6.6.4 Requests for Disclosure of Privacy Act Records
10.5.6.6.5 Privacy Act Complaints
10.5.6.6.6 Requests for Privacy Act Accounting of Disclosures
10.5.6.7 Privacy Act Accounting of Disclosures
10.5.6.7.1 Form 5482, Record of Disclosure (Privacy Act of 1974), Procedure
10.5.6.8 Personnel Records
10.5.6.8.1 Personnel Systems of Records
10.5.6.8.2 Requests for Personnel Records
10.5.6.8.3 Access to Records of Deceased Employees
10.5.6.8.4 Freedom of Information Act (FOIA) and Personnel Records

10.5.6.8.4.1 Commercial Solicitation
10.5.6.8.4.2 Public Information Listing
10.5.6.8.5 Disclosure Under 5 USC 7114
10.5.6.8.6 Disclosure Under IRC 6103(l)(4)
10.5.6.8.7 Congressional Inquiries on Individuals
10.5.6.8.8 Promotion Files
10.5.6.8.8.1 Promotion File Disclosure to Employees
10.5.6.8.9 Agency and Negotiated Agreement Grievance Files
10.5.6.8.10 Retirement Records
10.5.6.8.11 Medical Records
10.5.6.8.12 Official Personnel Folder (OPF)
10.5.6.8.13 Position Management and Classification and Classification Appeals Files
10.5.6.8.14 Disciplinary Action Files
10.5.6.8.15 Adverse Action Files
10.5.6.8.16 Equal Employment Opportunity Complaint Files
10.5.6.8.17 Supervisory Documentation Files
10.5.6.9 Privacy Act Reports
10.5.6.9.1 Privacy Act SORN Reports
10.5.6.9.2 Privacy Act Request Report
10.5.6.9.3 Annual FISMA Privacy Review and Report
10.5.6.9.4 Annual Matching Activity Review and Report
10.5.6.9.5 Section 803 Reports About Privacy Act Complaints

Exhibits

10.5.6-1 Agency Review Requirements
10.5.6-2 Agency Public Website Posting Requirements
10.5.6-3 Reporting Requirements
10.5.6-4 Federal Register Publication Requirements
10.5.6-5 Terms and Acronyms
10.5.6-6 References and Resources

10.5.6.1
(11-14-2023)
Program Scope and Objectives

(1) **Purpose**: This IRM discusses the Privacy Act of 1974, *5 United States Code (USC) 552a*, as amended (Privacy Act), provisions and their application to the IRS.

(2) This IRM does not intend to address all Privacy Act requirements, only those most applicable to IRS privacy policy. For example, the Privacy Act's Computer Matching requirements fall under IRM 11.3.39, Disclosure of Official Information, Computer Matching and Privacy Protection Act.

(3) Most of the IRS records are subject to an extensive body of law, including the confidentiality and disclosure provisions of IRC 6103 that are usually more specific and restrictive than the Privacy Act. The IRC preempts the Privacy Act and governs federal tax returns and return information. In applying the Privacy Act, consider all statutory requirements that apply. The result should be that the safeguards against the invasion of an individual's privacy should be not less than required by the Privacy Act.

(4) Where this IRM refers to agency requirements, this IRM applies the requirement to the IRS as a bureau of the Department of the Treasury throughout.

(5) This Program Scope and Objectives section addresses the following National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53) security and privacy controls. Refer to these sections of IRM 10.5.1:

a. PT-1 Personally Identifiable Information Processing and Transparency -- Policy and Procedures
b. PT-8 Personally Identifiable Information Processing and Transparency – Computer Matching Agreements

(6) **Audience**:
The audience to which the provisions in this manual apply includes:

a. All IRS organizations.
b. All IRS employees with any access to sensitive but unclassified (SBU) data (including personally identifiable and tax information).
c. All individuals and organizations with contractual arrangements with the IRS, including seasonal/temporary employees, interns, detailees, contractors, subcontractors, non-IRS-procured contractors, vendors, and outsourcing providers, with any access to SBU data.

Note: This IRM covers all sensitive data used by and for the IRS no matter what stage of the IT lifecycle (such as production, pre-production, and post-production systems).

For this IRM, the following terms apply:

a. IRS personnel or users includes:
   1. Employees
   2. Seasonal/temporary employees
   3. Detailees
   4. Interns
   5. Consultants
   6. IRS contractors (including contractors, subcontractors, non-IRS-procured contractors, vendors, and outsourcing providers)
b. Authorized or Unauthorized personnel applies to whether they are authorized or unauthorized to take a particular action.

Note: To be authorized, all personnel must complete required training (IRS annual and role-based privacy, information protection, and disclosure training requirements, Unauthorized Access [UNAX] awareness briefings, records management briefings, and all other specialized privacy training) and background investigations *before given access* to SBU data (including PII and tax information). [OMB A-130]

(7) **Policy Owner**: Privacy Policy and Knowledge Management (PPKM) under PGLD's Privacy Policy and Compliance (PPC) owns this policy and holds responsibility for Privacy Act oversight. The Director, PPC, reports to the IRS Chief Privacy Officer (CPO). The CPO is the executive director who oversees Privacy, Governmental Liaison and Disclosure (PGLD) and who holds responsibility for the IRS privacy program.

(8) **Program Owner**: The PPC office (referred to here as Privacy) is the program owner responsible for oversight of the IRS-wide Privacy Act policy, recordkeeping, requests, accounting of disclosures, and personnel records. PGLD's Disclosure office is the program owner for operational intake of Privacy Act requests from the public through *GLDS Support Services (GSS)* via mail or online from the *IRS Privacy Act Request via the FOIA Public Access Portal*. Refer to IRM 11.3.41.3, Disclosure Case Processing and Inventory Management, the General Disclosure Case Processing Procedures section.

(9) **Primary Stakeholders**: All business units are stakeholders for privacy.

10.5.6.1.1
(11-14-2023)
Background

(1) The Senate preface to the legislative history of the Privacy Act stated that, "The Bill of Rights guarantees to each American protections which we equate with specific rights of citizenship in a free society. This legislation is a major first step in a continuing effort to define the 'penumbra' of privacy which emanates from specific guarantees in the Bill of Rights and which helps to give them life and substance as recognized in *Griswold v. Connecticut*" [Legislative History of the Privacy Act of 1974 – S. 3418 (Pub. L. No. 93-579) Source Book on Privacy (1976)].

(2) Congress also found that the:

a. Privacy of an individual is directly affected by the collection, maintenance, use, and disclosure of personal information by federal agencies;
b. Increasing use of computers and sophisticated information technology has greatly magnified the harm to individual privacy that can occur; and
c. Misuse of some information systems may endanger an individual's rights.

(3) Congress decided that it was necessary to regulate the collection, maintenance, use, and disclosure of information by federal agencies to protect the privacy of individuals.

(4) Section 3 of the Privacy Act became effective September 27, 1975, with the intent to provide safeguards for an individual against invasions of personal privacy.

(5) The Privacy Act allows, with limited exceptions under very specific conditions, an individual to examine agency records about that individual and limits the conditions under which such records may otherwise be disclosed.

(6) The Privacy Act defines the term maintain as maintain, collect, use, or disseminate. In this IRM, the terms maintenance, maintain, or keep refer to the privacy lifecycle of information: creation, collection, receipt, use, processing, maintenance, access, inspection, display, storage, disclosure, dissemination, or disposal.

10.5.6.1.2
(11-14-2023)
Authority

(1) *The Privacy Act, 5 USC 552a*.

(2) *The Freedom of Information Act, as amended, 5 USC 552 (FOIA)*.

(3) *Federal Acquisition Regulations Part 24 FAR -- Part 24 Protection of Privacy and Freedom of Information*.

(4) *Internal Revenue Code (IRC)* 6103, Confidentiality and disclosure of returns and return information.

(5) *IRC 7852(e)*, Statutory exemption for tax records from certain provisions of the Privacy Act.

(6) The Taxpayer Bill of Rights (TBOR) lists rights that already existed in the tax code, putting them in simple language and grouping them into 10 fundamental rights. Employees hold responsibility for being familiar with and acting in accord with taxpayer rights. See IRC 7803(a)(3), Execution of Duties in Accord with Taxpayer Rights. For more information about the TBOR, see *https://www.irs.gov/taxpayer-bill-of-rights*. The TBOR includes the rights to privacy and confidentiality.

(7) Department of the Treasury Regulations.

(8) *E-Government Act (2002)*, P.L. 107-347.

(9) Office of Management and Budget (OMB) Circulars *A-130* and *A-108*.

(10) OMB Privacy Act Implementation: Guidelines and Responsibilities (OMB Guidelines), *40 Fed. Reg. 28,948*

(11) *The Civil Service Reform Act of 1978, 5 USC*.

(12) *Department of the Treasury Privacy Act Handbook*.

(13) To reference the origin of a privacy policy cited later in this IRM (National Institute of Standards and Technology (NIST), Treasury, etc.), this IRM may reference a requirement's origin in brackets at the end of the guidance, such as [Strict Confidentiality] (IRS Privacy Principles), [AC-1] (NIST SP 800-53 Security and Privacy Controls), or [TD P 85-01] (Treasury Directive Publications). If no specific origin reference appears, multiple origins may apply. Lack of a reference citation does not mean that no origin applies.

(14) The IRS cites the authorities and purposes (namely tax administration) for processing PII on its System of Records Notices (SORNs) published in the Federal Register and on other required privacy documentation, such as the Privacy and Civil Liberties Impact Assessment (PCLIA), before information collection. All IRS personnel must restrict the processing of PII to only that which is authorized and for the purposes collected. [Privacy Act; NIST SP 800-53]

(15) Primary authorities for processing PII include:

- *5 USC*, Government Organization and Employees, primarily section 301

- *18 USC*, Crimes and Criminal Procedure, primarily section 1030
- *26 USC*, Internal Revenue Code, primarily sections 6001, 6011, 6012, 6109, 7801
- *31 USC*, Money and Finance, primarily section 330

(16) This section addresses the following NIST SP 800-53 security and privacy controls: PT-2 Personally Identifiable Information Processing and Transparency -- Authority to Process Personally Identifiable Information. Refer to that section of IRM 10.5.1.

10.5.6.1.3
(11-14-2023)
Roles and Responsibilities

(1) The IRS follows the Privacy Act by integrating its provisions with the IRS's existing procedural instructions, such as the IRM.

(2) The IRS CPO holds responsibility for the overall IRS privacy program.

(3) The Director, PPC, with support from PGLD headquarters, holds responsibility for IRS privacy policy and overall coordination of the IRS efforts to administer the Privacy Act. Direct questions internally to the **Privacy mailbox*.

(4) PGLD's Disclosure office holds responsibility for operational intake of Privacy Act requests from the public through *GLDS Support Services (GSS)* via mail or online from the *IRS Privacy Act Request via the FOIA Public Access Portal*. Refer to IRM 11.3.41.3, the General Disclosure Case Processing Procedures section. Disclosure also processes requests for notification and access.

(5) All IRS personnel hold responsibility for being familiar with the provisions of the Privacy Act, in line with the level of their assigned duties, and for following the law as it applies to their activities. This includes following the protections outlined in IRM 10.5.1, Privacy Policy.

(6) All IRS personnel must report Privacy Act or PII incidents and data breaches immediately upon discovery to:

a. Their manager and
b. The correct organizations based on what was lost, stolen, destroyed, or disclosed.

Note: For more information on reporting an incident or data breach, refer to IRM 10.5.4, Privacy and Information Protection, Incident Management Program, or the *internal Report Losses, Thefts or Disclosures of Sensitive Data; Report Lost or Stolen IT Assets and BYOD Assets page on the Disclosure and Privacy Knowledge Base Site.*.

(7) All IRS officials hold responsibility for administering the Privacy Act as it applies to their business units and as regulations, published notices, and IRM instructions dictate.

(8) Managers must:

a. Make sure their personnel follow the Privacy Act.
b. Get employee consent before disclosing IRS personnel Privacy Act records beyond IRS need to know, unless otherwise authorized by section (b) of the Privacy Act.

Note: See IRM 10.5.6.2.2, Conditions of Disclosure Under the Privacy Act, and IRM 10.5.6.2.3, Privacy Act Consent to Disclosure.

(9) Most systems of records (SORs), as defined in Exhibit 10.5.6-5, Terms and Acronyms, name two system managers (or responsible officials): the official prescribing practices, and the official maintaining the SOR.

a. The official prescribing practices, generally a headquarters director, makes sure that all procedures for the SOR follow Privacy Act requirements.
b. The official maintaining the SOR (a SOR owner or SOR manager), who is generally an area manager or campus director, makes sure that personnel follow all procedural requirements for the SOR.

(10) The business unit of the SOR owner most familiar with the SOR must write the notices and other required reports and documents to publish a system of records notice (SORN) in the Federal Register. They must write any other required Privacy Act notifications, such as those required by section (e)(3) of the Privacy Act. See IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs).

(11) The individual business units hold responsibility for responding to requests under the Privacy Act. See IRM 10.5.6.6, Privacy Act Requests for Non-Tax Records.

(12) Contractors (and subcontractors) and their personnel must follow Privacy Act provisions. See IRM 10.5.6.2.9.1, Privacy Act Contract Requirements. Also refer to IRM 11.3.24, the Disclosures to Contractors, the Requirements section.

(13) All IRS personnel must properly manage, keep, and archive IRS records (hard copy and electronic) as required by the IRM 1.15 series, Records and Information Management, for records retention and disposition requirements before destroying documents. See the Records Management page on the *PGLD Virtual Library*. Refer to Document 12990, IRS Records Control Schedules (RCS), for the National Archives and Records Administration (NARA)-approved IRS records disposition to prevent unauthorized or unlawful destruction of records. Refer to Document 12829, General Records Schedules (GRS), for the NARA-issued disposal authorizations for temporary administrative records common to all federal agencies.

Caution: In situations when litigation has begun or is reasonably expected, keep in mind that we must maintain records (hard copy as well as electronic) beyond the normal record retention period. For more information, see IRM 25.3.1.7.6, What is a litigation hold?

(14) This Roles and Responsibilities section addresses the following NIST SP 800-53 security and privacy controls. Refer to these sections of IRM 10.5.1:

a. PM-11 Program Management -- Mission and Business Process Definition
b. PM-17 Program Management -- Protecting Controlled Unclassified Information on External Systems
c. PM-19 Program Management -- Privacy Program Leadership Role
d. PM-26 Program Management -- Complaint Management
e. SI-1 System and Information Integrity -- Policy and Procedures
f. SI-12 System and Information Integrity -- Information Management and Retention
g. SI-12(3) System and Information Integrity -- Information Management and Retention - Information Disposal

10.5.6.1.4
(11-14-2023)
Program Management and Review

(1) Business units hold responsibility for managing their program and establishing how they measure effectiveness and objectives within the scope of this IRM.

(2) For PGLD program management and review, the IRS formally documents its privacy program in the *IRS Privacy Program Plan*.

10.5.6.1.5
(11-14-2023)
Program Controls

(1) Business units hold responsibility for establishing and documenting the program controls developed to oversee their program as well as ensuring employee compliance with all applicable elements of this IRM.

(2) The NIST technical security and privacy controls address federal IT systems. For all the controls relevant to privacy, refer to IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls.

10.5.6.1.6
(11-14-2023)
Terms and Acronyms

(1) See Exhibit 10.5.6-5, Terms and Acronyms.

10.5.6.1.7
(11-14-2023)
Related Resources

(1) See Exhibit 10.5.6-6, References and Resources.

10.5.6.2
(11-14-2023)
Privacy Act General Provisions

(1) The Privacy Act came from a time when U.S. culture distrusted government collections and uses of data. It lays the foundation on which the IRS builds the trust necessary to achieve our mission. It underlies all IRS privacy policy.

(2) This section discusses general Privacy Act provisions and their application to the IRS as a bureau of the Department of the Treasury. The purpose of the Privacy Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring federal agencies, except as otherwise provided by law, to:

- Allow individuals to determine what records about them are collected, maintained, used, or disclosed by federal agencies
- Allow individuals to prevent records about them from being used or made available for another purpose without their consent

  Note: See IRM 10.5.6.2.3, Privacy Act Consent to Disclosure.

- Allow individuals to gain access to information about them, have copies made, and amend or correct such records
- Collect, maintain, use, or disclose any record of identifiable personal information in a manner that makes sure that such action is for a necessary and lawful purpose, that the information is current and accurate, for its intended use, and that adequate safeguards are provided to prevent misuse of such information

Except as otherwise provided by law, agencies are subject to civil suit for damages (of no less than $1,000) because of willful or intentional action that violates any individual's rights under the Privacy Act. Criminal penalties (misdemeanor with fines up to $5,000) apply to agency personnel who willfully make prohibited disclosures or who willfully operate a SOR without a SORN in violation of the law.

Note: See IRM 10.5.6.2.1, Requirements of the Privacy Act.

(3) The Privacy Act applies to agency records that identify an individual. Privacy Act records fall under a SOR and require a SORN when retrieved by an **identifying particular** (an identifier). A Privacy Act identifier is personally identifiable information (PII). Refer to IRM 10.5.1, the Personally Identifiable Information (PII) section.

(4) The Privacy Act defines **individual** as a citizen of the United States or an alien lawfully admitted for permanent residence. Corporations, partnerships, estates, organizations, and other entities are not **individuals** for Privacy Act purposes. An individual acting in an entrepreneurial capacity (such as a sole proprietor) is an **individual** for purposes of the Privacy Act. A deceased person is not an individual under the Privacy Act.

(5) Most of the IRS records are subject to an extensive body of law, including the confidentiality and disclosure provisions of IRC 6103, that are usually more specific and restrictive than the Privacy Act. The IRC preempts the Privacy Act and governs federal tax returns and return information.

(6) Agencies may propose rules that exempt certain records from certain Privacy Act provisions. Congress and the OMB must approve such rules, and agencies must publish them in the Federal Register. Treasury specifies whether exemptions apply to a specific IRS SOR in published Federal Register notices. See IRM 10.5.6.3.6, Notice to Establish an Exempt SOR.

(7) For the IRS to maintain records subject to the Privacy Act, it must meet certain publishing and reporting requirements. See IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs).

(8) Having notified the public of the records maintained (by meeting the publishing and reporting requirements), the IRS generally must give individuals asked to supply information a notice with the request for information. See IRM 10.5.6.4, Privacy Notices.

(9) The Privacy Act places restrictions on the information the IRS may collect and use. See IRM 10.5.6.5, Privacy Act Recordkeeping Restrictions (Civil Liberties Protections).

(10) Individuals may have access to certain records about them and may under some circumstances amend such records. See IRM 10.5.6.6, Privacy Act Requests for Non-Tax Records.

Note: IRC 7852(e) says that subsections (d)(2), (d)(3), (d)(4), and (g), of the Privacy Act (such as the amendment provisions) must not be applied, directly or indirectly, to the determination of liability of any person for any tax, penalty, interest, fine, forfeiture, other imposition, or offense to which the provisions of the IRC apply.

(11) The Privacy Act places restrictions on agency disclosure of the records maintained, and it generally requires an accounting of the disclosures made. See IRM 10.5.6.7, Privacy Act Accounting of Disclosures.

(12) The Privacy Act provisions apply to those personnel records with personal information retrievable by a personal identifier (employee PII). We must protect employee privacy, and employees may exercise their rights under the Privacy Act about these records. See IRM 10.5.6.8, Personnel Records.

(13) For the Department of the Treasury Privacy Act policy, refer to *TD P 25-04, Privacy Act Handbook*.

(14) For the Department of Justice Privacy Act Overview, refer to *Overview of the Privacy Act of 1974, 2020 Edition*.

(15) The following NIST SP 800-53 security and privacy controls address these Privacy Act provisions. Refer to these sections of IRM 10.5.1:

a. PM-22 Program Management -- Personally Identifiable Information Quality Management
b. PT-2 Personally Identifiable Information Processing and Transparency -- Authority to Process Personally Identifiable Information
c. PT-3 Personally Identifiable Information Processing and Transparency – Personally Identifiable Information Processing Purposes
d. SC-1 System and Communications Protection -- Policy and Procedures
e. SC-7(24) Boundary Protection -- Personally Identifiable Information

10.5.6.2.1
(11-14-2023)
Requirements of the Privacy Act

(1) IRS personnel must always follow the legal requirements of the Privacy Act and must make every effort consistent with law, regulations, and good administrative practice, to promote the spirit of the Privacy Act by performing their duties in a manner that recognizes and enhances individual rights of privacy.

(2) Restrict disclosure of Privacy Act information to Department of Treasury personnel who have a need to know the information in the performance of their official duties.

(3) With respect to Privacy Act records, the IRS must:

a. Maintain only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required by statute or Executive Order [Privacy Act section (e)(1)].
b. Collect information, to the greatest extent practical, from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs [Privacy Act section (e)(2)].
c. Inform each individual whom it asks to supply information, of the agency's authority for requesting the information; whether providing the information is voluntary or mandatory; the principal purpose(s) for which the information will be used; other routine uses of the information; and the effect(s), if any, on the individual of not providing all or part of the information requested. This statement may be on the form used to collect the information, or on a separate form or sheet that the individual may keep [Privacy Act section (e)(3)].
d. Meet SOR publication requirements [Privacy Act sections (e)(4) and (e)(11)]. See IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs).
e. Maintain all records used in making any determination about any individual with such accuracy, relevance, timeliness, and completeness to ensure fair treatment [Privacy Act section (e)(5)]. See IRM 10.5.6.5.6, Privacy Act Requirement to Maintain Accurate, Relevant, Timely, and Complete Records.
f. Verify the record's accuracy, completeness, timeliness, and relevancy before disclosing any record about an individual to any person other than an agency, unless made under section (b)(2) (the FOIA) [Privacy Act

section (e)(6)]. See IRM 10.5.6.5.6, Privacy Act Requirement to Maintain Accurate, Relevant, Timely, and Complete Records.

g. Maintain no records on how any individual exercises their First Amendment rights, unless certain exceptions apply [Privacy Act section (e)(7)]. See IRM 10.5.6.5, Privacy Act Recordkeeping Restrictions (Civil Liberties Protections).

h. Make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record [Privacy Act section (e)(8)]. See IRM 10.5.6.4, Privacy Notices.

i. Establish rules of conduct for persons involved in the design, development, operation, or maintenance of any SOR, or in maintaining any record, and instruct each such person on rules, requirements, and penalties for noncompliance (civil damages starting at $1,000 and criminal penalties with misdemeanor fines up to $5,000) [Privacy Act section (e)(9)]. The *IRS Rules of Behavior* serve as the rules of conduct required by the Privacy Act section (e)(9). Refer to IRM 10.5.1 the Responsibilities, Employees/Personnel section. For instruction on these rules, see IRM 10. 5.6.2.8, Privacy Act Training.

j. 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 that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained [Privacy Act section (e)(10)]. Refer to the protections outlined in IRM 10.5.1, Privacy Policy.

k. Follow computer matching agreement requirements [Privacy Act section (e)(12)]. Refer to IRM 11.3.39, Disclosure of Official Information, Computer Matching and Privacy Protection Act.

Note: The IRS Privacy Principles reflect these Privacy Act requirements. See IRM 10.5.6.2.7, IRS Privacy Principles.

(4) Through these requirements, the Privacy Act mandates the prompt disposition, proper destruction, safe storage, physical protection, and proper handling of records.

(5) The IRS meets these requirements by adhering to its policies found throughout the IRS-wide IRMs and this IRM specifically. Also, IRM 10.5.1 lays the foundation for protecting Privacy Act information.

(6) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1.8:

a. AT-1, Awareness and Training and subsections
b. MP-1 Media Protection and subsections
c. MP-6 Media Protection -- Media Sanitization and subsections
d. PE-1 Physical and Environmental Protection and subsections
e. PE-8(3) Physical and Environmental Protection -- Visitor Access Records – Limit Personally Identifiable Information Elements
f. PL-4 Planning -- Rules of Behavior
g. PM-22 Program Management -- Personally Identifiable Information Quality Management
h. SI-1 System and Information Integrity and subsections
i. SI-12 System and Information Integrity -- Information Management and Retention and subsections

10.5.6.2.2
(11-14-2023)
Conditions of Disclosure Under the Privacy Act

(1) The Privacy Act section (b) limits access to a record without the prior written consent of the individual to whom the record relates, unless it meets one of these conditions. See IRM 10.5.6.2.3, Privacy Act Consent to Disclosure.

(2) The Privacy Act section (b) lists Conditions of Disclosure where the IRS may disclose a record without prior written consent of the individual. Refer to *31 CFR 1.24*.

Caution: For tax records protected by IRC 6103, the requirements of that section take precedence over the Privacy Act. Unless IRC 6103 expressly provides for disclosure, then disclosure is not authorized, regardless of whether the Privacy Act permits disclosure.

(3) The following table outlines the most common conditions of disclosure under the Privacy Act that IRS personnel encounter:

Condition of Disclosure	Description
(b)(1) [need to know]	Internally to officers and employees of the agency who have a need for the information in the performance of their official duties. See IRM 10.5.6.5.5.2, Relevant and Necessary Guidelines. Also refer to IRM 10.5.1, the Need to Know section.
(b)(2) [FOIA]	For the release of a record as required by the FOIA. The existence of an actual FOIA request is a prerequisite for application of this provision.
(b)(3) [routine use]	The routine use provision allows for the disclosure of a record for a use that is compatible with the purpose for which the record was collected. A routine use generally involves disclosure to another agency, state, or local government or other organization. The agency must specify this in the SORN. Under this condition, disclosures are also made to unions recognized as exclusive bargaining representatives under 5 USC section 7114. Under this condition, disclosures are also made to unions recognized as exclusive bargaining representatives under 5 USC section 7114. The agency must specify each routine use in the SORN. ***Note:*** A routine use disclosure may not end the need to protect the information being disclosed. For example, routine use disclosures to contractors still require privacy protections in the contract.
(b)(5) [statistical]	This provision is for statistical research or reporting purposes. Provide the record only in a format that is not individually identifiable.

Condition of Disclosure	Description
(b)(7) [law enforcement]	For civil and criminal law enforcement activities. This condition of disclosure applies when federal, state, and local governments request information for investigations of welfare fraud, tax matters, unemployment compensation, and other civil or criminal law enforcement activities. The requirements for granting a (b)(7) request are specific as outlined in *31 CFR 1.24*. Responsible personnel must determine whether the request meets the four requirements of the (b)(7) condition as follows: a. The request must be in writing. b. The request must specify the particular part of the record(s) desired on a given individual(s). c. The request must say that the information is for a civil or criminal law enforcement activity that is authorized by law, including investigations related to such activities, and must specify the law enforcement purpose for which the record is sought. d. The request must be by the head of a federal, state, or local agency or an appropriate official of the agency. The head of a city or county department, District Attorney, Chief of Police, Chairperson of a county board or committee, tax commissioner, or deputy tax commissioner among others, would be considered an appropriate official. If the individual executing the request is below this level, contact may be with the requester to get either a new request from the proper level or a statement that authorizes the requester to execute such requests. When the request involves payroll data, send the request to the proper Payroll Center with responsibility for the employee's function. Responsible personnel may consult the Public Information Listing (PIL) to find the proper Payroll Center to contact. . ***Note:*** In the case of a subpoena or summons for payroll records, see IRM 11.3.13, the Public Information Listing section, for the PIL website access procedures, refer to the charts attached as exhibits to Delegation Order 11-2 in IRM 1.2.2.12.2, Delegation Order 11-2 (Rev. 4), Authority to Permit Disclosure of Tax Information and to Permit Testimony or the Production of Documents, and IRM 11.3.35, Requests and Demands for Testimony and Production of Documents. The IRS allows the IRS business unit processing the (b)(7) request also to authorize the (b)(7) release. Specify the level of authority official in business unit procedures.
(b)(8) [health or safety]	When there is a compelling circumstance affecting the health or safety of the individual. This provision is strictly interpreted. Limit release to emergency situations. ***Note:*** Notify the individual whose information you disclosed using their last known address and account for the disclosure. ***Reminder:*** For privacy considerations about pandemics and employee illness, refer to Infectious Disease in the Workplace, Document 13001.

Condition of Disclosure	Description
(b)(10) [GAO]	To the Comptroller General or the Government Accountability Office (GAO) in the performance of its duties. This condition includes any GAO audit or request for a Comptroller General decision where information from a record, subject to the Privacy Act, is disclosed. See IRM 11.3.23, Disclosure to the Government Accountability Office (GAO).
(b)(11) [court order]	Disclosure under an order of a court of competent jurisdiction. See IRM 10.5.6.2.5, Disclosure Under Court Order, for specific instructions on disclosures under this condition.

10.5.6.2.3
(11-14-2023)
Privacy Act Consent to Disclosure

(1) Whenever IRS policy refers to consent or permission to disclose non-tax information (usually personnel records) under section (b) of the Privacy Act, follow the requirements in this section.

Note: Even if we receive consent to disclose information, we must still protect it during the disclosure process.

(2) Privacy Act consent for disclosure must be in writing, but the format depends on the circumstances, context, and data collected. Email may be enough in most cases.

(3) To document consent, IRS personnel may use internal Form 15293, IRS Privacy Act Disclosure Consent, to note the information to be disclosed and identify the recipient, unless directed otherwise. Use of this form is optional.

Caution: This form is for use only by current IRS personnel and must not be used to authorize disclosure of tax information protected by IRC 6103. This form does not replace the process for disclosure to an exclusive representative under 5 USC 7114(b)(4).

a. Either the individual whose information is disclosed or the business unit or individual disclosing the information may prepare the form.
b. The individual whose information is disclosed must sign the form.
c. Keep this form for as long as the disclosed record requires, or five years after the disclosure, whichever is later. See Document 12829, General Records Schedules, General Records Schedule 4.2, Item 050.

(4) This process includes, but is not limited to, consent for disclosure of photos, recordings, contact information, or other non-tax information covered by the Privacy Act. Refer to IRM 10.5.1, the Recordings in the Workplace section.

Note: For photo or video in IRS publications, use Form 14483-A, Model/Photo Release, instead of Form 15293, IRS Privacy Act Disclosure Consent.

(5) Documenting written consent meets the requirement for accounting of disclosures under the Privacy Act. Keep the written consent the same as you would a Privacy Act accounting. See IRM 10.5.6.7, Privacy Act Accounting of Disclosures.

(6) For more information, including examples, of when to document consent, refer to the *Privacy Act Consent* site on the PGLD Disclosure and Privacy Knowledge Base on IRS Source.

10.5.6.2.4
(11-14-2023)
Health or Safety Disclosure

(1) The Privacy Act section (b)(8) allows us to disclose employee information in a compelling circumstance affecting the health or safety of the individual. This provision is strictly interpreted. Limit release to emergency situations. We must also tell the employee in writing of such disclosure and account for the disclosure following IRM 10.5.6.7.1, Form 5482 Procedure.

(2) In a situation affecting the health or safety of an individual, if you feel the circumstance is a compelling emergency, you may disclose an employee's identity to appropriate local officials or management to make sure the employee gets the immediate necessary attention.

(3) The emergency and compelling nature of this exception includes valid life and death situations such as an airplane crash, pandemic, or a threat to themselves or others.

(4) If you make such a disclosure, immediately tell your manager. Refer to IRM 11.3.34.3, Expedited Procedures in Emergency Situations.

(5) Upon disclosure under the health and safety exception, the officer who made or authorized the disclosure must notify the subject in writing within 5 days of the disclosure. Meet this requirement by making reasonable effort to locate the individual and mail the notification to the last known employment or home address. Notification must include the following information:

a. Nature of the information disclosed
b. Person or agency to whom it was disclosed
c. Date of disclosure
d. Compelling circumstances justifying the disclosure

10.5.6.2.5
(11-14-2023)
Disclosure Under Court Order

(1) Disclose documents controlled by OPM, such as the right (long-term) side of the Official Personnel Folder (OPF), according to the instructions in *5 CFR 297.402* and *5 CFR 297.403*.

(2) Process a court order, demand (subpoena or summons), or an order from an administrative body (such as a state unemployment compensation board), which requires testimony or the production of documents by an IRS official, per procedures for later approval by the proper official authorized by Delegation Order 11-2 in IRM 1.2.2.12.2. Process a court order, demand (subpoena or summons), or an order from an administrative body (such as a state unemployment compensation board), which requires testimony or the production of documents by an IRS official, per procedures for later approval by the proper official authorized by Delegation Order 11-2 in IRM 1.2.2.12.2.

(3) According to the *Civil Service Reform Act of 1978*, Title VII, Section 7132, Part (a)(2):

"No subpoena shall be issued under this section which requires the disclosure of intra-management guidance, advice, counsel, or training within an agency or between an agency and the Office of Personnel Management."

(4) Refer to IRM 11.3.35, Requests and Demands for Testimony and Production of Documents, and IRM 11.3.13, Freedom of Information Act, for further guidance on processing requests for personnel and payroll records.

(5) After an employee has left the IRS for any reason, the Human Capital Office (HCO) sends the OPF within 90 days to OPM for maintenance and retention. After the OPF transfer, OPM is the proper agency to respond to subpoenas or other requests for personnel records. OPM requires a subpoena or court order signed by a judge. Direct subpoenas to:

The Office of General Counsel
Office of Personnel Management
1900 E Street, NW
Washington, DC 20415

10.5.6.2.6
(11-14-2023)
Exemption from Access and Amendment Rights Under the Privacy Act

(1) The Privacy Act explicitly exempts, or allows agencies to exempt, certain categories of records, or information within a record, from certain Privacy Act provisions, including access and amendment requirements. Exempt SORs include those that contain records compiled in anticipation of a civil action or proceeding [(d)(5)], information compiled to investigate or enforce criminal laws [(j)(2)], or investigatory material compiled for non-criminal law enforcement purposes [(k)(2)]. Refer to *31 CFR 1.36* and a system's SORN to determine if the records it contains are exempt from access and amendment requirements pursuant to Privacy Act sections (d)(5), (j), or (k).

10.5.6.2.7
(11-14-2023)
IRS Privacy Principles

(1) The IRS Privacy Principles reflect the Privacy Act requirements outlined in IRM 10.5.6.2.1, Requirements of the Privacy Act.

(2) Privacy protection within the IRS includes adherence by all IRS personnel to the IRS Privacy Principles listed in that section of IRM 10.5.1, Privacy Policy.

(3) Policy Statement 1-1, Mission of the Service, also embodies these concepts. See that section in IRM 1.2.1, Servicewide Policies and Authorities, Servicewide Policy Statements.

(4) The following NIST SP 800-53 security and privacy control addresses these Privacy Act requirements: PM-11 Program Management -- Mission and Business Process Definition. Refer to that section of IRM 10.5.1.

10.5.6.2.8
(11-14-2023)
Privacy Act Training

(1) The OMB in Circular A-130 says:

"Agencies shall develop, maintain, and implement mandatory agency-wide privacy awareness and training programs for all employees and contractors."

Note: See Section (e)(9) of the Privacy Act.

(2) Annual Mandatory Privacy Information Protection and Disclosure Briefing offers basic Privacy Act training for all IRS personnel who handle PII. Refer to Integrated Talent Management (ITM) course number 49403-22 and the Mandatory Briefings section of IRM 10.5.1.

(3) The IRS requires the highest level of involvement in training for Privacy Act purposes for managers, government information specialists, and policy analysts serving in PGLD. This includes training beyond the mandatory briefings, such as *ITM* course number 78413, The Privacy Act, and the *Privacy Advocate Certification Program* courses, numbers 61972, 81027, and 81084.

(4) Business units with key personnel identified as requiring a high degree of training in Privacy Act matters may direct them to *ITM* course number 78413, The Privacy Act. For tailored Privacy Act presentations, send a request to the **Privacy mailbox*

(5) Business units revising existing training programs or starting new training programs must include Privacy Act segments designed by their specific needs to follow IRM 10.5.6.5.6, Privacy Act Requirement to Maintain Accurate, Relevant, Timely and Complete Records. Contact Privacy at the internal **Privacy mailbox* for help with such specialized course segments.

(6) For personnel requiring less involvement, conduct a periodic refresher or update by including Privacy Act topics in regular group meetings and by discussing the impact of the Privacy Act on specific jobs. Contact Privacy at the **Privacy mailbox* for information or help.

(7) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. AT-1 Awareness and Training -- Policy and Procedures
b. AT-2 Awareness and Training -- Literacy Training and Awareness
c. AT-3 Awareness and Training -- Role-Based Training
d. AT-3(5) Awareness and Training -- Role-Based Training - Processing Personally Identifiable Information
e. AT-4 Awareness and Training -- Training Records
f. PM-13 Program Management -- Security and Privacy Workforce
g. PM-17 Program Management -- Protecting Controlled Unclassified Information on External Systems

10.5.6.2.9
(11-14-2023)
OMB Privacy Act Guidance

(1) The OMB revised Circulars A-130 and A-108 in 2016 to emphasize Privacy Act compliance. The documents assert its importance by placing responsibility with a Senior Agency Official for Privacy (SAOP).

Note: Treasury houses the SAOP for the IRS, while the IRS CPO is the executive director responsible for the IRS privacy program.

(2) To make sure that agencies effectively carry out the privacy-related functions described in law and OMB policies, Presidential Executive Order 13719 requires the head of each agency to designate or re-designate an SAOP who holds agency-wide responsibility and accountability for the agency's privacy program. The SAOP must be a senior official at the Deputy Assistant Secretary or equivalent level who serves in a central leadership position at the agency, has visibility into relevant agency operations, and is positioned highly enough within the agency to regularly engage with other agency leadership, including the head of the agency. See OMB Memo M-16-24.

(3) The revised OMB A-108 replaced the prior OMB requirement for agencies to conduct annual Privacy Act reviews with the requirement to set up and

maintain a privacy continuous monitoring (PCM) program. The IRS PCM strategy is outlined in the Pub 5499, *IRS Privacy Program Plan*.

Note: See Exhibit 10.5.6-1, Agency Review Requirements, and Exhibit 10.5.6-2, Agency Public Website Posting Requirements.

(4) The OMB requires the IRS to design its privacy control selection process to include privacy controls that ensure compliance with applicable requirements in the Privacy Act and related OMB guidance. Controls selected for an information system that has information in a SOR must address the following elements:

a. Minimization: Make sure SORs include only information about an individual that is relevant and necessary to carry out a purpose required by statute or executive order.
b. SORNs: Make sure that all SORNs stay correct, up-to-date, and properly scoped; that all SORNs are published in the Federal Register; that all SORNs include the information required by OMB Circular A-108; and that all significant changes to SORNs have been reported to OMB and Congress (see section 7 of OMB Circular A-108 for information about reporting a modified SOR).
c. Routine Uses: Make sure that all routine uses stay proper and that the recipient's use of the records continues to be compatible with the purpose for which the information was collected (see section 6(k) of OMB Circular A-108 for information about routine uses).
d. Privacy Act Exemptions: Make sure that each exemption claimed for a SOR stays proper and necessary (see section 11 of Circular A-108 for information about Privacy Act exemptions).
e. Contracts: Ensure compliance with the contract requirements (as discussed in IRM 10.5.6.2.9.1, Privacy Act Contract Requirements), and that the applicable requirements in the Privacy Act and OMB policies are enforceable on the contractor and its personnel (see section 6(j) of Circular A-108 for information about SORs operated by contractors).
f. Privacy Training: Make sure training practices are sufficient and that personnel understand the requirements of the Privacy Act, OMB guidance, the IRS's implementing regulations and policies, and any job-specific requirements.

Note: For more information on privacy controls, see IRM 10.5.1, Privacy Policy.

(5) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. CA-1 Assessment Authorization and Monitoring -- Policy and Procedures
b. CA-2 Assessment Authorization and Monitoring -- Control Assessments
c. CA-6 Assessment Authorization and Monitoring – Authorization
d. CA-7 Assessment Authorization and Monitoring -- Continuous Monitoring
e. CA-7(4) Assessment Authorization and Monitoring -- Continuous Monitoring – Risk Monitoring
f. PM-9 Program Management -- Risk Management Strategy
g. PM-18 Program Management -- Privacy Program Plan
h. PM-19 Program Management -- Privacy Program Leadership Role
i. PM-31 Program Management -- Continuous Monitoring Strategy
j. SI-1 System and Information Integrity -- Policy and Procedures

k. SI-12 System and Information Integrity -- Information Management and Retention
l. SI-12(1) System and Information Integrity -- Information Management and Retention - Limit Personally Identifiable Information Elements
m. SI-12(2) System and Information Integrity -- Information Management and Retention - Minimize Personally Identifiable Information in Testing, Training, and Research

10.5.6.2.9.1
(11-14-2023)
Privacy Act Contract Requirements

(1) OMB A-108 requires privacy review of procurement solicitations involving Privacy Act records, approval of contracts, and Privacy Act clauses in contracts. It prescribes:

a. Agencies must design their procurement practices to make sure that the SAOP reviews and approves all contracts that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of information that identifies and is about individuals before awarding the contract to help evaluate whether a SOR will be established and, if so, to include proper clauses in the contract.

Note: See section 6(j) of OMB Circular A-108 for information about SORs operated by contractors.

b. The SAOP must have access to a complete and correct list of all the agency's contracts involving information that identifies and is about individuals.
c. The SAOP must establish a process to make sure that the language of each contract is sufficient and that the applicable requirements in the Privacy Act and OMB policies are enforceable on the contractor and its personnel consistent with the agency's authority.
d. Agencies must conduct these reviews with a frequency sufficient to ensure compliance and manage risks. See Exhibit 10.5.6-1, Agency Review Requirements.

(2) OMB A-130 also requires we make sure all IRS acquisitions and contract vehicles have proper language holding contractors and other service providers accountable for following federal and IRS privacy policies and procedures.

Caution: A contractor and its personnel are not considered employees of the Department of the Treasury for purposes of the Privacy Act. Privacy Act protected records cannot be disclosed to contractors under Privacy Act Section (b)(1). Make disclosures of such records to contractors only if one of the statutory disclosure provisions applies. The most commonly applicable disclosure provisions are 1) a published "routine use" in the proper SORN, and 2) written consent to the disclosure from the individual whose records are at issue.

Caution: Section (m)(1) subjects a contractor and its personnel to the Privacy Act's criminal penalties under section (i) if the contract is to operate a SOR for the agency. The IRS routinely includes disclosure prohibitions and other protection clauses in contracts that authorize contractor access to Privacy Act protected records.

Caution: For tax returns and return information, IRC 6103 preempts the Privacy Act. It controls disclosure of federal tax returns and return information. The IRS must not disclose returns and return information to a contractor

unless they meet the requirements of IRC 6103 (regardless of whether the Privacy Act authorizes disclosure). See IRM 11.3.24, Disclosures to Contractors, the Requirements section, for tax return and return information contract requirements.

(3) Federal Acquisition Regulations (FAR) Subpart 24.3 requires a Privacy Act Training Contract Clause for contractors whose personnel will have authorized access to Privacy Act information. Personnel must complete training that addresses protection of privacy per the Privacy Act and the handling and safeguarding of PII. These personnel must complete initial privacy training and annual privacy training thereafter. See *FAR Subpart 24.3* and *FAR 52.224-3* for more information.

Note: The IRS meets this requirement by including IRS-specific clauses in such contracts. To find the proper contract clauses, refer to the *Contractor Compliance* page on the *PGLD Disclosure and Privacy Knowledge Base* on IRS Source or the *IRS Acquisition Policy site*.

(4) A contractor who has personnel involved in these activities must also maintain records indicating that its personnel have completed the training and give these records to the contracting officer upon request. The prime contractor also must flow-down these requirements to all applicable subcontracts.

(5) Contractor privacy training must cover the following:

a. The provisions of the Privacy Act, including penalties for violations of the Privacy Act (civil damages starting at $1,000 and criminal penalties with misdemeanor fines up to $5,000).
b. The appropriate handling and safeguarding of PII.
c. The authorized and official use of a SOR or any other PII.
d. Restrictions on using unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise access, or store PII.
e. The prohibition against the unauthorized use of a SOR or unauthorized disclosure, access, handling, or use of PII or SORs.
f. Procedures to follow in case of a potential or confirmed breach of a SOR or unauthorized disclosure, access, handling, or use of PII.

(6) For more discussion on the impact of the Privacy Act on contracts, refer to the Personnel Engaged in Procurement Activities and Contractors sections of IRM 10.5.1.

(7) For more information on contract requirements, refer to Pub 4812, Contractor Security and Privacy Controls.

(8) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. PM-17 Program Management -- Protecting Controlled Unclassified Information on External Systems
b. SA-11 System and Services Acquisition -- Developer Testing and Evaluation
c. SI-12(3) System and Information Integrity -- Information Management and Retention - Information Disposal

10.5.6.3
(11-14-2023)
Privacy Act System of Records Notices (SORNs)

(1) To follow the Privacy Act, the IRS (via the Department of the Treasury) must publish in the Federal Register a notice of the existence and character of each SOR that it maintains. There must be a published System of Records Notice (SORN) covering any record retrieved by an identifier for an individual who is a citizen of the United States or an alien lawfully admitted for permanent residence.

Note: While a Privacy Act identifier is PII, not all PII falls under a Privacy Act SOR. For more information on PII, see that section of IRM 10.5.1.

(2) The SORN describes how the IRS uses Privacy Act records. A SORN serves as a promise to the public that the IRS will not do anything with their individual information other than what's described in the published notice. The Privacy Act prohibits any other use.

(3) When considering any new collection of Privacy Act information (in IT systems, paper, or any other format) retrieved by an identifier, you must verify a SORN covers those records. If not, the business unit of the record owner must publish or amend a SORN.

(4) Record owners most familiar with the SOR must write and maintain the SORN. For more information on preparing a SORN, refer to the internal *SOR Writing Guide* and *PGLD PPC SORN Development, Review, and Updates Standard Operating Procedure (SOP)*.

(5) The SORN must correctly describe the IRS use of the records to give sufficient transparency to the public.

(6) Any officer or employee of an agency who willfully maintains a SOR without meeting the notice requirements of the Privacy Act may be found guilty of a misdemeanor and fined not more than $5,000.

(7) See Exhibit 10.5.6-4, Federal Register Publication Requirements.

(8) For more information on SORNs, refer to the *internal SORNs page* and the *Self-Help Online Tutorial (SHOTs) video on System of Records Notices (SORN) Privacy Act Requirements*.

(9) Email the **Privacy mailbox* for help with SORN or reporting requirements.

(10) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. AC-3(14) Access Control -- Access Enforcement - Individual Access
b. PL-1 Planning -- Policy and Procedures
c. PL-2 Planning -- System Security and Privacy Plan
d. PL-8 Planning -- Security and Privacy Architecture
e. PM-27 Program Management -- Privacy Reporting
f. PT-2 Personally Identifiable Information Processing and Transparency -- Authority to Process Personally Identifiable Information
g. PT-3 Personally Identifiable Information Processing and Transparency – Personally Identifiable Information Processing Purposes
h. PT-6 Personally Identifiable Information Processing and Transparency -- System of Records Notice

10.5.6.3.1
(11-14-2023)
SORN Responsibilities

(1) While record owners most familiar with the SOR must write and maintain the SORN, they must work with PGLD and other stakeholders to complete the process. For more details on SORN responsibilities, refer to the internal *PGLD PPC SORN Development, Review, and Updates Standard Operating Procedure (SOP)*.

(2) With support of PGLD headquarters, the Director, PPC, holds responsibility for:

- Serving as Privacy and Civil Liberties Officer for the IRS and maintaining contact with the Departmental Privacy Act Coordinator for the Department of the Treasury to make sure that materials sent meet all departmental requirements.
- Reviewing all submissions for conformance with this section and ensuring that all submissions follow Privacy Act requirements.
- Ensuring that all submissions adequately inform the public and protect the rights of individual members of the public, per the Privacy Act.
- Ensuring the adequacy of all notices, with special regard to routine uses of records maintained in a system, and general Privacy Act matters.
- Accumulating notices involving deletions, editorial changes, or limited changes for inclusion in the Republication of Notices of Systems of Records, or for submission at such other intervals as appropriate.
- Reviewing the materials required for the Republication of Notices of Systems of Records, the Federal Inventory of Personal Data Systems, and the Annual Report.
- Preparing the reports described in this IRM.

(3) Systems owners hold responsibility for:

- Preparing Reports of New Systems of Records in final form.
- Preparing input materials required by this section and sending to PGLD via email to the **Privacy mailbox*.

Note: The business unit office that is most familiar with the SOR must write the notice. For more information on preparing a SORN, refer to the internal *SOR Writing Guide*.

Note: Changes that require a new Privacy Act SOR or altered system notice usually requires a new or amended Privacy and Civil Liberties Impact Assessment (PCLIA) under the E-Government Act, section 208, P.L. 107-347. See IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment, for information about PCLIAs.

(4) Records owners hold responsibility for:

a. Resolving inquiries and recommendations from officials and personnel within their business units.
b. Determining the adequacy of existing notices and updating them when necessary.
c. Assuring that existing practices conform to Privacy Act requirements.
d. Preparing new notices as necessary.

(5) Records owners must have a continuing program for carrying out these goals and monitoring business unit activities. All contacts with business units to ensure compliance and adequate input to the development of new or revised notices will be along business unit lines with their IRM provisions authorizing the maintenance of the SOR.

(6) Direct inquiries and recommendations from personnel about the adequacy of existing notices to the official identified in the published notice as maintaining the system. Process inquiries and recommendations about SORs that do not appear to be covered by an existing notice through normal supervisory channels within the business unit whose records are involved. The responsibility for the SOR lies with the official who instructed the records be accumulated.

(7) Officials identified in notices as maintaining a SOR must send any matters they are unable to resolve and their own inquiries and recommendations to the official who issued the governing instructions authorizing or prescribing the existence or maintenance of the SORs.

(8) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. PM-5(1) Program Management -- System Inventory - Inventory of Personally Identifiable Information
b. PM-20 Program Management -- Dissemination of Privacy Program Information
c. RA-8 Risk Assessment -- Privacy Impact Assessments

10.5.6.3.2
(11-14-2023)
When to Publish a SORN

(1) When considering any new collection of Privacy Act information (in IT systems, paper, or any other format) retrieved by an identifier, you must verify a SORN covers those records. If not, the business unit of the record owner must publish or amend a SORN.

(2) Responsible IRS personnel must publish a SORN in the Federal Register when setting up a new SOR, before collecting the information for inclusion in a SOR.

(3) Responsible IRS personnel also must publish notice in the Federal Register when making significant, substantive changes to an existing SOR. Examples of significant changes include:

a. A large increase in the number or categories of individuals about whom the system keeps records. For example, a system covering physicians that is being expanded to include other health care providers (such as nurses or technicians) would require a revised SORN. Increases attributable to normal growth in a single category of individuals generally would not require a revised SORN.
b. A change that expands the categories of records maintained in the system. For example, a benefit system that originally included only earned income information that is being expanded to include unearned income information would require a revised SORN.
c. A change in the scope of the system. For example, the combining of two or more existing SORs.
d. A change in the purpose(s) for which the information in the SOR is maintained.
e. A change in the IRS's authority to maintain the SOR or maintain, collect, use, or disclose the records in the system.
f. A change in the way the system works or its location(s) that changes the process by which individuals can exercise their rights under the statute (such as to seek access to or amendment of a record).

10.5.6.3.3
(11-14-2023)
Records Not Subject to SORN Requirements

(1) Records not retrieved by an identifier do not need a SORN.

(2) Files consisting of records input to another SOR are not subject to the SORN requirement. If the input records have personal information that is retrieved but not input to the reported system, they will form a separate SOR. Files that have a continued existence of their own may be subject to the SORN requirement even though they may be part of another SOR.

(3) Files with records produced from another SOR are not subject to the SORN requirement if all personal information in the output is derived from the system being reported. If more information is later added to the output, if the records are later used for an unrelated or different purpose, or if they have a retention period longer than the system being reported, they will form a separate SOR.

(4) Files set up to help process a reported SOR – but with no meaningful existence of their own and with no personal information other than that being corrected, correlated, or otherwise moved to or from one or more reported systems of records – are not subject to the SORN requirement.

(5) Copies of records, whether in the same or altered format, are not subject to the SORN requirement, if all personal information in the copy merely shows information in the system being reported. If more information is later given a different characterization, the records will form a separate SOR.

(6) A file that temporarily has records for processing purposes that will be returned to a reported system upon completion is not subject to the SORN requirement if information in the temporary file can be located by reference to the reported file.

(7) Information derived from a reported file for temporary use (such as work planning, scheduling field visits, controlling individual inventories, reviewing caseloads, or other activities related to the management of the IRS) and not reflective of any individual information not recorded in a reported file is not subject to the SORN requirement.

(8) Telephone directories and similar lists that do not assign any characterization to any person listed are not considered subject to the SORN requirement.

(9) Directories, industrial guides, reference works, and other source materials prepared commercially are not SORs subject to the SORN requirement.

(10) Separate SORNs are not required for the closed parts of files that have been reported as a SOR.

(11) The officials who had responsibility for records when they were open hold responsibility for preparing SORNs for closed or retired files that have no active counterpart. This must not be considered an instruction to search for and account for any document files from which records are no longer retrieved for IRS purposes.

10.5.6.3.4
(11-14-2023)
Scope of a SOR

(1) Before developing a SORN, responsible IRS personnel must consider the proper scope of the SOR. Agencies have discretion in determining what forms a SOR for purposes of preparing a notice. However, responsible IRS personnel must consider the following general factors when determining whether to treat a group of records as a single system or multiple systems for the purposes of the Privacy Act:

a. The IRS's ability to follow the requirements of the Privacy Act and help individuals exercise their rights.
b. The informative value of the notice. Responsible IRS personnel must consider whether a single SORN or multiple SORNs would give the most informative notice to the public about the existence and character of the system(s).
c. The IRS's ability to respond to individual access requests. Responsible IRS personnel must consider whether a single SORN or multiple SORNs would give the best notice to individuals about how and where they may request access to their records maintained in the system(s) and would allow the IRS to respond to such requests most effectively.
d. The purpose(s) and use(s) of the records. If different groups of records are used for distinct purposes, it may be proper to treat those different groups of records as separate systems. Although different groups of records may serve a general common purpose, responsible IRS personnel must also consider whether different routine uses or security requirements apply to the different groups, or whether different personnel of the IRS regularly access the groups.
e. The cost and convenience to the IRS, but only to the extent consistent with the above considerations about compliance and individual rights. Agencies have considerable latitude in defining the scope or grouping of records that form a SOR. The IRS may choose to consider the entire group of records for a certain program as a single system, or the IRS may consider it proper to segment a group of records (such as by business unit or geographic unit) and treat each segment as a SOR to give better notice to the public. When an agency chooses to segment a group of records into separate SORs, the agency must make sure that the SORN for each segment clearly describes any linkages that exist between the different SORs based on the retrieval of the records.

Example: If records described in different SORNs are in fact linked together through a central indexing or retrieval ability – such that an employee or contractor retrieving records described in one SORN would necessarily also retrieve and gain access to records described in another SORN – the agency must explain this linkage in the "Policies and Practices for Retrieval of Records" section of both SORNs.

(2) A government-wide SOR is where one agency has regulatory authority over records in the custody of multiple agencies, and the agency with regulatory authority publishes a SORN that applies to all the records regardless of their custodial location. The application of a government-wide SORN makes sure that privacy practices with respect to the records are carried out uniformly across the federal government according to the rules of the responsible agency. For a government-wide SOR, all agencies – not just the agency with government-wide responsibilities – must follow the terms of the SORN and the applicable requirements in the Privacy Act, including the access and amendment provisions that apply to records under an agency's control.

(3) As a general matter, a government-wide SOR is proper when one agency has government-wide responsibilities that involve administrative or personnel records maintained by other agencies. For example, the Office of Personnel Management (OPM) has published some government-wide SORNs relating to the operation of the federal government's personnel programs.

(4) A Treasury-wide SOR covers many Treasury bureaus, including the IRS.

(5) For information on SORNs, refer to the internal *Privacy Act Systems of Records* site. Also refer to the *System of Records Notices* page on IRS.gov for more information on SORNs, including links to government-wide, Treasury-wide, and IRS SORNs.

10.5.6.3.5
(11-14-2023)
Content of a SORN

(1) Each SORN must include the following information:

Note: For more information on preparing a SORN, refer to the *SOR Writing Guide*

a. **Identification:** Always shown as Treasury/IRS.
b. **System Number:** Each SOR is assigned a system number. The coded title for each IRS system is Treasury/IRS followed by a five-digit number with a period after the second digit. Each of the first two digits shows the business unit and the division that controls the records. When preparing a new SORN, request a system number from Privacy via the **Privacy mailbox*. For a list of IRS systems of records and numbers, go to the *internal Privacy SORN List* or the public *Treasury SORNs page*.
c. **System Name:** The system name should be a title that generally shows the categories of individuals in the system or the goal of maintaining the system, informative to the user of the notice. However, you do not have to rename systems with established names for this purpose. A dash and the identifier Treasury/IRS should follow the system name.
d. **Security Classification:** Only show a security classification if the entire system is classified Top Secret, Secret, or Confidential.
e. **System Location:** Because the IRS is a decentralized organization, a system usually has segments at various locations. For SORN purposes, consider these separate segments part of an overall system, although they function separately. Show the system location as headquarters, IRS offices, posts of duty (PODs), campuses, or a computing center (as may apply) followed by the legend "(See IRS Appendix A)." Appendix A cites the addresses for headquarters, area offices, territory offices, campuses, and computing centers. Individual notices citing one or more of the above should not repeat the address. Any notice that cites a location other than the above (except POD) should specify the city and street address or building name where the SOR is located.
f. **Categories of Individuals Covered by the System:** The purpose of the requirement to state categories of individuals covered by the system is to help individuals find if information on them might be in the system. Clearly list the description of the categories in non-technical terms understandable to individuals unfamiliar with data collection techniques. The more specific and limited the categories described are, the fewer inquiries are likely to result from persons wondering if they are in the system. However, any future broadening of the categories of individuals on whom records are maintained would require publication of a revised public notice before putting the change into effect.
g. **Categories of Records in the System:** The categories should describe the information included using non-technical terms. The addition of any new categories of records not within the categories described in a current notice would require the issuance of a revised public notice before putting the change into effect.

h. **Authority for maintenance of the system:** Each SOR should identify the specific statutory authority or Executive Order that authorizes maintaining the system.

i. **Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses:** Each SOR should identify:

a. The disclosures made from the system under Privacy Act Section (b)(3).
b. The category of recipients and the purpose of disclosure. Include disclosures required by other statutes and proper citations.

Note: Release of information to a member of Congress in response to written authorization of the constituent is a section(b) release and not a routine use release.

Note: Any new routine use or change in an existing routine use that has the effect of expanding the availability of the information in the system requires publication of a revised public notice before putting the change into effect.

j. **Policies and Practices for the storing, retrieving, accessing, retaining, and disposing of records in the system:** Each SOR requires four separate entries as follows.

1. **Storage:** Each SOR should list the medium in which records are maintained (such as paper records, machine readable, digital media, or magnetic media).
2. **Retrievability:** Each SOR should list the individual identifiers used to retrieve records from the system (such as by name or SSN).
3. **Safeguards:** Each SOR should explain measures taken to prevent unauthorized disclosure of records (such as physical security or personnel screening). When appropriate, use a statement that Access Controls and Protections are not less than required by chapter 10.2, Physical Security Program, chapter 10.5, Privacy and Information Protection, and chapter 10.8, Information Technology (IT) Security.
4. **Retention and Disposal:** Each SOR should explain how long the records are maintained, if and when they are removed to a Federal Records Center or to the Archives, and if and when they are destroyed. Base the entry on or refer to the right records disposition schedule. Refer to the IRM 1.15 series, Records and Information Management.

k. **System manager(s) and addresses:** Each SOR generally requires two entries:

a. The title of the official who prescribed the system.
b. The official or, in a dispersed system, the officials, who have physical control of the system as “Officials maintaining the system.”

Note: The official who prescribed the system is generally a management official or executive. The official maintaining the system is generally an executive. Give locations for maintaining officials only.

l. **Notification procedure:** Each SOR should include:

a. The title and office of the official to whom an inquiry should be sent.
b. A citation to applicable regulations.

c. A statement of exemption.

m. **Record Access Procedure:** Each SOR should name the business unit that owns the records and how to request a copy of the records in the system.

n. **Contesting Record Procedure:** Each SOR should have appropriate elements like those in (k). In proper circumstances, this entry may reference IRC 7852(e), which prevents use of the Privacy Act to contest tax liability.

o. **Record Source Categories:** Each SOR should note in general terms the sources of the information in the system. This section does not intend to make available information about sources in investigations whose records would be exempt from the inspection provision.

p. **Exemptions Claimed for the System:** Systems exempted from certain provisions of the Privacy Act is an entry intended to allow ready identification of those items that have been published in the Federal Register as part of a Notice of Exempt Systems. "None" is listed, or no entry is made for systems that are not exempt.

(2) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. AC-1 Access Control -- Policy and Procedures

b. AC-3(14) Access Control -- Access Enforcement - Individual Access

10.5.6.3.6
(11-14-2023)
Notice to Establish an Exempt SOR

(1) The requirement to publish a public notice applies to all SORs maintained by the IRS. The Privacy Act also allows agencies to exempt SORs from certain provisions of the Act by publishing a rule stating which provisions and why the exemptions are proper. Find such notices published in the Federal Register at *31 CFR 1.36*.

(2) The contents of some SORs may be exempted from the requirement that individuals be allowed access to those records and other requirements. When proposing a new SORN for a system intended to be exempt from some provision of the Privacy Act, send a revision to the Notice of Exempt Systems for the Commissioner's approval.

(3) Systems of records are never automatically exempt from provisions in the Privacy Act.

(4) Exemptions require an agency head to decide that a system is allowed to be exempt and publish it as a rule subject to the Administrative Procedure Act, that a system falls within one of the categories of systems allowed to be exempted. That notice must include the specific provisions from which the system is proposed to be exempted and why the agency considers the exemption necessary.

Note: Even when a published rule exempts a SOR from certain provisions, the IRS Privacy Principles still apply. For example, a civil law enforcement SOR might be exempt from the relevant and necessary requirements of section (e)(1) of the Privacy Act. Especially in the early stages of investigation, it may be impossible to immediately decide whether information collected is relevant and necessary, and information that first appears irrelevant and unnecessary often may, upon further evaluation or with information developed later, prove relevant to a law enforcement program. However, the IRS

Privacy Principles require us to minimize data where possible, limiting access only to those with a need to know. Refer to the IRS Privacy Principles section of IRM 10.5.1. See IRM 10.5.6.5.5.2, Relevant and Necessary Guidelines.

(5) Consider exemptions on a case-by-case basis. The broad exemption for criminal law enforcement comes under (j)(2) and does not apply to most typical IRS uses.

(6) Whenever this exemption is exercised, the SORN may be less detailed or simplified, especially about the statement of sources of information since in many investigative situations a suitable source of information can only be decided by the needs of the investigation.

(7) Any meaningful change in the categories of individuals covered by the system or the categories of records in the system may make it advisable to republish the Notices of Exempt Systems.

(8) A report identifying the changes or additions, and describing the nature, effect, and reasons for the proposed exemption in greater detail than in the notice itself, must go with Notices of Exempt Systems.

10.5.6.3.7
(11-14-2023)
New Notices of SORs

(1) The IRS cannot collect information about individuals for inclusion in a SOR until it issues a public notice of that system.

(2) A Report on New Systems must go with or precede the notice. For more information on such reports, see IRM 10.5.6.3.12, SORN Reports.

(3) The transmittal memorandum must note any necessary expeditious handling and must include a proposed schedule for carrying out the various related actions such as:

- Submission of the Report of New System.
- Publication of proposed and final Notice of Exempt System.
- Consideration of any public comments.
- Issuance of data collection forms or instructions.
- Issuance of Request for Proposal or Invitation to Bid for computer or communications systems.
- Installation of equipment.
- Implementation of the system.

(4) In some cases, a statute may require that a SOR begin functioning before the agency can follow all Privacy Act requirements; identify any such conflict in the transmittal memorandum.

10.5.6.3.8
(11-14-2023)
Modified System

(1) Treat a change to a SORN, which modifies an existing SOR falling within the criteria established for submission of a Report on New Systems, as a notice for a new system. The transmittal memorandum must include the information specified for a new system.

(2) For more information on such reports, see IRM 10.5.6.3.12, SORN Reports.

10.5.6.3.9
(11-14-2023)
Editorial Changes

(1) Editorial changes consist of:

- Corrections of typographical errors.
- Correction of spelling or grammatical errors.
- Minor rewording intended to clarify an existing notice.
- Similar revisions.

(2) An editorial change reissues the SORN but does not show any change in the SOR. It requires very little justification in the associated memorandum.

10.5.6.3.10
(11-14-2023)
Limited Changes

(1) Limited changes show modifications of an existing SOR that do not fall within the criteria established for submission of a Report on New Systems.

(2) They do not involve any interruption or delay in operating the system pending the submission of such Report and the publication of a new SORN.

(3) Fully justify a proposed limited change in the associated memorandum to show the business unit of the record owner considered and found inapplicable the requirements for report and notice before operating the system.

(4) For more information on such reports, see IRM 10.5.6.3.12, SORN Reports.

10.5.6.3.11
(11-14-2023)
Deleting a SORN

(1) Delete a SORN because the system:

- Was submitted in error,
- Was not subject to the Privacy Act, or
- System has been discontinued.

(2) If the business unit of the record owner must inform the public as soon as possible of a SORN deletion, prepare a suitable announcement for insertion in the Federal Register. When time is not a factor, delete the SORN by memorandum as part of the regular republishing of notices.

(3) Once a SORN is deleted, any later proposal to reinstate the same SOR must follow reporting requirements as a new system.

10.5.6.3.12
(11-14-2023)
SORN Reports

(1) Submit a report on a new SOR when proposing setting up a new SOR subject to the Privacy Act or when any change to an existing system meets any of the following criteria:

a. Increases the number, or changes the categories, of individuals about whom records are maintained. Report changes involving the number of individuals about whom records are kept only when that change significantly alters the character and purpose of the SOR.

Note: Do not report normal increases in historical files or other increases in the number of records in a file attributed to normal growth patterns.

b. Expands the categories of information maintained.

c. Alters the way the records are organized, indexed, or retrieved to change the nature or scope of those records.

Example: The combining of two or more existing systems or splitting an existing system into two or more different systems such as might occur in a centralization or decentralization of organizational responsibilities would require a report. However, the

combining or splitting of notices without any significant change to the system does not require a report.

Example: A reorganization that placed a system or a part of a system formerly maintained by SB/SE under the control of Criminal Investigation would require a report. A mere physical relocation, such as would occur if a state formerly served by one campus were served by another campus, or if the number or location of area offices were to change, would not require a new report.

d. Alters the purposes for which the information is used. A proposal to set up or change the "routine uses" of the system will not require the submission of a Report on New System if such use is compatible with the purposes for which the system is maintained (if it does not, in effect, create a new purpose). Any new or changed "routine use" would be subject to the requirements to give 30 days prior notice of such change in the Federal Register, if the effect were to expand the release of information, but not if the effect were to restrict the release.

e. Changes the equipment configuration (such as hardware or software) to create the potential for either greater or easier access.

Example: The addition of a telecommunications ability that would increase the risk of unauthorized access would require a report. However, the routine acquisition of equipment meant to effectively use processing capabilities, which is consistent with the development of the existing system, and which does not involve a risk of improper access or create an ability for a massive release of information outside the agency, does not require a report.

Example: Using automated equipment for preparing an analysis of information maintained in a manual system without creating a continuing storage or retrieval capacity is not a change in equipment configuration.

(2) The Report on New Systems does not intend to inhibit the application of technology to data processing or to reduce the efficiency with which the IRS serves the public. It allows examination of the impact of new or altered data systems on citizens, the provision for confidentiality and security in those systems, and the extent to which the creation of the system will alter or change interagency or intergovernmental relationships related to information programs. The application of this reporting criteria must be consistent with these goals.

(3) In applying the submission criteria, use a reasonable standard to avoid excessive reporting of insignificant details that would have no meaningful effect upon any Privacy Act consideration.

(4) **Report Contents**: The Report on New Systems must consist of a brief narrative description and supporting documentation. The business unit that owns the records prepares the report.

(5) The narrative description must be a brief statement, no more than four pages, that:

a. Describes the purposes of the SOR.
b. Identifies the authority under which the SOR is to be maintained.

c. Gives the IRS's evaluation of the probable or potential effect of such proposal on the privacy including compliance with section (e)(7) of the Privacy Act, which says that 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."

d. Gives a brief description of steps taken by the IRS to minimize the risk of unauthorized access to the SOR, including a discussion of higher or lower risk alternatives considered for meeting the requirements of the system. Make a more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established available on request.

(6) The narrative statement should refer to any information in the supporting documentation rather than restate such information.

(7) Where changes to computer installations, communications networks, or any other general changes in information collection, handling, storage, or disclosure affect multiple SORs, submit a single combined new system report. In such cases, the narrative statement should address the overall privacy implications of the proposed change, identify all SORs affected by the change, and briefly describe any unique effect on any specific SOR.

(8) **Supporting Documentation**: Include an advance copy of the new or revised system notice.

a. For proposed alterations of existing systems, give the documentation in the same form as the IRS proposes to publish the public notice of such changes. If the IRS proposes to publish changes in the form of a revision to the public notice, give a copy of the proposed notices of revision.

b. If the IRS plans to supersede the entire existing notice, highlight changes from the published notice by underlining all new or revised parts. In some situations, the modification of the system may involve aspects not shown in the SORN, which requires no change; submit a copy of the existing notice with an explanation. Where the planned changes will be complex and will take place over years, it may not be possible to give an advance copy of the system notice; instead, submit a tentative outline or a suitable explanation.

(9) If the IRS proposes new exemption rules or changes to published exemption rules for the new or altered system, include an advance copy. If no change to existing exemption rules is required for the proposed new or altered system, the report must say that. Give proposed changes to existing exemption rules like that described for the system notices.

(10) Include an advance copy of any proposed rules setting forth the reasons why the system is to be exempted from any specific provision, if applicable.

(11) Submit the Narrative Statement and Supporting Documentation with a transmittal memorandum identifying the materials attached. Include existing descriptive materials in the Supporting Documentation. Copies of SORN, Notices of Exemptions or proposed rules should, to the extent possible, be consistent with the established publishing requirements for such materials.

(12) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. CM-1 Configuration Management -- Policy and Procedures
b. CM-4 Configuration Management -- Impact Analyses

10.5.6.3.12.1
(11-14-2023)
Reporting Systems of Records to OMB and Congress

(1) **General.** The Privacy Act requires each agency that proposes to set up or significantly change a SOR to give adequate advance notice of any such proposal to OMB, the Committee on Oversight and Accountability of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate. This advance notice is separate from the public comment period for new or modified routine uses required by subsection (e)(11) of the Privacy Act and discussed in section 6 of OMB Circular A-108. Agencies give advance notice to OMB and the committees of jurisdiction in Congress to allow an evaluation of the probable or potential effect of such a proposal on the privacy or other rights of individuals.

(2) **Advance Notice of a New or Modified System of Records.** Agencies must report to OMB and Congress any proposal to set up or significantly modify a SOR at least 30 days before the submission of the notice to the Federal Register for publication. OMB has 30 days to review the proposal and give any comments to the agency. The 30-day review period is separate from – and may not run concurrently with – the publication period in the Federal Register. Only significant changes to a SOR that require revision to the SORN, as described in section 6 of OMB Circular A-108, need to be reported to OMB and Congress; changes that are not significant do not need to be reported. Advance notice to OMB and Congress is required by subsection (r) of the Privacy Act. The purpose of the advance notice to OMB and Congress is to allow an evaluation of the potential effect of the proposal on the privacy and other rights of individuals.

(3) Although the review period generally requires no more than 30 days, OMB has the discretion to extend the 30-day review period based on the specific circumstances of the proposal. If an agency has questions about the timing of the review, the agency's SORN liaison must consult with OMB's Office of Information and Regulatory Affairs (OIRA).

(4) In circumstances where the agency cannot wait until the 30-day review period for OMB and Congress has expired to publish the notice in the Federal Register, the agency may send a formal written request from the SAOP to OIRA for an expedited advance review period (see section 7(d) of OMB Circular A-108 for information about expedited review requests).

(5) See Exhibit 10.5.6-3, Reporting Requirements, for new or altered Privacy Act Systems of Records reporting requirements.

10.5.6.4
(11-14-2023)
Privacy Notices

(1) This section gives instructions, guidelines, and procedures necessary for notification programs when privacy notices must be on forms and online.

(2) The section also explains when the Privacy Act requires notice of disclosure of a person's information due to compulsory legal process.

(3) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. PT-2 Personally Identifiable Information Processing and Transparency -- Authority to Process Personally Identifiable Information
b. PT-3 Personally Identifiable Information Processing and Transparency – Personally Identifiable Information Processing Purposes
c. PT-5 Personally Identifiable Information Processing and Transparency -- Privacy Notice
d. PT-5(2) Personally Identifiable Information Processing and Transparency -- Privacy Notice - Privacy Act Statements

10.5.6.4.1
(11-14-2023)
Privacy Notice Responsibilities

(1) The Privacy office oversees IRS compliance with Privacy Act notification programs.

(2) The business units must be familiar with the requirements because they prepare documents that ask individuals to fill out forms supplying personal information.

(3) Records owners hold responsibility for including necessary Privacy Act notices in administrative and tax forms and updating them when necessary.

(4) Media and Publications Services control the forms creation process, which includes routing necessary approvals of Privacy Act and Paperwork Reduction Act notices (PAPRANs). For more information on this process, refer to the *Paperwork Reduction Act Clearances page* on IRS Source.

Note: Federal agencies collect a wide variety of information to make sure the public is kept safe from harm, receive benefits to which they are entitled, and fulfill their missions. Such collections can also impose significant burdens on the public. The goal of the Paperwork Reduction Act (PRA) is to minimize the burden of these collections and maximize their usefulness. To help do this, the PRA requires agencies to estimate the burden and consult with the public on these estimates.

(5) Office of Chief Counsel (Procedure and Administration) approves changes to PAPRANs on forms related to tax administration when necessary. Counsel may coordinate with Privacy staff if necessary.

(6) Privacy Act notices on administrative (non-tax, such as personnel) forms require approval of Privacy, via email to the **Privacy mailbox*.

(7) If necessary, Privacy may coordinate with the Office of Chief Counsel (Procedure and Administration) about Privacy Act notices.

10.5.6.4.2
(11-14-2023)
Notice to Individuals Asked to Supply Information (Privacy Act Notice)

(1) The Privacy Act (Section (e)(3) requires each agency that maintains a SOR to inform each individual requested to supply information (either on the form it uses to collect the information, or on a separate form that can be kept by the individual) of:

a. The authority (whether granted by statute or by executive order) that authorizes the collection of the information and whether disclosure of such information is mandatory or voluntary.
b. The principal purpose(s) for which the information is intended to be used.
c. The routine uses of the information.
d. The effects on the individual, if any, of not supplying all or any part of the requested information.

Note: See Exhibit 10.5.6-5, Terms and Acronyms, for the definitions of applicable terms used in this list.

Caution: Do not mislead or inadvertently coerce the individual.

(2) The Privacy Act, OMB and NIST all include notice requirements for public information collections, including online (such as the privacy control PT-5, Privacy Notice). For Online Data Collection and Privacy Policy Notices, see those sections of IRM 10.5.1, Privacy Policy.

Note: Under Privacy Act Section (j), Treasury has exempted IRS Criminal Investigation records from the application of the Section (e)(3) notification requirement.

(3) A simple example or template, with brackets **[like this]** to fill in the details pertinent to the website or application, is:

[Name of information collection] Privacy Act Notice
Purpose: We are collecting *[what information]* to *[do what for what purpose]*.
Authority: The IRS is authorized to collect this information by the *[primary statute or other legal authority specifically for this purpose, usually without subsections, with links helpful for online]*.
Routine Uses: We may disclose this information to *[those listed in routine uses from the applicable Privacy Act SORN]* for *[purpose of routine use disclosure from the SORN]* under the routine uses published in *[SORN, with links helpful for online]*.
Consent: Providing this information is *[voluntary or required]* and necessary to *[do what this process does].* By giving us your information, you consent to its use for this purpose.
Consequences: If you choose not to give your information, *[list consequences to individual]*.
Online: *[For online data collection, including online forms, add:]* We protect your information in a secure and readily accessible environment. See IRS.gov/privacy for more information on your privacy rights. We may automatically collect *[what (such as user's IP address, location, and time of visit)]* for *[what purpose (such as site management or security purposes)]*.
Other: *[Other – Add any more considerations unique to this collection or mode of collection.]*

Reminder: Privacy Act notices on administrative (non-tax, such as personnel) forms require approval of Privacy, via email to the **Privacy mailbox*. For notices related to tax administration, Office of Chief Counsel (Procedure and Administration) approves changes to those PAPRANs when necessary.

(4) This provision makes sure agencies inform individuals from whom personal information is collected of the reasons for requesting the information, how it may be used, and what the consequences are, if any, of not supplying the information.

(5) The notion of informed consent is implicit in this provision, since agencies must give an individual with sufficient information about the inquiry to make an informed decision on whether to respond.

(6) The notice must inform the recipient. To be meaningful to the average person, it should avoid using technical language and should not be so lengthy as to discourage or confuse the reader. The content should summarize rather than itemize the information required to avoid unnecessary detail.

(7) This provision of the Privacy Act applies only to inquiries where agencies request individuals to give information about themselves or their own affairs, not about inquiries directed to third parties asking for information about someone else.

10.5.6.4.3
(11-14-2023)
Notice to Individuals Asked to Disclose Their Social Security Number

(1) Section 7 of the Privacy Act says it is unlawful for any federal, state, or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose that individual's social security number (SSN).

Note: This provision does not apply when the SSN is required by federal statute (such as in IRC 6109 and 5 USC).

(2) The Tax Reform Act of 1976 allows a state or political subdivision to require the disclosure of SSNs to establish the identity of any person affected by:

- Any tax law.
- Any general public assistance law.
- Any driver's license law.
- Any motor vehicle registration law.
- In the issuance of birth certificates and enforcement of child support orders.

Exception: An exception is made for any disclosures that are required by federal statute, and for a disclosure to any federal, state, or local government agency maintaining a SOR in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted before such date for the purpose of verifying the identity of an individual.

(3) An agency that requests an individual to disclose that individual's SSN is to inform the individual:

a. Whether the disclosure is mandatory or voluntary.
b. By what statutory or other authority such number is solicited.
c. What uses will be made of it.

(4) IRC 6109 gives the authority for requiring SSNs as identifying numbers for tax administration purposes.

(5) For more information on SSN Elimination and Reduction (SSN ER) efforts, refer to that section of IRM 10.5.1.

(6) The following NIST SP 800-53 security and privacy control addresses these Privacy Act requirements: PT-7(1) Personally Identifiable Information Processing and Transparency – Specific Categories of Personally Identifiable Information – Social Security Numbers. Refer to that section of IRM 10.5.1.

10.5.6.4.4
(11-14-2023)
The "Umbrella" Approach for Tax Returns

(1) The various inquiries made of individuals by the IRS during tax administration are part of a single process. Rather than include the same Privacy Act notice information in many forms or letters that are repeated contacts with the same individual about the same situation, the IRS has adopted an "umbrella" approach where the first contact of a series includes a notice that the individual may keep and that would apply to all future inquiries related to that situation. This approach spares the recipient from receiving repetitious and unnecessary identical notices.

(2) A universal Privacy Act notice in the Form 1040 instructions applies to:

a. U.S. Individual Income Tax Returns.
b. Declarations of estimated tax.
c. Any forms or other returns required to be filed as an attachment to, or in conjunction with, the Form 1040 series form.
d. Schedules, statements, or other documents related to the returns.
e. Later inquiries necessary to complete, correct and process the returns of taxpayers.
f. Determining the correct tax liability.
g. Collection of any unpaid tax, interest, or penalty.

(3) This umbrella notice fulfills the Privacy Act notice requirements for any further inquiries in the normal course of IRS campus processing, including initial billing of tax due on the returns.

(4) Although the notice given with the return instruction package would be legally adequate for later inquiries, the IRS makes available a further notice, Notice 609, Privacy Act Notice, for use when a distinct series of actions takes place beyond campus processing.

(5) The IRS revises Notice 609 as necessary to conform to the wording used for the universal notice approved for inclusion in the Form 1040 instruction packages.

(6) The IRS distributes Notice 609 to:

a. Taxpayers subject to collection activity on Taxpayer Delinquent Accounts.
b. Taxpayers subject to Taxpayer Delinquency Investigations (according to instructions provided by the proper Division Commissioner).
c. Taxpayers whose returns are selected for examination according to instructions provided by the proper Division Commissioner.

(7) The IRS gives more copies of Notice 609 to any taxpayer upon request.

(8) The distribution of Notice 609 described in (6) and (7) does not require any individual documentation, as such distribution is made in addition to the minimal legal requirement.

(9) The distribution of the universal notice, plus the distribution of separate Notice 609 for the collection- and examination-related stream, should satisfy the Privacy Act notice requirement for all expected tax administration inquiries.

Note: For Notice 609 purposes, the Appeals process is considered a continuation of the examination and collection processes.

(10) If officials meet circumstances requiring more notices, they may further distribute Notice 609, if the wording appears proper to the circumstances.

(11) Do not adopt separate Privacy Act notices for tax administration purposes without prior approval of the:

a. Proper headquarters business unit.
b. Privacy (via the **Privacy mailbox*).
c. Office of Chief Counsel (Procedure and Administration).

10.5.6.4.5
(11-14-2023)
Privacy Notices Not Related to Tax Administration

(1) The Privacy Act requirements for a notice to individuals asked to supply information, and a notice to individuals asked to disclose their SSNs, also apply to inquiries not related to tax administration, such as requests for information from IRS personnel for administrative purposes (such as personnel forms).

(2) The variety of information requested on such forms has made using a universal notice inappropriate, so those forms have individual Privacy Act notices. Include the notices in the form itself, whenever workable.

(3) The inclusion of necessary Privacy Act notices in administrative forms is the responsibility of the records owner. Such notices require approval of Privacy (via the **Privacy mailbox*). If necessary, Privacy coordinates with the Office of Chief Counsel (Procedure and Administration) about Privacy Act notices not related to tax administration.

10.5.6.4.6
(11-14-2023)
Online Privacy Policy Notices

(1) For more information on Online Data Collection and Privacy Policy Notices, see those sections of IRM 10.5.1, Privacy Policy.

(2) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. PM-20(1) Program Management -- Dissemination of Privacy Program Information – Privacy Policies on Websites, Applications, and Digital Services
b. PT-4 Personally Identifiable Information Processing and Transparency -- Consent

10.5.6.4.7
(11-14-2023)
Notifying Individuals that Their Records Were Made Available to a Person Under Compulsory Legal Process

(1) Subsection (e)(8) of the Privacy Act requires that agencies “make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record.”

(2) This provision applies to disclosures made under:

a. Subpoenas and summonses.
b. The order of a court of “competent jurisdiction,” as authorized by subsection (b)(11) of the Privacy Act.
c. An IRC 6103(i) ex parte order. See IRM 10.5.6.4.7.1, Notification Procedure.

Note: For disclosure of tax return and return information, refer to IRM 11.3.28, Disclosure to Federal Agencies for Administration of Non-Tax Criminal Laws, the Disclosure of Returns and Return Information Pursuant to IRC 6103(i)(1), IRC 6103(i)(2) and IRC 6103(i)(5) section. For the accountings required by IRC 6103(p)(3), refer to IRM 11.3.35, Requests and Demands for Testimony and

Production of Documents, the Accounting Requirements section, and IRM 11.3.37, Recordkeeping and Accounting for Disclosures, the General Rules section.

d. This provision does not apply to disclosures from a SOR exempt under subsection (j)(2) of the Privacy Act, as they are not subject to the subsection (e)(8) notification requirement.

(3) This provision does not apply to disclosures made under a written request by, or with the written consent of, the individual to whom the record relates. It does not apply if the process leading to disclosure is at the request or on the behalf of the subject of the record.

(4) While this provision does not apply to disclosures made under subsections (b)(1), (2), (4)-(10), and (12) of the Privacy Act, this provision does apply when a disclosure is made under a routine use as provided by subsection (b)(3) that authorizes disclosures in response to subpoenas or court orders.

10.5.6.4.7.1
(11-14-2023)
Notification Procedure

(1) The person authorized to make the disclosure following established procedures for the compulsory legal process carries out this procedure.

(2) Examine any compulsory legal process that appears to make an individual's record (which is subject to the Privacy Act) available to a third party to find whether it is subject to the notification procedure.

Note: The notification procedure only becomes effective if the IRS disclosed the record. Do not interpret this instruction as authorization for any disclosure.

(3) Give notice within five business days of making a disclosure under compulsory legal process, except as provided in (4).

(4) If the disclosure is in response to a grand jury subpoena or an ex parte order under IRC 6103(i)(1), (5), or (7)(C), do not give the notice until the subpoena or order becomes a matter of public record. If the subpoena or order does not note whether a matter of public record, it may be necessary to request the issuing authority to tell the IRS when the matter becomes public, so that the IRS may issue the required notice. For notification rules involving ex parte orders in judicial, administrative, or grand jury situations, refer to IRM 11.3.28, the Notifying Individuals That Their Records Were Made Available Under a Compulsory Legal Process section, and IRM 11.3.35, the Notifying Individuals That Their Records Were Made Available to a Person Under Compulsory Legal Process section.

(5) Mail the notice to the individual's last known address. Keep one copy of the notice in the administrative or other file from which the disclosed documents originated. Associate one copy with the record disclosed, if practical.

10.5.6.5
(11-14-2023)
Privacy Act Recordkeeping Restrictions (Civil Liberties Protections)

(1) This section and its subsections offer Privacy Act recordkeeping restriction policies designed to carry out fair information practices, including:

- Protecting civil liberties and Constitutional rights, such as First Amendment compliance, by not gathering information that is not authorized by statute or presidential executive order.

  Note: For more information, refer to the Civil Liberties section of IRM 10.5.1.

- Reducing the chances of receiving less accurate information from third parties by collecting information, to the greatest extent practical, directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs.

  Note: For more information, refer to the Data Quality IRS Privacy Principle in IRM 10.5.1.

- Maintaining only such information about an individual as is relevant and necessary to carry out an agency purpose required by statute or by presidential executive order.

  Note: For more information, refer to the Purpose Limitation and Minimizing Collection, Use, Retention, and Disclosure IRS Privacy Principles in IRM 10.5.1.

(2) The Privacy Act says that agencies will maintain no record describing how any individual exercises their rights guaranteed by the First Amendment unless at least of one of these applies:

a. Expressly authorized by statute.
b. Expressly authorized by the individual about whom the record is maintained.
c. Pertinent to and within the scope of an authorized law enforcement activity.

Note: In this IRM, the terms maintenance, maintain, or keep refer to the privacy lifecycle of information: creation, collection, receipt, use, processing, maintenance, access, inspection, display, storage, disclosure, dissemination, or disposal.

(3) The First Amendment says:

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof, or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for redress of grievances."

(4) Congress intended that in determining whether a particular activity is the exercise of a right guaranteed by the First Amendment, agencies should apply the broadest reasonable interpretation.

(5) Keep no file of individuals who are merely exercising their constitutional rights. See IRM 10.5.6.5.2, Permissible Records, for records we may keep.

(6) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. PM-20(1) Program Management -- Dissemination of Privacy Program Information – Privacy Policies on Websites, Applications, and Digital Services
b. PM-22 Program Management -- Personally Identifiable Information Quality Management
c. PT-2 Personally Identifiable Information Processing and Transparency -- Authority to Process Personally Identifiable Information

d. PT-3 Personally Identifiable Information Processing and Transparency – Personally Identifiable Information Processing Purposes
e. PT-4 Personally Identifiable Information Processing and Transparency – Consent
f. PT-7 Personally Identifiable Information Processing and Transparency – Specific Categories of Personally Identifiable Information
g. PT-7(2) Personally Identifiable Information Processing and Transparency – Specific Categories of Personally Identifiable Information - First Amendment Information

10.5.6.5.1
(11-14-2023)
Recordkeeping Restrictions - Responsibilities

(1) All IRS personnel involved in the design, development, operation, or maintenance of any SOR subject to the Privacy Act must be aware of the Act's recordkeeping restrictions outlined in IRM 10.5.6.5, Privacy Act Recordkeeping Restrictions (Civil Liberties Protections). You should be alert to any potential violation of such.

(2) If you recognize any questionable practices of this prohibition, report the details to the official responsible for prescribing the SOR, for evaluation, and correction.

(3) If you receive any inquiry from a member of the public questioning the content of any SOR about the exercise of First Amendment rights, you must send the inquiry, supplying any available background information, through channels, to their management for response and proper action.

(4) Personnel and management requiring guidance about any information being recorded in a SOR under their control should seek Privacy's help by email to the **Privacy mailbox*.

(5) All supervisory or other personnel that have review responsibilities for case records should be alert to First Amendment issues and include them in their reviews.

10.5.6.5.2
(11-14-2023)
Permissible Records

(1) The IRS may maintain records describing the exercise of First Amendment rights only if one of the following conditions is met.

a. A statute specifically authorizes it.

1) Specific authorization means that a statute explicitly says an agency may maintain records on activities whose exercise is covered by the First Amendment, not merely that the agency is authorized to set up a system of records.
2) The statute need not specifically address the maintenance of records of First Amendment activities if it specifies that such activities are relevant to a determination about the individual.

Example: Taxpayers must give information necessary to verify deductions on their tax returns. The IRS may record such information although, sometimes, it may reveal how individuals exercise their First Amendment rights, such as, religious affiliation, group membership, or political preference.

b. The individual expressly authorizes it.

Example: IRS employees may offer information about their activities in a community group to enhance their chances for advancement by showing the acquisition of some specialized experience or leadership skill.

c. The agency requires the record for an authorized law enforcement function. Congress intended to make certain that political and religious activities are not used as a cover for illegal activities.

Example: The IRS may reasonably consider individuals who advocate, or who are active in organizations that advocate, noncompliance with the tax laws, as possibly being involved in actual violations of the tax laws. The IRS may maintain appropriate records of such activities for compliance purposes.

10.5.6.5.3
(11-14-2023)
Equal Treatment

(1) This section of the Privacy Act requires agencies to treat all persons fairly and equally under applicable laws. The absence of First Amendment information from agency records helps to prevent selective treatment of persons based on religion, opinion, or group membership.

(2) IRS personnel hold responsibility for avoiding any possible inference of selective treatment of individuals based on their exercise of First Amendment rights.

(3) Refer to the Data Quality IRS Privacy Principle and Civil Liberties sections of IRM 10.5.1.

10.5.6.5.4
(11-14-2023)
Collecting Information Relating to Individuals from Third Party Sources

(1) Subsection (e)(2) of the Privacy Act says that an agency must:

"Collect information to the greatest extent practical directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits and privileges under Federal programs."

(2) This provision stems from a concern that information collected from third party sources could be erroneous, outdated, irrelevant, or biased.

(3) This provision requires that agencies make decisions under federal programs that affect an individual based on information supplied directly by that individual "to the greatest extent practicable."

(4) Officials responsible for SORs with information collected from third-party sources must consider in their periodic review of procedures whether their practices are consistent with the intent of subsection (e)(2) of the Privacy Act and IRM 10.5.6.2, Privacy Act General Provisions. This periodic review of procedures must include a review of those parts of the IRM about the collecting information from third-party sources.

(5) In analyzing each situation where the IRS collects personal information from a third-party source, each business unit should consider the following:

a. The nature of the program. We might only be able to collect the kind of information needed from a third party, such as investigations where the individual's records are not available.
b. The cost of collecting the information directly from the individual as compared with the cost of collecting it from a third party.
c. The risk that the particular elements of information we proposed to collect from third parties, if incorrect, could result in an adverse determination.
d. The need to ensure the accuracy of information supplied by an individual by verifying it with a third party or to get a qualitative assessment (such

as in verifying information submitted on a tax return or in connection with the review of an application for employment).

e. The opportunities for verifying, whenever practical, any such third-party information by consulting with the individual before making a determination based on third-party information.

(6) The aim is to get information directly from the individual involved whenever practical to do so.

(7) Refer to the Data Quality IRS Privacy Principle section of IRM 10.5.1.

10.5.6.5.4.1
(11-14-2023)
Inquiries Affected

(1) Most inquiries made by the IRS, both in determining tax liability and in dealing with its personnel, are subject to the requirement of subsection (e)(2) of the Privacy Act.

(2) Inquiries in connection with criminal investigations, maintained as SORs exempt under subsection (j)(2) of the Privacy Act, are not subject to the requirements of subsection (e)(2).

(3) Although the IRS must "collect information to the greatest extent practicable directly from the subject individual," the IRS cannot verify compliance with internal revenue laws solely by using information from returns and documents filed with the IRS. The IRS must get certain information from outside sources.

(4) We must still follow the guidelines in this IRM for inquiries to third parties (in connection with the gathering, solicitation, and documentation of evidence necessary in developing cases that have been assigned for collection of taxes or examination or investigation of a tax liability), including IRM 10.5.6.2, Privacy Act General Provisions, and IRM 10.5.6.5.4, Collecting Information Relating to Individuals from Third Party Sources.

(5) See IRC 7602 for rules for recording third party contacts. Refer to IRM 11.3.21, Investigative Disclosure, the Disclosure of Returns and Return Information for Tax Administration Purposes under IRC 6103(k) section.

10.5.6.5.5
(11-14-2023)
Restrictions on the Maintenance of Information About Individuals

(1) To protect civil liberties and avoid unnecessary intrusion upon individual privacy, subsection (e)(1) of the Privacy Act says that each agency that maintains a SOR must:

"Maintain in its records only such information about an individual as is relevant and necessary to carry out a purpose of the agency required by statute or by executive order of the President."

(2) Use or collect PII only when necessary and relevant for legitimate IRS purposes, namely tax administration and other authorized purposes. Refer to IRM 10.5.1, the Purpose Limitation section.

(3) To reduce risk of intentional or inadvertent improper use of personal data, limit the collection, use, retention, and disclosure of PII to what is minimally necessary for the specific purposes for which it was collected, unless specifically authorized. Refer to IRM 10.5.1, the Minimizing Collection, Use, Retention, and Disclosure section.

(4) See Exhibit 10.5.6-5, Terms and Acronyms, for definitions for the following terms, which are used throughout the rest of this IRM:

- Maintain
- Relevant
- Necessary

(5) See the Monitoring of Individuals section of IRM 10.5.1.

10.5.6.5.5.1
(11-14-2023)
Records Affected

(1) Subsection (e)(1) of the Privacy Act applies to all records maintained by the IRS (including those about taxpayers, IRS personnel, and other individuals), unless otherwise exempted.

(2) The IRS has asserted exemptions provided by the Privacy Act under subsection (e)(1) for various SORs.

(3) The exempt systems are primarily those that are investigative. They are exempted to allow an orderly collection of data without challenge until the investigator can decide whether the data is relevant and necessary. They cannot decide the relevance or necessity of specific information during the early stages of an investigation. Relevance and necessity are questions of judgment and timing. What appears relevant and necessary when collected may later be found irrelevant or unnecessary. Only after evaluating the information can the investigator find the relevance and necessity of such information with certainty.

(4) When the IRS receives information about violations of law within the jurisdiction of other agencies, the IRS keeps this information to send the material to the proper agencies or to respond to valid requests from those agencies to the extent provided by law or regulation.

(5) The handwritten notes of an agent taken during the interview of a witness continue to be relevant and necessary. Do not destroy them even though they may have been in a formal report. Court decisions have held that you must preserve such notes as discoverable.

(6) The IRS must limit its inquiries to information necessary for the enforcement and administration of tax laws, other matters within its jurisdiction or delegated authority, and IRS internal administration.

10.5.6.5.5.2
(11-14-2023)
Relevant and Necessary Guidelines

(1) For the IRS to maintain information in its records, the information must serve a purpose required by statute or executive order.

(2) The authority of the IRS to maintain a SOR does not give it the authority to maintain any information that is merely useful, nor may the IRS maintain information merely because it is relevant. The information must be both relevant and necessary to carry out the authorized purpose.

(3) A determination that information is relevant and necessary is judgmental. Base such judgments on a realistic evaluation of the purpose served by the information maintained and a sound understanding of the principles underlying the Privacy Act. Refer to the IRS Privacy Principles section in IRM 10.5.1.

(4) The standards used to define necessity and relevance vary widely depending upon the activity involved and the specific needs of a case.

(5) Some examples of factors the IRS may consider in determining whether information is relevant and necessary are:

a. How does the information relate to the legal purpose for which the system is maintained?
b. What are the adverse consequences, if any, of not collecting this information?
c. Could we meet the need using information not in individually identifiable form?
d. Do we need to collect the information on every individual who is the subject of a record in the system, or would a sampling procedure suffice?
e. At what point will the information have satisfied the purpose for which it was collected, such as how long is it necessary to keep the information?
f. Is the information, while generally relevant and necessary to carry out a statutory purpose, specifically relevant and necessary only in certain areas?

(6) Besides providing a standard that protects the privacy of the individual, the concepts of relevance and necessity can contribute to effective operations. If you keep irrelevant and unnecessary information, it wastes resources. Instead, use this standard to promote efficiency and good management.

(7) This provision does not intend to interfere with the maintenance, evaluation, or presentation of evidence in civil or criminal matters.

(8) Although the IRS may have exempted some SORs from subsection (e)(1), the principles of relevance and necessity stay applicable to all records to the extent that the IRS can apply them. Apply these provisions to exempt SORs to the extent practical. Refer to the Purpose Limitation and Minimizing Collection, Use, Retention, and Disclosure IRS Privacy Principles in IRM 10.5.1.

(9) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. SA-3 System and Services Acquisition -- System Development Life Cycle
b. SA-8(33) System and Services Acquisition -- Security and Privacy Engineering Principles - Minimization

10.5.6.5.5.3
(11-14-2023)
Recordkeeping Restrictions Required

(1) The Privacy Act does not require a detailed review of the contents of each record within a system. Yet IRS personnel consider the legality, relevance, and necessity of the general categories of information we maintain to follow the law.

(2) Responsible officials must review SORs to follow these recordkeeping requirements when:

a. Designing a new SOR.
b. Proposing any changes to an existing SOR.
c. Republishing a SORN.
d. Considering an individual's request for deletion of information not relevant and necessary.

Note: In review of such request, consider whether the inappropriate information is an isolated occurrence or is characteristic of the SOR. If the inclusion of inappropriate information appears characteristic of the SOR or sufficiently widespread to call for broad remedial action, refer the concern to the official responsible for prescribing the SOR to take proper action.

e. Reviewing the SOR after receiving information showing the need for such.

(3) All IRS personnel involved in the design, development, operation, or maintenance of any SOR subject to the Privacy Act must be aware of the provisions about the legality, relevance, and necessity of information maintained about an individual.

(4) Personnel recognizing any questionable or undesirable practices on these provisions should report the details, through channels, to the official prescribing the SOR for evaluation and proper action.

(5) Each headquarters official who prescribes the maintenance of a SOR or issues IRM instructions to personnel involved in the design, development, operation, or maintenance of any SOR, should expand such instructions to include proper or necessary guidance to follow the relevance and necessity provisions of the Privacy Act, as outlined in (6) and (7).

(6) Automated SORs characteristically involve limited data elements that apply to many records. Including inappropriate information tends to be characteristic of any SOR in which it occurs. Emphasize proper evaluation of the information recorded at the time you update or design the system. Since all the data elements to be included are known at the time of first design, consideration of each element should result in an extremely high degree of compliance with the Privacy Act requirements.

(7) Systems of records that consist primarily of information entered upon preprinted forms require a different approach. The form design must request only relevant and necessary information. Besides designing or revising forms, also consider these aspects in the instructions on the use and preparation of the forms.

(8) Far more complex problems exist when a SOR consists of information gathered by personal interviews or investigative procedures and recorded in narrative form. The unstructured nature of such information gathering creates a risk of abuse in individual cases, which is difficult to detect and correct. Instructions for designing or maintaining such records should stress the following:

a. Guidelines to help personnel follow the relevance and necessity provisions, keeping in mind the wide variance between activities and the specific needs of cases. Guidelines should, to the extent possible, help prevent inappropriate inquiries without hampering investigative techniques.
b. Personnel engaged in investigative inquiries should use mature judgment and exercise self-discipline in deciding the information to request and record.
c. Use extreme caution when dealing with highly personal information relating to the relationships between individuals or personal activities that would not generally be made public by the individual involved.
d. The mere fact that a person volunteers personal information does not serve as authority to record it, as it may be irrelevant and unnecessary.
e. Personnel may have contact with individuals who follow a variety of lifestyles. Such factors may be irrelevant and unnecessary. Do not collect information about them unless relevant and necessary to a case.
f. If possible, avoid opinions or subjective impressions of individuals. However, certain cases may require recording such impressions, especially those involving potential assaults upon IRS personnel, cases in high crime areas, cases about uncollectible accounts, and cases recommend-

ing further investigation. Identify opinions or subjective impressions as such, and, whenever proper, add factual substantiation.

Caution: Use extreme caution when dealing with highly personal information relating to the relationships between individuals or personal activities that would not generally be made public by the individual involved.

g. Use existing supervisory or other review procedures to identify when personnel maintain information that is not relevant or necessary. If you create or discover a record that is irrelevant to the SOR, remove it from the SOR and place it in the correct filing or recordkeeping location. Do not dispose of the record until its authorized destruction date (if one exists), as identified in either Document 12829, General Records Schedules, or Document 12990, Records Control Schedules. Refer to the IRM 1.15 series, Records and Information Management, for more information on records management responsibilities. If you discover erroneous or incorrect information, correct it and note the file with the date of correction. Reviewers should tell personnel of the irrelevant entry to help them clearly understand the meaning and importance of relevance and necessity. Whatever trends reviewers identify, make recommendations to the responsible official for further guidelines or other corrective actions.

h. In appropriate situations, develop awareness and responsiveness to Privacy Act principles as factors for use in employee evaluations. For more information, refer to IRM 10.5.1, the IRS Privacy Principles section.

10.5.6.5.6
(11-14-2023)
Privacy Act Requirement to Maintain Accurate, Relevant, Timely, and Complete Records

(1) Subsection (e)(5) of the Privacy Act says each agency that maintains a SOR must:

"... Maintain all records that are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."

a. This provision looks to minimize, if not eliminate, the risk that an agency will make an adverse determination about an individual based on incorrect, incomplete, irrelevant, or out-of-date records. See Exhibit 10.5.6-5, Terms and Acronyms, for the definition of the term *Determination.*

b. The phrase "as is reasonably necessary" recognizes the difficulty of setting absolute standards of data quality.

Note: Place emphasis on assuming the quality of the record in terms of its use in making decisions affecting the rights, benefits, entitlements, or opportunities (including employment) of the individual. Apply the standards at the time of making a determination.

(2) Subsection (e)(6) of the Privacy Act says:

"... prior to disseminating any record about any individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section (the Freedom of Information Act), make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes."

a. The primary aim of this provision is to assure the quality of records disclosed to persons that are not subject to the provisions of subsection (e)(5).

Note: This applies whenever the IRS makes a disclosure to a person other than the individual to whom it relates.

b. The provision also recognizes that information disclosed to other agencies is subject to the standards of accuracy established by those agencies. This provision does not apply to disclosures made to an agency. See Exhibit 10.5.6-5, Terms and Acronyms, for the definition of the term **Agency.**

(3) Refer to the IRM 10.5.1, sections on Data Quality and Verification and Notification.

(4) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. PM-22 Program Management -- Personally Identifiable Information Quality Management
b. SI-1 System and Information Integrity -- Policy and Procedures
c. SI-12 System and Information Integrity -- Information Management and Retention
d. SI-18 System and Information Integrity -- Personally Identifiable Information Quality Operations
e. SI-18(4) System and Information Integrity -- Personally Identifiable Information Quality Operations - Individual Requests

10.5.6.5.6.1
(11-14-2023)
Exempt Systems

(1) Various SORs have been named exempt under subsection (j)(2) of the Privacy Act from the provisions of subsection (e)(5).

(2) The Privacy Act subjects all SORs to the provisions of subsection (e)(6) of the Privacy Act.

10.5.6.5.6.2
(11-14-2023)
Actions Required to Ensure Accurate, Relevant, Timely, and Complete Records

(1) When putting information into any system, phrase the language so as not to misrepresent the facts, or subject it to an incorrect or misleading interpretation.

Note: Record statements made by witnesses about an individual as such and do not note them as established facts.

(2) Information collected must be relevant, timely, and complete.

Reminder: Tell technical employees such as Revenue Agents and Revenue Officers to keep their files clean of unrelated materials.

Example: When you print information from third-party data or asset information services or other such system, immediately discard all material on unrelated parties unless you decide such information is necessary (such as to detail specific search methods).

(3) Information put into IRS records must relate to some matter that the IRS is authorized and required to maintain to carry out its lawful mission.

Note: Information maintained about personnel must relate only to their employment.

(4) Information must be complete to avoid misrepresentation or unfairness, or to avoid presenting an unfair picture of a situation that could result in a determination harmful to the rights of the individual.

Caution: Completeness does not mean more information than relevant or necessary. Records should include only those elements of information that clearly bear on the determination for which the records are intended to be used, but they should include all elements necessary to make the determination.

(5) Before disclosing any record about an individual to a person (not an agency) other than the individual to whom it relates, make reasonable efforts to meet the requirements of subsection (e)(6) relating to accuracy, completeness, timeliness, and relevance and that the record relates to the purposes of the IRS.

(6) Any record disclosed must be as accurate as when the IRS made the determination about the individual. If the information does not meet this standard, correct the record before disclosure.

(7) The actions required by (6) and (7) do not lend themselves to specific periodic actions. However, this does not reduce the importance of the IRS responsibility to follow the provisions.

a. Meeting the demands of these provisions requires all IRS personnel to have an awareness of the rights of individuals.
b. Personnel must be aware that notations made and actions taken may have far-reaching effects.
c. Personnel must make sure that the records they help to create do not result in an unfair determination about any individual.

10.5.6.6
(11-14-2023)
Privacy Act Requests for Non-Tax Records

(1) The Privacy Act gives individuals certain rights to request information as to records in agency SORs, subject to various exemptions and restrictions. This section addresses individual non-tax Privacy Act requests about their information in IRS SORs. Privacy Act Requests and offices responsible for processing include:

a. IRM 10.5.6.6.2, Requests for Notification of and Access to Privacy Act Records: Disclosure.
b. IRM 10.5.6.6.3, Requests for Amendment of Non-Tax Privacy Act Records: The business unit with control of the records.
c. IRM 10.5.6.6.4, Requests for Disclosure of Privacy Act Records: Internally, the business unit with control of the records; externally, Disclosure.
d. IRM 10.5.6.6.5, Privacy Act Complaints: Privacy.
e. IRM 10.5.6.6.6, Requests for Privacy Act Accounting of Disclosures: Privacy.

Note: For tax records protected by IRC 6103, the requirements of that section take precedence over the Privacy Act. For a request for tax records, refer to the Routine Established Agency Procedures section of IRM 11.3.13, Freedom of Information Act.

(2) Since most IRS non-tax records relate to personnel files, see IRM 10.5.6.8, Personnel Records, for details on personnel records individuals might request.

(3) These Privacy Act requirements for notification, access, amendment, and accounting reflect the IRS Privacy Principle of Access, Correction, and Redress. Refer to that section of IRM 10.5.1.

(4) The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. AC-1 Access Control -- Policy and Procedures
b. AC-3(9) Access Control -- Access Enforcement - Controlled Release
c. AC-3(14) Access Control -- Access Enforcement - Individual Access
d. PM-20 Program Management -- Dissemination of Privacy Program Information
e. SI-1 System and Information Integrity -- Policy and Procedures
f. SI-12 System and Information Integrity -- Information Management and Retention
g. SI-18 System and Information Integrity -- Personally Identifiable Information Quality Operations
h. SI-18(4) System and Information Integrity -- Personally Identifiable Information Quality Operations - Individual Requests

10.5.6.6.1
(11-14-2023)
How to Make a Privacy Act Request

(1) This policy applies to current internal personnel for non-tax Privacy Act records. For members of the public, refer them to How to write a Privacy Act request on the *IRS.gov Privacy Policy page*.

Note: If the request is for your own tax records, refer to the Routine Established Agency Procedures section of IRM 11.3.13, Freedom of Information Act.

(2) Current internal personnel may request access to, amendment of, or disclosure of information about themselves through established procedures directly from the business unit in control of the record. For most, this means asking your manager or HCO about your personnel records. Give enough information for them to find the records, using the elements in this section. Cite this IRM section in your request to help the record owner understand their responsibility.

Note: For managers or HCO, if an employee asks about their own records, respond to them (subject to any access exemptions and restrictions). If you have questions about Privacy Act requests, email **Privacy*.

(3) If you still need your records after asking for them directly, make a formal Privacy Act request via **Privacy*, including the required elements in this section. Privacy works with the business unit with control of the records for them to respond.

(4) This policy applies to all Privacy Act requests. The types of requests are described in these sections:

a. IRM 10.5.6.6.2, Requests for Notification of and Access to Privacy Act Records.
b. IRM 10.5.6.6.3, Requests for Amendment of Non-Tax Privacy Act Records.
c. IRM 10.5.6.6.4, Requests for Disclosure of Privacy Act Records.
d. IRM 10.5.6.6.5, Privacy Act Complaints.

e. IRM 10.5.6.6.6, Requests for Privacy Act Accounting of Disclosures.

(5) For all Privacy Act requests, follow the regulations in *section 3, Appendix B of Title 31, Part I, Subpart C, of the CFR* and include these elements. They must:

a. Be made in writing and signed by the person making the request, who must be the individual about whom the record is maintained.

Note: Internally, a request on IRS.gov email is a signature.

b. Be marked "Privacy Act Request" and state the kind of request (for notification and access, amendment or review of refusal to amend, disclosure, complaint, or accounting).

c. Give the name of the SOR to which access is sought. See IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs).

d. Give enough information (such as the record sought, the date of the record, or the period in which the record was compiled) to help find the record with a reasonable amount of effort.

e. State that you are a citizen of the United States or an alien lawfully admitted for permanent residence in the United States.

f. Give verification of your identity. See IRM 10.5.6.6.2.1, Verification of Identity.

g. Be sent internally to **Privacy*. Members of the public must refer to How to write a Privacy Act request on the *IRS.gov Privacy Policy page*.

h. State whether you wish to inspect the records or want to have a copy made.

i. Give a firm agreement to pay the fees for duplication that might be incurred (see IRM 10.5.6.6.2.2, Duplication Fee); and if necessary, give written consent for release of the information to your authorized representative (see IRM 10.5.6.6.4, Requests for Disclosure of Privacy Act Records).

10.5.6.6.2
(11-14-2023)
Requests for Notification of and Access to Privacy Act Records

(1) A request for notification of and access to non-tax Privacy Act records comes from an individual wanting to know what non-tax records the IRS has about them and asking for access to such records.

(2) This section explains how we respond to requests for notification of and access to non-tax Privacy Act records. We may receive requests internally or externally.

(3) For managers, if your employee asks for their own records directly, allow them access (subject to any access exemptions and restrictions) under established agency procedures, if possible, without the need for a formal Privacy Act request.

(4) For HCO, if you receive a request from an employee for their own records directly, allow them access (subject to any access exemptions and restrictions).

(5) If you have questions about Privacy Act requests, email **Privacy*. Disclosure works with the business unit in control of the records to help the business unit to respond.

(6) Disclosure helps the business unit with control of the requested records respond to Privacy Act requests for notification and access as follows:

a. Send requests marked as FOIA to Disclosure. For more information on the FOIA, refer to IRM 11.3.13, Freedom of Information Act. Disclosure processes FOIA requests.
b. For responsibilities, time limits, and processing steps for notification and access in *section 3, Appendix B of Title 31, Part I, Subpart C, of the CFR*.
c. Upon receipt of a written Privacy Act request for notification of and access to records, verify its completeness with the elements in IRM 10.5.6.6.1, How to Make a Privacy Act Request.
d. Although individuals should meet all the requirements, all the requested information may not be necessary to process every request. Exercise discretion in accepting requests as filed if they meet enough procedural requirements to allow processing.
e. For requests by mail, verify the identity of the requestor following IRM 10.5.6.6.2.1, Verification of Identity. For internal requests from current personnel received from an IRS email account, you do not need to verify their identity further because the system authenticates them as IRS personnel. For requests from the public through the online portal from How to write a Privacy Act request on the *IRS.gov Privacy Policy page*, the portal verifies their identity.
f. For requests about information in a SOR that is exempt from notification and access under Privacy Act Section (k)(2), establish that the requester has been denied a right, privilege, or benefit that the requester would have otherwise been entitled to under federal law because of the maintenance of such material, which may give them right to access. Refer to Privacy Act Section (k)(2) for details.
g. If a request for notification and access omits any information needed to process the request, tell the requester within 10 business days of the information needed before the IRS can process the request. Then close the case.
h. If a request extends to many SORs, or systems that could not possibly have information relating to the requester, contact the requester to help them refine the request.
i. Contact the business unit with control of the requested records. Give a copy of the request to the official with control of the records, asking them to find whether they have a record and whether they can give access.
j. The business unit with control of the records must tell the requester whether the SOR has a record about the requester and allow access, unless the system is exempt from the notification requirement.
k. If the request is for medical records, including psychological records, consult with the official with control of the records to decide if release could have an adverse effect on the individual; if so, that release will be only to a physician authorized in writing to have access to such records.
l. All disclosures made under the access and notification provisions must be consistent with all other disclosure requirements. Deletions may be necessary to protect information about persons other than the requester.
m. The business unit with control of the records must decide whether to grant or deny access within 30 business days after receipt of a valid request. If we cannot respond within 30 days, tell the requester of the reasons for the delay and of the estimated date we will answer the request.
n. The Privacy Act gives no provision for the administrative appeal of access denials. Responses must not mention any right to judicial review when a request does not follow proper regulations and is not adequate to allow processing. Make no mention of a right to judicial review when requested

records are in an exempt SOR, or where the requester has not established that the requester was denied a specific right, privilege, or benefit to which the requester would otherwise be entitled under federal law because of the maintenance of such material.

10.5.6.6.2.1
(11-14-2023)
Verification of Identity

(1) This section applies to requests received by mail. For internal requests from current personnel received from an IRS email account, you do not need to verify their identity further because the system authenticates them as IRS personnel. For requests from the public through the online portal from How to write a Privacy Act request on the *IRS.gov Privacy Policy page*, the portal verifies their identity.

(2) **Decedents:** Use discretion in decedent Privacy Act situations. The IRS must disclose only the minimum information necessary to a person who has documentation to prove they have legal responsibilities to the decedent to allow that person to fulfill their legal duties. For further information about deceased employees, see IRM 10.5.6.8.3, Access to Records of Deceased Employees.

(3) The regulations in *section 3, Appendix B of Title 31, Part I, Subpart C, of the CFR* require:

a. A signature, address, and one other item of identification, such as a copy of a driver's license or other document bearing the individual's signature.
b. Individuals may also establish their identity either in person or by mail by supplying a notarized statement swearing or affirming to their identity, and to the fact that they understand the penalties provided in Privacy Act Section (i)(3) for requesting or getting access to records under false pretenses.

(4) In addition to the requirements above, the employee receiving or processing the written request may require more proof of an individual's identity before acting, if necessary to protect against an unauthorized disclosure.

(5) A parent of any minor, the attorney-in-fact of a person, or the legal guardian of any individual who has been declared incompetent due to physical or mental incapacity by a court of competent jurisdiction, must (in addition to the identification requirements) give adequate proof of legal relationship and authority before the parent, attorney-in-fact, or guardian may act on behalf of such minor or individual.

10.5.6.6.2.2
(11-14-2023)
Duplication Fee

(1) The sole fee to the public under the Privacy Act is for the cost of providing copies of records. For more information, see IRM 11.3.5, Fees.

10.5.6.6.3
(11-14-2023)
Requests for Amendment of Non-Tax Privacy Act Records

(1) A request for amendment of non-tax Privacy Act records comes from an individual wanting to correct non-tax records the IRS has about them that they feel are not correct, relevant, timely, or complete.

Note: Statutory exemption for amendment of tax records: IRC 7852(e) says that the IRS must not apply subsections (d)(2), (d)(3), (d)(4), and (g), of the Privacy Act (the amendment and civil litigation provisions), directly or indirectly, to the determination of liability of any person for any tax, penalty, interest, fine, forfeiture, other imposition or offense to which the provisions of the IRC apply. Respond to Privacy Act requests to correct tax records that

may affect a person's liability by citing or quoting IRC 7852(e), within the context of a proper explanation. Give no statement explaining appeal rights.

(2) This section explains how we respond to requests for amendment of non-tax Privacy Act records. We may receive requests internally or externally.

(3) For managers, if your employee asks for you to amend their records directly, respond to them (subject to any access exemptions and restrictions).

(4) For HCO, if you receive a request from an employee to amend their records directly, respond to them (subject to any access exemptions and restrictions).

(5) If you have questions about Privacy Act requests, email **Privacy*. Privacy works with the business unit in control of the records to help the business unit respond.

(6) For responsibilities, time limits, and processing steps to amend records, including any review and adjudication of an adverse determination, refer to *section 3, Appendix B of Title 31, Part I, Subpart C, of the CFR*. This guidance mirrors that in IRM 10.5.6.6.2, Requests for Notification of and Access to Privacy Act Records, including IRM 10.5.6.6.2.1, Verification of Identity, and IRM 10.5.6.6.2.2, Duplication Fee.

(7) Send requests to amend a non-tax record under the Privacy Act to the business unit with control of the requested records (usually the official named in the SORN). Refer the business unit to this IRM section and tell them to email **Privacy* with any questions.

(8) As needed, Privacy helps the business unit with control of the requested records (usually the official named in the SORN) respond to Privacy Act requests for amendment following the regulations and this policy. The responder in the responsible office must:

a. Send, within 10 business days, written acknowledgement of the request and that the responsible office will respond within 30 business days.
b. If the request omits any information needed to process the request, let the requester know what you need.

Reminder: The IRS does not amend tax records under the Privacy Act. See IRM 10.5.6.6.3, Requests for Amendment of Non-Tax Privacy Act Records.

c. Respond in writing within 30 business days of the decision whether to grant the request in whole or part.
d. If you cannot respond within 30 business days, tell the individual in writing within such time of the reasons for the delay and the approximate time needed.
e. If you decide to amend the record, make the requested changes and tell the individual in your response. If you disclosed the record and accounted for it via Form 5482, Record of Disclosure, let the recipient know of the changes. See IRM 10.5.6.7, Privacy Act Accounting of Disclosures. Upon request, give the individual a copy of the record, as amended, subject to the payment of the right fees.
f. If not amending the record, tell the individual in writing of the adverse determination with the reasons for refusal to amend the record and their right to request an independent review of the adverse determination by a reviewing officer under the regulations in *section 3, Appendix B of Title*

31, Part I, Subpart C, of the CFR. See IRM 10.5.6.6.3.1, Review of Refusal to Amend a Record.

10.5.6.6.3.1
(11-14-2023)
Review of Refusal to Amend a Record

(1) The regulations in *section 3, Appendix B of Title 31, Part I, Subpart C, of the CFR* explain how an individual requests review of refusal to amend a record.

Reminder: The IRS does not amend tax records under the Privacy Act. See IRM 10.5.6.6.3, Requests for Amendment of Non-Tax Privacy Act Records.

(2) Within 35 days of being notified of the refusal to amend a non-tax record, an individual may request an independent review of such refusal by a reviewing officer. The reviewing officer for the IRS is the Commissioner, the Deputy Commissioner, or an Assistant Commissioner. For a SOR maintained by the Office of General Counsel for the IRS, the reviewing officer is the Chief Counsel or delegate.

(3) The request must include the specific changes and the reasons for the changes, along with the elements outlined in IRM 10.5.6.6.1, How to Make a Privacy Act Request.

(4) Members of the public send requests for review of a refusal to amend a non-tax record to Privacy following the regulations in *section 3, Appendix B of Title 31, Part I, Subpart C, of the CFR* or How to write a Privacy Act request on the *IRS.gov Privacy Policy page*.

(5) Internally, send requests for review of a refusal to amend a non-tax record to Privacy via internal email to the **Privacy* mailbox.

(6) Privacy refers the request and proposed response to the proper reviewing officer for review and final determination. The reviewing officer must:

a. Respond in writing within 30 business days of the decision whether to grant the request in whole or part.
b. If you cannot respond within 30 business days, tell the individual in writing within such time of the reasons for the delay and the approximate time needed.
c. If you decide to amend the record, make the requested changes and tell the individual in your response. If you disclosed the record and accounted for it via Form 5482, Record of Disclosure, let the recipient know of the changes. See IRM 10.5.6.7, Privacy Act Accounting of Disclosures. Upon request, give the individual a copy of the record, as amended, subject to the payment of the right fees.
d. If not amending the record, tell the individual in writing of the final adverse determination with the reasons for refusal to amend the record and their right to submit a statement of disagreement in the record and of their right to seek judicial review by a United States district court of a final adverse determination under the regulations in *section 3, Appendix B of Title 31, Part I, Subpart C, of the CFR*. See IRM 10.5.6.6.3.2, Statement of Disagreement.

10.5.6.6.3.2
(11-14-2023)
Statement of Disagreement

(1) An individual who disagrees with a final determination not to amend a non-tax record under the Privacy Act may submit a concise statement for insertion in the record, stating the reasons for disagreement with the refusal of the reviewing officer.

(2) Members of the public send requests for statement of disagreement to Privacy following the regulations in *section 3, Appendix B of Title 31, Part I, Subpart C, of the CFR* or How to write a Privacy Act request on the *IRS.gov Privacy Policy page*.

(3) Internally, send requests for statement of disagreement to Privacy via internal email to the **Privacy* mailbox.

(4) Privacy sends the statement to the proper official for insertion in the individual's record.

Note: Whenever possible, bracket the contested entries in the record and place a note on the record: "See attached Statement of Disagreement."

(5) Give the statement of disagreement to all future recipients of the applicable part of the record.

10.5.6.6.4
(11-14-2023)
Requests for Disclosure of Privacy Act Records

(1) Externally, members of the public may send requests for disclosure of non-tax Privacy Act records following the How to write a Privacy Act request on the *IRS.gov Privacy Policy page*. Disclosure processes external requests.

(2) Internally, as IRS personnel, if you need to request disclosure of your non-tax Privacy Act record to a third party, ask the business unit in control of your non-tax record (usually HCO or management) in writing. You may use Form 15293, IRS Privacy Act Disclosure Consent. See IRM 10.5.6.2.3, Privacy Act Consent to Disclosure.

(3) Send questions about requests for disclosure of non-tax Privacy Act records to Privacy via internal email to the **Privacy* mailbox.

10.5.6.6.5
(11-14-2023)
Privacy Act Complaints

(1) A privacy complaint is a written allegation about a problem with or violation of privacy protections in the administration of our programs and operations that may cause harm or violation of personal or information privacy. This information may include:

- Process and procedural issues, such as consent, collection, and proper notice.
- Issues about unauthorized disclosures or identity theft mitigation.
- General IRS privacy policies and procedures
- Other Privacy Act issues.

(2) The OMB NIST security and privacy controls require agencies to implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices. [A-130; PM-26]

(3) Externally, for how the public files a Privacy Act complaint, refer to the *Privacy Complaints section of the IRS.gov Privacy Policy page*.

(4) Internally, email privacy complaints to Privacy via the **Privacy mailbox*.

(5) To resolve privacy complaints, Privacy follows the procedures outlined in the internal *Management of Privacy Complaints and Inquiries from the Public* standard operating procedure.

(6) To resolve a privacy complaint, Privacy can answer the privacy policy aspects and help those responsible resolve issues. We defer to management, Counsel, and Labor Relations for any managerial, legal, and labor issues respectively. Privacy does not have the authority to discipline misconduct of employees outside its organization.

(7) For individuals seeking action beyond the complaint resolution, they may personally follow legal options under the Privacy Act. See IRM 10.5.6.2, Privacy Act General Provisions, for civil remedies and criminal penalties for willful Privacy Act violations. If you know of a willful violation of law by an IRS employee, you may report that to TIGTA for investigation.

(8) This Privacy Act Complaints section addresses the following NIST SP 800-53 security and privacy control: PM-26 Program Management -- Complaint Management. Refer to that section of IRM 10.5.1.

10.5.6.6.6
(11-14-2023)
Requests for Privacy Act Accounting of Disclosures

(1) Subsection (c)(3) of the Privacy Act says that accounting of disclosures made under the Privacy Act are available to the individuals named in the records at their request.

Exception: Most Privacy Act accounting is for non-tax records. Accounting of disclosures of most tax records falls under IRC 6103(p)(3)(A), which exempts them from separate Privacy Act accounting. See IRM 11.3.37, Recordkeeping and Accounting for Disclosures.

(2) The request must:

a. Come from an individual and must be for an accounting of disclosures for records subject to the Privacy Act.
b. Be in writing and signed by the individual.
c. Give identification to meet the requirements discussed in IRM 10.5.6.6.2.1, Verification of Identity.
d. Be specific enough (stating the specific record or SOR and its location) to allow a search of Form 5482 files.

If the request does not include these elements, respond that you cannot process the request without them.

(3) If your office receives a request for Privacy Act accounting of records your business unit does not have, send it to the responsible office, if known, or email it to **Privacy* for privacy to contact responsible personnel. Otherwise, if your office has the records, follow these procedures.

(4) For responsibilities, time limits, and processing steps for accounting requests, including any review and adjudication of an adverse determination, refer to *section 3, Appendix B of Title 31, Part I, Subpart C, of the CFR*. This guidance mirrors that in IRM 10.5.6.6.2, Requests for Notification of and Access to Privacy Act Records, including IRM 10.5.6.6.2.1, Verification of Identity, and IRM 10.5.6.6.2.2, Duplication Fee.

(5) Privacy helps the business unit with control of the requested records respond to Privacy Act requests for accounting of disclosures.

(6) To prevent a requester from getting premature knowledge of the existence of an investigation and defeating the law enforcement process, review accountings before release and withhold those that are exempt.

(7) If a SORN lists an exemption, those records are exempt from the accounting request. Respond to the requester that the records are exempt.

(8) Also exempt are disclosures made under subsection (b)(7) (if Form 5482 shows box for (b)(7) checked). Respond to the requester that the records are exempt, unless the information is:

a. Available that the investigation which prompted the disclosure has become a matter of public record.
b. Known to the requester.
c. No longer needs protection.

(9) Using the information in the request, responsible personnel must find the Form 5482 necessary to process the Privacy Act accounting request.

(10) After finding the Form 5482, the responsible personnel must prepare a response, informing the requester that the listed items are those accountings of disclosures the Privacy Act requires the IRS to make available.

(11) The listed items in the response include:

a. Date, nature, and purpose of the disclosure.
b. System of records or specific record disclosed.
c. Name of recipient agency, activity, or person.
d. City and state address of recipient, if available.

(12) Responsible personnel must send the response to the requester.

Reminder: Give no appeal rights.

10.5.6.7
(11-14-2023)
Privacy Act Accounting of Disclosures

(1) Subsection (c) of the Privacy Act requires each agency to keep a correct accounting of the date, nature, and purpose of each non-tax disclosure of an individual's record to any person or to another agency and the name and address of the person or agency to whom the disclosure is made. This requirement only applies to records maintained in a SOR.

Note: Treasury regulations in *31 CFR 1.25* require accounting records in the least expensive and most convenient form that allows the system manager to tell individuals, promptly upon request, what records about them have been disclosed and to whom.

(2) The IRS must keep and maintain correct and complete accountings of disclosures required by the Privacy Act to be able to respond to an individual's request for access to that accounting of disclosures. Employees authorized to make disclosures of Privacy Act records must account for such disclosures using Form 5482, Record of Disclosure. See IRM 10.5.6.7.1, Form 5482 Procedure.

(3) For processing requests for Privacy Act accounting of disclosures, see IRM 10.5.6.6.6, Requests for Privacy Act Accounting of Disclosures.

(4) Most Privacy Act accounting is for non-tax records. Accounting of disclosures of most tax records falls under IRC 6103(p)(3)(A), which exempts them from separate Privacy Act accounting. See IRM 11.3.37, Recordkeeping and Accounting of Disclosures.

(5) The following disclosures of Privacy Act information do not require accounting:

a. Disclosures made to the individual or another recipient at the individual's request (with written consent) [Privacy Act section (b)]. See IRM 10.5.6.2.3, Privacy Act Consent to Disclosure.
b. Disclosures to those officers and employees of the agency that maintains the record who have a need for the record in the performance of their duties [Privacy Act section (b)(1)].
c. Disclosures made or would be required by a FOIA request [Privacy Act section (b)(2)]. Release of publicly available information maintained in a Privacy Act SOR released by a FOIA request does not require an accounting. Routinely this occurs when no FOIA exemption applies to withhold the records.
d. Tax disclosures made expressly exempt under IRC 6103(p)(3)(A). For tax disclosures, see IRM 11.3.37, Recordkeeping and Accounting for Disclosures

(6) The following NIST SP 800-53 security and privacy control addresses these Privacy Act requirements: PM-21 Program Management -- Accounting of Disclosures. Refer to this section of IRM 10.5.1.

10.5.6.7.1
(11-14-2023)
Form 5482, Record of Disclosure (Privacy Act of 1974), Procedure

(1) For accounting of disclosures under the Privacy Act, use Form 5482, Procedure, Record of Disclosure (Privacy Act of 1974).

(2) If your business unit has procedures for Form 5482, follow them. For example:

a. For HCO personnel record disclosures, refer to IRM 6.711.2, Processing Information Requests, the Analyzing/Processing the Request section.
b. For Labor Relations disclosures to TIGTA, refer to IRM 6.751.1, Discipline and Disciplinary Actions: Policies, Responsibilities, Authorities, and Guidance, in the TIGTA Cases exhibit.
c. For disclosures to the Joint Committee on Taxation under IRC 6405, refer to IRM 4.36.4, the Disclosure of Individual Information - Form 5482, Record of Disclosure section, and IRM 8.7.9, the Disclosure Provisions for JC Cases - Form 5482 section.

(3) Each employee who makes a disclosure of a record subject to the accounting requirement, must prepare Form 5482.

Example: **Non-tax disclosure by Labor Relations:** In a labor dispute, Labor Relations (LR) receives an Information Request from an authorized party (such as an employee's representative) for related personnel files, which are non-tax Privacy Act information. A Human Resources Specialist (HRS) reviews the Information Request and decides what information may be released and sends the request for that specific information to the employee's manager. That manager responds to LR with the requested documents. The HRS reviews the documents and works with the employee's manager to ensure a complete response, with proper redactions. The HRS then sends the complete response of information to the Chief of LR for that Section to sign the release of information memo. Then LR gives the information to the requestor. In this example, the manager's disclosure to LR is in the normal performance of duties to another agency official, under the Privacy Act, and does not require an accounting. The LR disclosure to the requestor requires a Privacy Act accounting. File Form 5482 with the records disclosed and keep for 5

years or the life of the record, whichever is longer. However, managers and LR specialists should discuss the accounting requirement in addressing such responses.

Example: **Non-tax disclosure in an emergency:** A manager, whose Post of Duty is in on the east coast, has employees in several locations throughout the US. During a string of heavy spring storms in the Midwest, water levels continue to rise around the area where one of their employees lives. They stay in regular contact and the employee can continue performing duties remotely, from home throughout, with no concerns. Suddenly, a single storm in the employee's area causes widespread power outages and heavy localized flooding. The employee is not online the next day and doesn't respond to phone calls. Concerned for the employee's safety during this emergency, the manager reaches out to local emergency services to complete a "wellness check" of the employee, giving name, address, and related contact information (all non-tax Privacy Act information). This disclosure by the manager to local authorities is permissible under Privacy Act subsection (b)(8) and requires an accounting. The manager must document the accounting on Form 5482 and keep it in the employee's file for five years, or the life of the file, whichever is longer. Managers are encouraged to work with Labor Relations Specialists in such events to make sure they follow and document all procedures.

(4) Though a business unit might disclose information about an individual from more than one of its SORs, the business unit should prepare an accounting record for only the SOR where the greatest amount of information is given.

Note: This procedure is consistent with the spirit of subsection (c) of the Privacy Act. Limit the number of sources when several SORs are involved to avoid confusion over the amount of information disclosed.

(5) The business unit making the Privacy Act disclosure must maintain the original Form 5482 (electronic or paper) in a separate Form 5482 file held by the official with custody of the SOR. File forms in alphabetical order by name of the subject in a separate section for each calendar year. Maintain this file for five years or the record retention period of the subject record, whichever is longer. At the end of each year, destroy all the forms that have reached the retention period. See Document 12990, Records Control Schedules, RCS 8, Item 44.

Note: Do not research to find the existence of the underlying record simply to allow destruction of Forms 5482.

(6) For paper records, copy the Form 5482 and associate the duplicate with the record disclosed and keep it for the retention period of that record.

(7) For non-paper records that prevent attaching Form 5482, do not prepare a duplicate.

(8) For multiple disclosures, where all entries would be the same, except the identity of the subject, prepare a single Form 5482 by leaving the name block blank. Attach a list of all persons involved to the original form, and place in front of the alphabetical items in the Form 5482 file. However, do not attach

the list to the copy placed in the record disclosed. Copy the Form 5482 (one for each person whose records are disclosed) and insert the proper individual's name before association with the disclosed record.

(9) Associate a Form 5482 recording a disclosure made under (b)(7) of the Privacy Act with the record disclosed only if the SOR has an exemption that would prevent the subject from getting the Form 5482 or learning of the (b)(7) disclosure. If the SOR would be generally available for the subject's inspection (such as the official personnel folder), do not associate the Form 5482 with the record. Mark it for retention to be kept for as long as its associated record file exists in the agency and file it in a special section of the Form 5482 file. Destroy the Form 5482 whenever the associated record disclosed is known to have been destroyed.

10.5.6.8
(11-14-2023)
Personnel Records

(1) The Privacy Act applies to personnel records that have information retrieved by a personal identifier, which fall under a SOR. Such records are considered employee PII. For more information about these SORs, see IRM 10.5.6.8.1, Personnel Systems of Records.

(2) While the Privacy Act applies specifically to PII in a SOR, IRS personnel must protect employee privacy and protect all PII from unauthorized access and disclosure as required by the Privacy Act, the OMB, and described throughout this IRM and IRM 10.5.1, Privacy Policy.

(3) Employees may exercise their rights under the Privacy Act about their personnel records. We must not disclose employee PII from personnel records without consent unless we follow a condition of disclosure under the Privacy Act, such as need to know.

Note: For specific Conditions of Disclosure Under the Privacy Act, see IRM 10.5.6.2.2.

Note: For Privacy Act Consent to Disclosure, see IRM 10.5.6.2.3.

Note: For disclosure of personnel records under the FOIA, refer to the Personnel Records section of IRM 11.3.13.

(4) Regulations for protecting personnel records fall under *5 CFR 293*, Personnel Records.

(5) This section and subsections give general guidelines for the protection and disclosure of certain Privacy Act personnel records or categories of records maintained by the HCO or division employees with personnel responsibilities and certain records controlled by the OPM.

(6) Personnel records include a wide range of categories, including but not limited to the following.

a. IRM 10.5.6.8.8, Promotion Files
b. IRM 10.5.6.8.9, Agency and Negotiated Agency Grievance Files
c. IRM 10.5.6.8.10, Retirement Records
d. IRM 10.5.6.8.11, Medical Records
e. IRM 10.5.6.8.12, Official Personnel Folder (OPF)
f. IRM 10.5.6.8.14, Disciplinary Action Files
g. IRM 10.5.6.8.15, Adverse Action Files

h. IRM 10.5.6.8.16, Equal Employment Opportunity Complaint Files
i. IRM 10.5.6.8.17, Supervisory Documentation Files (including EPFs)

(7) The OPM issued rules and regulations about federal records required for personnel management in *5 CFR 297, Privacy Procedures for Personnel Records*. Such rules and regulations granted individuals access to most records about themselves. We must maintain personnel records in confidence and release them only to those individuals within or outside the agency who have a definite need for the information.

Note: If records have gone to OPM, refer requests for such records to OPM.

(8) The exclusive representative (National Treasury Employees Union, NTEU, in the case of the IRS) receives access to certain information by the rights defined under 5 USC 7114(b)(4).

(9) The appropriate HCO business unit handles personnel issues. For simplicity, this IRM uses HCO personnel throughout to denote the responsible business unit for personnel issues.

10.5.6.8.1
(11-14-2023)
Personnel Systems of Records

(1) The IRS patterns its personnel SORs after those of OPM. The IRS groups the records into SORs according to similar purposes for setting up the files, similar handling of records, and similar records.

(2) The Privacy Act applies to most personnel records, as we usually maintain them by employee name, SSN, or Standard Employee Identifier (SEID). They are in one or more of the personnel SORs.

(3) The OPM also has Privacy Act responsibilities for certain personnel records maintained by federal agencies. If records have gone to OPM, refer requests for such records to OPM. Refer to *5 CFR 297* for the OPM's Privacy Act rules and regulations.

(4) HCO management serves as the system manager for most IRS personnel records. Make requests for access to IRS employee personnel records through the office maintaining the records.

(5) Request access to those records not under the control of HCO from the system managers or designees listed under each SOR in the SORN.

(6) The Privacy Act requires agencies to publish SORNs in the Federal Register. The IRS publishes its SORNs as a part of the Department of the Treasury's publication.

(7) A specific coding shows the SORs belong to Treasury and the IRS. This coding is part of the title of each SOR. The coded title for each system is Treasury/IRS followed by a five-digit number with a period after the second digit. The first two digits show the business unit and the division that controls the records.

Example: The SORNs controlled by HCO Personnel business units all have a "3" as the first digit. The SORNs controlled by HCO all have a "6" as the second digit. The last three digits following the period show the specific SOR controlled by HCO.

(8) A title for the system is also used with the coding structure.

Example: Treasury/IRS 36.001, Appeals, Grievances and Complaints Records, would show that the records are under the control of Treasury, the IRS, HCO Personnel function, and Personnel Services and that appeals, grievances, and complaints are in this system.

(9) The personnel SORs under the control of HCO Personnel include:

- Treasury/IRS 36.001, Appeals, Grievance and Complaints Records
- Treasury/IRS 36.003, General Personnel and Payroll Records

(10) Each department or agency in the federal government uses similar coding. The OPM controls certain personnel records maintained by other federal agencies. The OPM uses a coding system that shows whether the system has records of federal employees or only OPM employees, as follows:

- OPM/GOVT-1, General Personnel Records, is a government-wide SOR controlled by the OPM and has records about federal employees.
- OPM/Internal-7, Complaints and Inquiries Records, is a SOR controlled by OPM and has records on OPM employees only.

(11) The OPM also has a third SOR. This SOR has records on all federal employees that are both controlled and maintained by OPM. The coding for these systems uses the words OPM/Central.

Example: OPM/Central-1, Civil Service Retirement and Insurance Records.

(12) Two other federal agencies have government-wide systems:

- The Equal Employment Opportunity Commission controls and maintains the EEO complaint records maintained by agencies in the system EEO/GOVT-1, Equal Employment Opportunity in the Federal Government Complaint and Appeal Records.
- The Department of Labor controls and maintains records on all federal employees who have filed Workers Compensation claims. These records are in DOL/GOVT-1, Office of Workers Compensation Program, Federal Employees Compensation Act File.

10.5.6.8.2
(11-14-2023)
Requests for Personnel Records

(1) If an individual requests their own personnel records, allow them access under established procedures, subject to any access exemptions and restrictions. See IRM 10.5.6.6, Privacy Act Requests for Non-Tax Records.

(2) The HCO usually handles the release of personnel information, with a functional area Payroll Center sometimes involved. For HCO procedures, refer to the Litigations, Grievances, Arbitrations and Information Requests with Service-wide Impact section of IRM 6.300.1, Employment (General), and IRM 6.711.2, Processing Information Requests.

(3) HCO processes, under the Privacy Act:

a. Requests by employees relating to their own records.
b. Routine requests they can process under OPM rules or negotiated labor agreements.
c. Matters that traditionally fall within the area of HCO activities, if tax returns or return information subject to IRC 6103 are not involved.

Note: If records have gone to OPM, refer requests for such records to OPM under OPM/GOVT-1.

(4) Send requests citing the FOIA or involving tax returns or return information subject to IRC 6103 to Disclosure.

(5) Privacy is available to help and advise HCO on personnel records matters via the **Privacy* mailbox.

(6) HCO works requests that require payroll information. If the IRS employee whose payroll records are requested consents to release, and salary information is all that is needed by a third party, use the proper system or website.

(7) Send requests from the exclusive representative, under their rights defined in 5 USC 7114(b)(4), to the Workforce Relations office.

10.5.6.8.3
(11-14-2023)
Access to Records of Deceased Employees

(1) The Privacy Act only applies to living individuals. See OMB Guidelines, *40 Fed. Reg. 28,948*. While the Privacy Act does not give deceased employees confidentiality, their surviving families and friends have some expectations of privacy about certain aspects of records of deceased employees.

(2) Generally, the IRS privacy policy is to keep information about employees who died confidential. Sometimes the IRS may be required to disclose limited information about the deceased person to executors and relatives when the disclosure is necessary for implementation of a will or other necessary business to complete the deceased person's affairs.

(3) If a surviving family member calls for protection of sensitive graphic details about a death or other very sensitive information when disclosure would cause mental anguish and pain to the survivor, keep the following in mind:

- Survivors have the right to keep their privacy from being invaded by the disclosure of embarrassing, painful, or distressing information about the employee who died.
- When workable, only share basic information about an employee's death (name, date of death, and announced memorial services) with co-workers.
- Treat the cause of death or the identities of surviving relatives and friends as confidential, unless the next of kin says the IRS may share the information.
- As with ill employees, information given unofficially by the next of kin is not an agency record.
- Be clear about what the next of kin wants to tell co-workers. Ask for an announcement to share or invite them to send a message to send to co-workers.

(4) Email privacy and security standards require encryption to protect sensitive but unclassified (SBU) information (including PII), unless the information is meant for the public (such as a death announcement). See the Email section of IRM 10.5.1, for more information.

10.5.6.8.4
(11-14-2023)
Freedom of Information Act (FOIA) and Personnel Records

(1) If a request for access to a SOR mentions the FOIA, process the request per procedures for administering the FOIA. Refer to IRM 11.3.13, Freedom of Information Act, for further instructions.

(2) Process an access request under the statute that gives the greatest right of access to the individual regardless of the statute cited by the individual.

10.5.6.8.4.1
(11-14-2023)
Commercial Solicitation

(1) When a commercial solicitation firm requests information on employees, refer to IRM 11.3.13, the Commercial Solicitation section.

10.5.6.8.4.2
(11-14-2023)
Public Information Listing

(1) OPM has designated certain items of personnel records as public or official information, known as the Public Information Listing (PIL).

(2) For FOIA policy on disclosing this information, refer to IRM 11.3.13, the Public Information Listing section.

10.5.6.8.5
(11-14-2023)
Disclosure Under 5 USC 7114

(1) As part of the agency's and exclusive representative's (NTEU, in the case of the IRS) duty to negotiate in good faith, the *Civil Service Reform Act of 1978* (5 USC 7114(b)) defines the agency's obligation to give to the exclusive representative involved or its authorized representative, upon request and, to the extent not prohibited by law, data:

a. Which is normally maintained by the agency in the regular course of business.
b. Which is reasonably available and necessary for full and proper discussion, understanding, and negotiation of subjects within the scope of collective bargaining.
c. Which is not guidance, advice, counsel, or training offered for management officials or supervisors relating to collective bargaining.

(2) Direct requests from the NTEU under the collective bargaining rights to the Labor Relations (LR) office of HCO or other designated LR functional unit.

(3) For FOIA policy, refer to IRM 11.3.13, the Personnel Records section.

(4) For HCO policy, refer to IRM 6.711.2, Processing Information Requests.

10.5.6.8.6
(11-14-2023)
Disclosure Under IRC 6103(l)(4)

(1) Tax returns and return information may be used in disciplinary or adverse actions, suitability determinations, and other personnel decisions when relevant, under IRC 6103(l)(4). These include unemployment compensation and workers compensation cases filed by IRS employees or former employees where the IRS is the employer involved. Also included are EEO cases or Merit System Protection Board (MSPB) cases where the IRS is one of the named parties.

(2) The IRC applies here, not the Privacy Act. Refer to the Disclosure of Returns and Return Information for use in Personnel or Claimant Representative Matters - IRC 6103(l)(4) section of IRM 11.3.29.

(3) You must account for tax disclosures under the IRC, not the Privacy Act. For tax disclosure accounting procedures, refer to IRM 11.3.37, Recordkeeping and Accounting for Disclosures.

10.5.6.8.7
(11-14-2023)
Congressional Inquiries on Individuals

(1) Most Congressional inquiries on individuals relate to tax accounts. Process these under the IRC, not the Privacy Act. Refer to IRM 11.3.4, Congressional Inquiries, the Processing Requests for Disclosure section.

(2) This policy addresses non-tax Congressional Privacy Act inquiries for Privacy Act information, such as employee requests.

(3) Do not disclose Privacy Act information to the Congressional office without written consent of the individual. Routine uses for systems relating to disclosures to Congressional offices limit disclosures to inquiries made at the written request and consent of the individual who is the subject of the record(s). See IRM 10.5.6.2.3, Privacy Act Consent to Disclosure.

(4) Give publicly available non-tax information to the Congressional office without any contact with the individual subject of the record(s).

(5) Maintain letters or referrals from Congressional offices either as a part of the general correspondence files or in files such as adverse or disciplinary files.

10.5.6.8.8
(11-14-2023)
Promotion Files

(1) The term “promotion files” refers to all files set up for the purpose of selecting individuals for vacant positions. The promotion file includes those documents used or started in the selection process.

(2) The IRS maintains the promotion file by the vacancy announcement number or Promotion Certificate Number. While the information in the file may be found in other SORs, the promotion file itself is not subject to the Privacy Act unless retrieved by a personal identifier.

(3) For promotion file disclosure to employees, see that section in IRM 10.5.6.8.8.1.

(4) For promotion file disclosure to an exclusive representative under 5 USC 7114, see IRM 10.5.6.8.5, Disclosure Under 5 USC 7114.

(5) For HCO policy, refer to the Documentation and Release of Evaluative Information to Employees, Unions and Others sections of IRM 6.335.1.

(6) For promotion file disclosure to the public, refer to the Personnel Records section of IRM 11.3.13, Freedom of Information Act.

10.5.6.8.8.1
(11-14-2023)
Promotion File Disclosure to Employees

(1) Employees, acting independently of the exclusive representative under 5 USC 7114, do not receive the same amount of information as the exclusive representative when requesting information from promotion files on a bargaining unit position. See IRM 10.5.6.8.5, Disclosure Under 5 USC 7114.

(2) Delete the items listed to protect the other employees’ information:

- Names
- Dates of training
- Schooling
- Assignments

Note: Also delete pronouns and other similar identifying information.

(3) Give sufficient information to allow an employee to grieve the file.

(4) These procedures are also applicable for all non-bargaining unit promotion files, regardless of the union status of the employee requesting the file.

(5) For HCO policy, refer to the Documentation and Release of Evaluative Information to Employees, Unions and Others sections of IRM 6.335.1 .

(6) If the request is made under the FOIA, process as a FOIA request. Refer to IRM 11.3.13, the Personnel Records section.

10.5.6.8.9
(11-14-2023)
Agency and Negotiated Agreement Grievance Files

(1) Agency grievance records are those that are compiled and maintained by HCO as the result of an employee filing a grievance under IRM 6.771.1, Agency Grievance System (AGS). Negotiated Agreement Grievance Files are those records that are compiled and maintained by HCO as the result of an employee filing a grievance under one of the negotiated agreements.

(2) These files, maintained by the employee grievant's name, generally fall under the SOR for Treasury/IRS 36.001, Appeals, Grievances and Complaints Records.

(3) These files are subject to the Privacy Act, which governs access by the individual to whom the record relates. Routine use and the other disclosure provisions in subsection (b) of the Privacy Act apply.

(4) For HCO procedures, refer to the Litigations, Grievances, Arbitrations and Information Requests with Servicewide Impact section of IRM 6.300.1, Employment (General), and IRM 6.711.2, Processing Information Requests.

(5) Certain documents may receive protection from disclosure under the (d)(5) provision of the Privacy Act about information compiled in reasonable anticipation of a civil action or proceeding.

(6) To the extent third party tax information is in these files, the grievant's access, as well as the grievant's representative's access, is only under IRC 6103(l)(4)(A). Refer to the Disclosure of Returns and Return Information for use in Personnel or Claimant Representative Matters - IRC 6103(l)(4) section of IRM 11.3.29.

(7) There may be grievances with related files that are not subject to the Privacy Act, such as promotion files. Consider the disclosure of these files separately from the grievance.

(8) To the extent a request for negotiated agreement grievance files cites the FOIA, refer to the Personnel Records section of IRM 11.3.13 for more information on the right FOIA exemptions and personnel files.

10.5.6.8.10
(11-14-2023)
Retirement Records

(1) Retirement records are those records compiled because of an employee applying for voluntary retirement or disability retirement, and those retirements started by the IRS.

(2) Retirement records fall under the access provisions of the Privacy Act by the individual to whom the records relate.

(3) For disability retirement, the special provisions for access under the Privacy Act for medical records are described in IRM 10.5.6.8.11, Medical Records.

(4) Intra-management memoranda and discussions that may occur during an agency-initiated disability retirement may receive protection from disclosure under the (d)(5) provision of the Privacy Act relating to information compiled in reasonable anticipation of a civil action or proceeding

(5) Both voluntary and disability retirement records in the control of HCO fall under the SOR for Treasury/IRS 36.003, General Personnel and Payroll Records. They include information on both voluntary and disability retirement and such documents as SF-2801, Application for Retirement, health and life insurance forms, and medical records.

(6) Find disability retirement records listed in both OPM/GOVT-10, Employee Medical File System Records, and Treasury/IRS 36.003, General Personnel and Payroll Records. Access medical records associated with a disability retirement under Treasury/IRS 36.003.

Note: OPM requires approval by an OPM medical officer before an employee separates by disability retirement, and the IRS may need to keep a copy of the records while the OPM medical officer does the review. In certain circumstances, the employee's physician may give the agency the SF-3112-C, Physician's Statement, in a sealed envelope.

(7) The retirement records, once OPM receives them, fall under the SOR for OPM/Central-1, Civil Service Retirement and Insurance Records. Once OPM receives retirement records, refer all requests to OPM.

(8) For processing FOIA requests for these records, refer to the Personnel Records section in IRM 11.3.13, Freedom of Information Act.

10.5.6.8.11
(11-14-2023)
Medical Records

(1) We must keep all medical information confidential in a separate file from the individual's personnel file. Refer to HCO policy in the Requests for Medical Information and Confidentiality and Disclosure sections of IRM 1.20.2, Providing Reasonable Accommodation for Individuals with Disabilities.

Reminder: For privacy considerations about pandemics and employee illness, refer to Infectious Disease in the Workplace, Document 13001.

(2) The IRS compiles and maintains medical records at the request of both the employee and the agency.

(3) The HCO maintains medical files for HCO personnel purposes.

(4) The Health Unit maintains medical records associated with the Health Unit.

(5) The IRS maintains medical records by employee name. The purpose of the file determines its inclusion in a SOR.

(6) Most medical records are in:

- *Treasury/IRS 36.003*, General Personnel and Payroll Records
- *OPM/GOVT-10*, Employee Medical File System Records
- *Treasury .020*, Health Screening and Contact Tracing Records

(7) OPM also includes medical records associated with the OPF In *OPM/GOVT-1*, General Personnel Records.

(8) Medical records are available to the individual to whom the record relates under the Privacy Act, subject to special procedures outlined in *5 CFR 297.205*, Access to Medical Records.

(9) When medical records fall under the special handling of *5 CFR 297.205*, Access to Medical Records:

a. Release the records to the employee's chosen physician rather than to the employee. When the medical records have information that is unfamiliar or for which the HCO hesitates to release, a physician should review the requested medical records to decide whether to release the records to the individual or chosen physician.
b. Inform the employee and ask for the name and address of the chosen physician.
c. When the employee declines to choose a physician, use the services of the Health Unit physician or geographic area Medical Officer, if available.
d. When the IRS Health Unit physician or Medical Officer is unavailable and the employee refuses to choose a physician, we cannot release the records. However, we have met the requirements of the Privacy Act.
e. Once we send the medical records to the chosen physician, the physician and the employee hold responsibility for the disclosure to the employee and any financial charges involved.

(10) For medical determination records, refer to IRM 1.20.2, Providing Reasonable Accommodation for Individuals with Disabilities.

(11) For alcohol, drug abuse and Employee Assistance Program records, refer to IRM 6.800.3, Employee Assistance & Worklife Referral Program.

(12) For medical qualification records, refer to IRM 6.339.1, Medical Qualification Determination Requirements.

(13) For injury compensation records, refer to IRM 6.800.1, Workers' Compensation Program.

10.5.6.8.12
(11-14-2023)
Official Personnel Folder (OPF)

(1) The OPF is the official record of an individual's career in the federal government. For HCO policy, refer to IRM 6.300.1, the Litigations, Grievances, Arbitrations and Information Requests with Servicewide Impact section.

(2) While the OPF is an OPM file, the agency employing the individual maintains it during employment.

(3) The OPF is in OPM/GOVT-1, General Personnel Records, and includes those records in the permanent (right) part of the OPF. The temporary records on the temporary (left) part of the OPF are agency records and solely under the control of the agency and are in Treasury/IRS 36.003, General Personnel and Payroll Records SORNs.

(4) Follow the routine uses in OPM/GOVT-1 for release of information (other than public information) from the permanent part of the OPF. Follow the routine uses in Treasury/IRS 36.003 for release of information from the temporary part of the OPF.

(5) OPM/GOVT-1, designates four more items we may release to prospective non-federal employers without the prior written consent of the employee. They are:

a. Tenure of employment.

b. Civil service status.
c. Length of service in the agency and the government.
d. When separated, the date and nature of actions as shown on the Notification of Personnel Action, Standard Form 50.

(6) When an employee retires and receives a Civil Service or Federal Employee Retirement annuity or separates from federal service, the OPM takes control of the OPF and retirement records. Refer requests for such records to OPM under OPM/GOVT-1.

(7) For FOIA requests for OPF records, refer to IRM 11.3.13, the Personnel Records section.

(8) When prospective non-federal employers request information (other than public information and the four items above), you must get prior written consent from the employee.

(9) The IRS may allow access to the OPF by the individual to whom the record relates. See IRM 10.5.6.6.2, Requests for Notification of and Access to Privacy Act Records.

(10) The IRS may grant or deny a request to amend a record in the OPF; however, if denied, direct the appeal rights to OPM. See IRM 10.5.6.6.3.1, Review of Refusal to Amend a Record.

10.5.6.8.13
(11-14-2023)
Position Management and Classification and Classification Appeals Files

(1) The HCO compiles and maintains these records and files. For HCO policy, refer to IRM 6.511.1 , Position Management and Classification Policy and Operational Guidance.

(2) The IRS maintains these files and records by position designation or numbers rather than by an individual identity. Because we do not retrieve these files by an identifier, they are not Privacy Act records.

10.5.6.8.14
(11-14-2023)
Disciplinary Action Files

(1) The IRS compiles these records in anticipation of a proposed disciplinary action against an employee. OPR handles disciplinary action matters under 31 USC 330 (conference and practice). The OPR follows the general rules of this subsection in processing requests.

(2) Refer to the definition and requirements of the various disciplinary actions in IRM 6.751 , Discipline and Disciplinary Actions: Policies, Responsibilities, Authorities, and Guidance, and IRM 6.752 , Disciplinary Suspensions and Adverse Actions.

(3) These files are a part of Treasury/IRS 36.003, General Personnel and Payroll Records. Copies may also exist in Treasury/IRS 00.007, Employee Complaint and Allegation Referral Records.

(4) For the documents and records in the file, refer to IRM 6.711.2, Processing Information Requests.

(5) The HCO maintains only copies of those parts of the investigation report used as the basis of the proposed action.

(6) Since these records are maintained as a part of Treasury/IRS 36.003, the Privacy Act allows access by employees to their own disciplinary action files.

(7) These files may include intra-management memoranda and discussions that may receive protection from access by the individual to whom a file relates under the (d)(5) provision of the Privacy Act.

(8) Disclosure of tax information from these files is subject to the confidentiality provisions of IRC 6103.

(9) To the extent a request for Disciplinary Action Files is received and cites the FOIA, refer to IRM 11.3.13 for more information on the right FOIA exemptions and personnel files.

10.5.6.8.15
(11-14-2023)
Adverse Action Files

(1) The IRS compiles these records in anticipation of proposing and taking adverse action against an employee.

(2) The HCO maintains these files by the employee's name and are in Treasury/IRS 36.003, General Personnel Records. The Privacy Act allows access by employees to their own adverse action files.

(3) For certain required documents, refer to IRM 6.752, Disciplinary Suspensions and Adverse Actions.

(4) If a Treasury Inspector General for Tax Administration (TIGTA) report is used to document the charges, HCO keeps only copies of those parts about the charges.

(5) The employee or chosen representative, upon request, receives copies of the information used to support the proposed changes.

(6) These files may include intra-management memoranda and discussions that may receive protection from access by the individual to whom a file relates under the (d)(5) provision of the Privacy Act.

(7) Disclosure of tax information from these files is subject to the confidentiality provisions of IRC 6103.

(8) To the extent a request for Adverse Action Files is received and cites the FOIA, refer to IRM 11.3.13 for more information on the right FOIA exemptions and Personnel files.

10.5.6.8.16
(11-14-2023)
Equal Employment Opportunity Complaint Files

(1) The Equal Employment Opportunity (EEO) complaint files consist of materials compiled in connection with an informal complaint against the agency. For EEO policy, refer to Equal Employment Opportunity and Diversity IRM 1.20.

(2) Find EEO formal complaint files with the Treasury Office of Civil Rights and Equal Employment Opportunity (OCRE).

(3) The EEO complaint files are in Treasury/IRS 36.001, Appeals, Grievances and Complaints Records, and EEO/GOVT-1, Equal Employment Opportunity in the Federal Government Complaint and Appeal Records. The Privacy Act allows access by employees to their own complaint files.

(4) Evaluate a request for access to an EEO complaint or investigative file by an individual, other than the complainant (the subject of the file) or their representative, or an EEO Program official who holds responsibility for the processing of the complaint, under the FOIA, not the Privacy Act. Refer to IRM 11.3.13, Freedom of Information Act, for how to process under FOIA.

(5) Treasury OCRE is the official repository of EEO formal complaint files. Refer requests for such files to Treasury OCRE. The IRS Office of Equity, Diversity and Inclusion, Civil Rights and Anti-Harassment Division, assesses requests for information related to EEO complaint processing that did not advance to the formal complaint stage.

10.5.6.8.17
(11-14-2023)
Supervisory Documentation Files

(1) The IRS compiles and maintains these records at the discretion of the supervisor and as required (such as the Employee Performance File, EPF) by the HCO IRM 6.430 , Performance Management series.

(2) The SORN Treasury/IRS 36.003, General Personnel Records, covers supervisory files. The Privacy Act allows access by employees to their own documentation files.

(3) Supervisors use the records in these files primarily to evaluate and counsel employees on work performance and must protect them under *5 CFR 293*, Personnel Records. Refer to IRM 1.4.1, the Employee Performance File (EPF) section.

(4) Supervisory files may include promotion appraisal forms, narrative recordation, commendations, copies of awards, copies of SF-50s and SF-1126s, requests for training, and training evaluations. These files may also include documents required by functional managers. These documents have information such as caseloads, time reports, emergency contact lists, and other work-related information.

Reminder: Do not allow access to or share supervisory file information without consent, a need to know, or another allowable condition from IRM 10.5.6.2.2, Conditions of Disclosure Under the Privacy Act.

(5) Do not maintain outdated and irrelevant material, which could adversely affect an employee.

(6) The records maintained in the supervisory file may at times be in other files such as grievance and promotion files. Disclose tax information in these files only as authorized by IRC 6103. Those records with labor relations advice are subject to 5 USC 7114(b)(4)(C).

(7) To the extent a request for Supervisory Documentation Files is received and cites the FOIA, refer to IRM 11.3.13 for more information on the right FOIA exemptions and Personnel files.

(8) In certain circumstances, an employee may have an NTEU official in a meeting with a supervisor. You might discuss personal information (about the employee) in the employee's records in such meetings. They may have access to such personal information.

(9) The NTEU official may also contact the supervisor for copies of documents discussed or reviewed in an earlier meeting at which the employee and representative were in attendance. The supervisor cannot discuss more topics or expand upon the discussion with the representative without the prior written consent or presence of the employee.

10.5.6.9
(11-14-2023)
Privacy Act Reports

(1) PGLD headquarters generally prepare the reports in the following subsections, except that PGLD prepares the privacy section for the Federal Information Security Modernization Act (FISMA) report and sends it to IT. However, other functional units hold responsibility for giving PGLD requested information to complete sections of the reports.

10.5.6.9.1
(11-14-2023)
Privacy Act SORN Reports

(1) See IRM 10.5.6.3.12, SORN Reports.

10.5.6.9.2
(11-14-2023)
Privacy Act Request Report

(1) The IRS files an annual report with the Department of the Treasury for inclusion in the Freedom of Information Act Annual Report submission to the Department of Justice that has statistical data about Privacy Act and FOIA requests, administrative appeals, and litigation.

(2) Refer to IRM 11.3.13, the Report Submission section, for more information on this report.

10.5.6.9.3
(11-14-2023)
Annual FISMA Privacy Review and Report

(1) The Privacy Act originally required the president to send a biennial report to Congress describing the administration of the statute. However, this requirement was later repealed. In place of the biennial Privacy Act report, OMB now reports to Congress on agencies' compliance with privacy requirements through the annual Federal Information Security Modernization Act of 2014 (FISMA) report to Congress.

(2) Each year, OMB issues guidance instructing each SAOP to review the administration of the agency's privacy program and report compliance data to OMB. OMB uses the reports from agencies to develop its annual FISMA report to Congress.

(3) The PGLD office of Privacy Policy and Compliance contributes the privacy elements to this report.

10.5.6.9.4
(11-14-2023)
Annual Matching Activity Review and Report

(1) The Computer Matching and Privacy Protection Act IRM covers this content. Refer to the Annual Matching Activity Review and Report section of IRM 11.3.39.

(2) The following NIST SP 800-53 security and privacy control addresses these Privacy Act requirements: PM-24 Program Management -- Data Integrity Board. Refer to that section of IRM 10.5.1.

10.5.6.9.5
(11-14-2023)
Section 803 Reports About Privacy Act Complaints

(1) Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 requires certain executive branch departments, agencies, and elements to designate at least one senior official as a "privacy and civil liberties officer." In enacting the statute, Congress explained that such officers are meant "to function as a source of advice and oversight on privacy and civil liberties matters to the agency." More specifically, Section 803 directs that each privacy and civil liberties officer "serve as the principal advisor" to the agency with respect to three issues:

a. Assisting the agency in considering privacy and civil liberties concerns in the development and implementation of laws and policies related to efforts to protect the nation against terrorism.
b. Investigating and reviewing agency actions and procedures to make sure that the agency is adequately considering privacy and civil liberties in its actions.
c. Ensuring that the agency has adequate procedures to respond to complaints from individuals who allege that the agency has violated their privacy or civil liberties.

(2) Each agency's privacy and civil liberties officer must issue semiannual reports on the discharge of each of their functions under the statute. PGLD headquarters holds responsibility for preparing sections of the report about privacy and the Privacy Act and sending the information to Treasury, which compiles the department's reports.

(3) **Privacy Complaints formal and informal:** For report purposes, a privacy complaint is a written allegation filed with the department about a problem with or violation of privacy protections in the administration of the programs and operations of the department that may be the cause of harm or violation of personal or information privacy. This information may include:

- Process and procedural issues, such as consent, collection, and proper notice.
- Issues about unauthorized disclosures or identity theft mitigation.
- General IRS privacy policies and procedures.
- Other Privacy Act issues.

Note: For how we respond to a complaint, see IRM 10.5.6.6.5, Privacy Act Complaints.

(4) **Civil Liberties Complaints formal and informal:** For report purposes, a civil liberties complaint is a written allegation filed with the Department alleging harm or violation of an individual's constitutional rights. Civil liberties complaints include:

- First Amendment (Freedom of speech, religion, assembly, and association).
- Fourth Amendment (Protection against unreasonable search and seizure).
- Fifth Amendment or Fourteenth Amendment, section 1 (due process and equal protection).

Note: For more information on how members of the public can file a civil rights complaint, refer to the *Taxpayer Discrimination Complaints* section under the Taxpayer Civil Rights tab on the Office of Equity, Diversity, and Inclusion webpage.

(5) The following NIST SP 800-53 security and privacy control addresses these Privacy Act requirements: PM-26 Program Management -- Complaint Management. Refer to that section of IRM 10.5.1.

Exhibit 10.5.6-1 (11-14-2023)
Agency Review Requirements

The following table is from OMB Circular A-108 and lists Privacy Act agency review requirements, which the IRS meets through privacy continuous monitoring:

Review	Description	Timing	Reviewer	Citation(s)
Minimization – Continuous Monitoring	Agencies must make sure that no SOR includes information about an individual that is not relevant and necessary to accomplish a purpose required by statute or executive order.	Agencies must perform assessments of privacy controls with a frequency sufficient to ensure compliance and manage risks.	Senior Agency Official for Privacy	5 USC 552a(e)(1); section 12 of Circular A-108.
System of Records Notices – Continuous Monitoring	Agencies must make sure that all SORNs stay accurate, up-to-date, and properly scoped; that all SORNs are published in the Federal Register; that all SORNs include the information required by OMB Circular A-108; and that all significant changes to SORNs have been reported to OMB and Congress.	Agencies must perform assessments of privacy controls with a frequency sufficient to ensure compliance and manage risks.	Senior Agency Official for Privacy	5 USC 552a(e)(4); section 12 of Circular A-108.
Routine Uses – Continuous Monitoring	Agencies must make sure that all routine uses stay proper and that the recipient's use of the records continues to be compatible with the purpose for which the information was collected.	Agencies must perform assessments of privacy controls with a frequency sufficient to ensure compliance and manage risks.	Senior Agency Official for Privacy	5 USC 552a(a)(7); section 12 of Circular A-108.

Exhibit 10.5.6-1 (Cont. 1) (11-14-2023)
Agency Review Requirements

Review	Description	Timing	Reviewer	Citation(s)
Privacy Act Exemptions – Continuous Monitoring	Agencies must make sure that each exemption claimed for a SOR under 5 USC 552a(j) and (k) stays proper and necessary.	Agencies must perform assessments of privacy controls with a frequency sufficient to ensure compliance and manage risks.	Senior Agency Official for Privacy	5 USC 552a(j)-(k); section 12 of Circular A-108.
Contracts – Continuous Monitoring	Agencies must make sure that the language of each contract that involves the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of information that identifies and is about individuals, is sufficient and that the applicable requirements in the Privacy Act and OMB policies are enforceable on the contractor and its employees.	Agencies must perform assessments of privacy controls with a frequency sufficient to ensure compliance and manage risks.	Senior Agency Official for Privacy	5 USC 552a(m); section 12 of Circular A-108.
Privacy Training – Continuous Monitoring	Agencies must make sure that the agency's training practices are sufficient and that agency personnel understand the requirements of the Privacy Act, OMB guidance, the agency's implementing regulations and policies, and any job-specific requirements.	Agencies must perform assessments of privacy controls with a frequency sufficient to ensure compliance and manage risks.	Senior Agency Official for Privacy	5 USC 552a(e)(9); section 12 of Circular A-108.

Exhibit 10.5.6-1 (Cont. 2) (11-14-2023)
Agency Review Requirements

Review	Description	Timing	Reviewer	Citation(s)
FISMA Review – Annual	The Senior Agency Official for Privacy must review the administration of the agency's privacy program as part of the annual FISMA reporting process.	Agencies must refer to OMB's annual FISMA guidance for review instructions.	Senior Agency Official for Privacy	44 USC 3551-3558; section 13 of Circular A-108.
Review of Matching Programs – Annual (refer to IRM 11.3.39, Computer Matching and Privacy Protection Act)	Agencies' Data Integrity Boards must review all matching programs in which the agency has participated during the calendar year.	Agencies' Data Integrity Boards must conduct the review at the end of the calendar year and report to OMB by June 1.	Agency's Data Integrity Board	5 USC 552a(u)(3)(B)-(C); section 14 of Circular A-108.
Review of Other Matching Activities – Annual (refer to IRM 11.3.39)	Agencies' Data Integrity Boards may also review any agency matching activities that are not matching programs.	Agencies' Data Integrity Boards must conduct any review at the end of the calendar year and report to OMB by June 1.	Agency's Data Integrity Board	5 USC 552a(u)(3)(H); section 14 of Circular A-108.

The following NIST SP 800-53 security and privacy controls address these Privacy Act requirements. Refer to these sections of IRM 10.5.1:

a. CA-1 Assessment Authorization and Monitoring -- Policy and Procedures
b. CA-2 Assessment Authorization and Monitoring -- Control Assessments
c. CA-6 Assessment Authorization and Monitoring – Authorization
d. CA-7 Assessment Authorization and Monitoring -- Continuous Monitoring
e. CA-7(4) Assessment Authorization and Monitoring -- Continuous Monitoring – Risk Monitoring
f. PM-9 Program Management -- Risk Management Strategy
g. PM-31 Program Management -- Continuous Monitoring Strategy
h. PT-6(1) Personally Identifiable Information Processing and Transparency -- System of Records Notice - Routine Uses
i. PT-6(2) Personally Identifiable Information Processing and Transparency -- System of Records Notice – Exemption Rules
j. RA-1 Risk Assessment -- Policy and Procedures
k. RA-3 Risk Assessment -- Risk Assessment

Exhibit 10.5.6-2 (11-14-2023)
Agency Public Website Posting Requirements

The following table is from OMB Circular A-108 and lists Privacy Act agency public website posting requirements:

Posting	Description	Location	Citation(s)
Compilation of agencies' system of records notices and Privacy Act implementation rules	The Office of the Federal Register must post a compilation of agencies' system of records notices and Privacy Act implementation rules.	The website of the Federal Register at https://www.federalregister.gov/.	5 USC 552a(f).
System of Records Notices	Agencies must list and give links to complete, up-to-date versions of all agency SORNs.	www.treasury.gov/privacy ***Note:*** https://www.irs.gov/privacy for IRS	5 USC 552a(e)(4); section 15 of Circular A-108.
Matching Notices and Agreements	Agencies must list and give links to up-to-date matching notices and agreements for all active matching programs.	www.treasury.gov/privacy	5 USC 552a(o), (r); section 15 of Circular A-108.
Privacy Act Exemptions	Agencies must give citations and links to all Privacy Act exemption rules	www.treasury.gov/privacy	5 USC 552a(j)-(k); section 15 of Circular A-108.
Privacy Act Implementation Rules	Agencies must list and give links to all Privacy Act implementation rules.	www.treasury.gov/privacy	5 USC 552a(f); section 15 of Circular A-108.
Instructions for Submitting a Privacy Act Request	Agencies must give instructions for individuals who wish to send an access or amendment request.	www.treasury.gov/privacy	5 USC 552a(d); section 15 Circular A-108.

Exhibit 10.5.6-3 (11-14-2023)
Reporting Requirements

The following table is from OMB Circular A-108 and shows various Privacy Act reporting requirements for exemption rules, new or significantly modified SORs, matching programs and FISMA. The IRS sends the reports to Treasury for approval. Upon approval, Treasury sends the reports to OMB.

Report	Description	Timing	Recipient(s)	Citation(s)
Privacy Act Implementation and Exemption Rules	Agencies must send Privacy Act rules to OMB under applicable regulatory review procedures and as part of a proposal to establish or significantly modify a SOR.	Agencies must give proposed and/or final rules before publication and consult OMB about applicable review procedures.	OMB (via ROCIS system).	5 USC 552a(f), (j)-(k); Executive Orders 12866 and 13563; sections 10 and 11 of Circular A-108.
Report of New or Significantly Modified System of Records	Agencies must report any proposal to establish or significantly modify a SOR.	Agencies must send reports at least 30 days before submission of the notice to the Federal Register.	OMB (via ROCIS system) and Congress (via mail).	5 USC 552a(r); section 7 of Circular A-108.
Report of New or Significantly Modified Matching Program	Agencies must report any proposal to establish, re-establish, or significantly modify a matching program.	Agencies must send reports at least 30 days before submission of the notice to the Federal Register.	OMB (via ROCIS system) and Congress (via mail).	5 USC 552a(r); section 9 of Circular A-108.
Annual Matching Activity Report	Agencies' Data Integrity Boards must send a report describing any matching programs that occurred during the calendar year.	Agencies must send the annual report for the preceding calendar year to OMB by June 1.	OMB (via email to privacy-oira@omb.eop.gov) and the head of the agency.	5 USC 552a(u)(3)(D); section 14 of Circular A-108.
Annual FISMA Privacy Report	The Senior Agency Official for Privacy must report privacy compliance information to OMB as part of the annual FISMA reporting process.	Agencies must refer to OMB's annual FISMA guidance for reporting instructions.	OMB (see OMB's annual FISMA guidance for reporting instructions).	44 USC 3551-3558; section 13 of Circular A-108.

Exhibit 10.5.6-4 (11-14-2023)
Federal Register Publication Requirements

The following table is from OMB Circular A-108 and lists the requirements for creating a Federal Register notice and associated reports for OMB and the Congressional committees that oversee the Privacy Act:

Publication	Description	Timing	Citation(s)
System of Records Notices	Agencies must publish a notice in the Federal Register describing the existence and character of a new or significantly modified SOR. Agencies must also publish a notice of rescindment when the agency stops maintaining a SOR.	A new or revised SORN is effective upon publication in the Federal Register, except for any new or modified routine uses, which require a minimum of 30 days after publication in the Federal Register before they can become effective.	5 USC 552a(e)(4); section 6 of Circular A-108.
Matching Notices	Agencies must publish a notice in the Federal Register describing an established, re-established, or significantly modified matching program.	A new or revised matching notice is not effective until at least 30 days after its publication in the Federal Register.	5 USC 552a(e)(12); section 8 of Circular A-108.
Privacy Act Implementation Rules	Agencies must issue rules to implement the provisions of the Privacy Act.	Agencies must publish a final rule before the rule is effective.	5 USC 552a(f); section 10 of Circular A-108.
Privacy Act Exemption Rules	In certain circumstances, agencies may issue a rule to exempt a SOR from certain requirements of the Privacy Act.	Agencies must publish a final rule before the exemption is effective.	5 USC 552a(j)-(k); section 11 of Circular A-108.

Exhibit 10.5.6-5 (11-14-2023)
Terms and Acronyms

Term	Definition or description
Agency	Includes any executive department, military department, government corporation, government-controlled corporation, or other establishment in the executive branch of the [federal] government (including the Executive Office of the President), or any independent regulatory agency.
Annual Report	The report by the president to the Speaker of the House and the President of the Senate, required by 5 USC 552a(s). See IRM 10.5.6.9.3, Annual FISMA Privacy Review and Report.
Approving Official	a. Area Managers and Directors of IRS Computing Centers for their respective offices; b. In headquarters, division directors or equivalent positions.
Authority	The **authority** that authorizes the collection of the information would generally be the applicable sections of the IRC.
CIP	Compliance Initiative Project
CFR	Code of Federal Regulations
CPO	Chief Privacy Officer
Determination	Any decision affecting the individual that is in whole or in part based on information in the record and that is made by any person or any agency.
OL	Department of Labor
EEO	Equal Employment Opportunity
EEOC	Equal Employment Opportunity Commission
Effects on individual	The **effects** upon an individual for not supplying all or part of the requested information, including incidental effects such as possible accrual of interest, loss of benefits, initiation of enforcement action, or other applicable results of that individual's refusal.
EPF	Employee Personnel Folder
FAR	Federal Acquisition Regulations
Federal Inventory of Personal Data Systems	The requirement that SORNs be published in a form available to the public at low cost, under 5 USC 552a(f). See IRM 10.5.6.3.5, Content of a SORN.
FISMA	Federal Information Security Modernization Act of 2014
FOIA	Freedom of Information Act
GAO	Government Accountability Office
GLDS	Governmental Liaison, Disclosure and Safeguards
GRS	General Records Schedule
GSS	GLDS Support Services
HCO	Human Capital Office

Exhibit 10.5.6-5 (Cont. 1) (11-14-2023)
Terms and Acronyms

Term	Definition or description
HRS	Human Resources Specialist
Individual	A citizen of the United States or an alien lawfully admitted for permanent residence (including sole proprietors). The Privacy Act does not apply to any entity that is not a natural person, such as a partnership, corporation, decedent, estate, or trust.
Information from Third Parties	Information collected about individuals from someone other than the individual. It does not include the following: • Information received from the individual or their representative. • Information required to be filed with the IRS, such as a Form W-2 from an employer or Form 1099 from banks and other payers of income. • Information given by anyone to resolve specific cases worked by the IRS. ***Example:*** Examination of a return, collection of taxes, resolution of match errors or information return discrepancies. • Information received from state tax agencies under an exchange agreement under IRC 6103(d)
IRC	Internal Revenue Code
IT	Information Technology
LR	Labor Relations
Maintain	The terms maintenance, maintain, or keep refer to the privacy lifecycle of information: creation, collection, receipt, use, processing, maintenance, access, inspection, display, storage, disclosure, dissemination, or disposal of information about an individual.
Mandatory or voluntary disclosure	Whether the individual must give the information requested or may refuse to do so.
MSPB	Merit Systems Protection Board
NARA	National Archives and Records Administration
Necessary	Requisite or needful in doing a given task.
Notice of Exempt System	Rules issued by a head of agency to exempt any SOR from provisions of the Privacy Act under 5 USC 552a(j) and/or (k).
NTEU	National Treasury Employees Union
OMB	Office of Management and Budget
OIRA	(OMB's) Office of Information and Regulatory Affairs
OPF	Official Personnel Folder
OPM	Office of Personnel Management
OPR	Office of Professional Responsibility

Exhibit 10.5.6-5 (Cont. 2) (11-14-2023)
Terms and Acronyms

Term	Definition or description
PAPRAN	Privacy Act and Paperwork Reduction Act Notice
PCLIA	Privacy and Civil Liberties Impact Assessment
PCM	Privacy Continuous Monitoring
PGLD	Privacy, Governmental Liaison and Disclosure
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIL	Public Information Listing
POD	Post of Duty
PPC	Privacy Policy and Compliance
Privacy	Privacy Policy and Knowledge Management
PRA	Paperwork Reduction Act
Principal purpose(s)	The reason the information is needed, which is the overall reason the IRS performs the operation where it will use the information.
privacy lifecycle	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.
RCS	Records Control Schedule
Record	Defined in 5 USC 552a(a)(4) as any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to education, financial transactions, medical history, and criminal or employment history and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. a. A record can include as little as one descriptive item about an individual. b. A file or list with only names but headed by a label that conveys some information about the people named could constitute a record if retrieved by an individual identifier. ***Note:*** Congressional intent was to encompass all records and record systems whereby specific information on an individual is retrieved in any fashion. However, such lists occurring within a SOR do not form separate systems. c. The physical form of a record within a system is irrelevant. A record that has information about an individual and is retrievable by an individual identifier may be in any form that technology allows and would be subject to the Privacy Act.
Relevant	Means pertinent to and bearing upon the matter at hand.

Exhibit 10.5.6-5 (Cont. 3) (11-14-2023)
Terms and Acronyms

Term	Definition or description
Report on New Systems	The advance notice to Congress and the OMB of any proposal to establish or alter any SOR, which is required by 5 USC 552a(r). For more information on such reports, see IRM 10.5.6.3.12, SORN Reports.
RISC	Regulatory Information Service Center
ROCIS	RISC/OIRA Consolidated Information System
Routine uses	The disclosure of a record outside the Department of the Treasury for a purpose that is compatible with the purpose for which it was collected.
SAOP	Senior Agency Official for Privacy
SB/SE	Small Business/Self Employed
SBU	Sensitive But Unclassified
SEID	Standard Employee Identifier
SOR	System of Records
SORN	System of Records Notice
SSN	Social Security Number
System of records	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 particular assigned to the individual.
System of Records Notice	Information that must be published in the Federal Register by 5 USC 552a(e)(4). See IRM 10.5.6.3.5, Content of a SORN.
TIGTA	Treasury Inspector General for Tax Administration
USC	United States Code

Exhibit 10.5.6-6 (11-14-2023)
References and Resources

Resource	Title or Description
The Privacy Act, 5 USC 552a	*The Privacy Act, 5 USC 552a*
U.S. Department of Justice, Office of Privacy and Civil Liberties home page	*https://www.justice.gov/opcl*
Overview of the Privacy Act of 1974, 2020 Edition	*https://www.justice.gov/Overview_2020/download*
TD P 25-04, Privacy Act Handbook	*https://home.treasury.gov/system/files/236/Privacy-Act-Handbook-Final.pdf*
Chief Counsel Directives Manual (CCDM) 37.2.1, Privacy Act of 1974	*CCDM 37.2.1, Privacy Act of 1974; Freedom of Information Act - Privacy Act of 1974*
Disclosure and Privacy Law Reference Guide	Pub 4639
Document 12829	IRS Records Control Schedules
Document 12990	General Records Schedules
Form 5482	Record of Disclosure (Privacy Act of 1974)
Form 15293	IRS Privacy Act Disclosure Consent
IRM 10.9.1, Classified National Security Information	Gives instructions for the proper handling and disposition of all classified National Security information.
IRM 1.15 series, Records and Information Management	Gives instructions for the proper handling of information (hard copy and electronic) in the creation, maintenance, retrieval, preservation, and disposition of all records.
IRM 10.2, Physical Security Program	Gives instructions for the protection of records.
IRM 10.5.1, Privacy Policy	Gives privacy policy information and instructions.
IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance	Gives instructions for security requirements for electronic records.
IRM 11.3, Disclosure of Official Information	Gives instructions for disclosure of tax records in conjunction with the Privacy Act requirements.
NIST SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations, December 2020